GERENCIAMENTO DE RISCOS DE TECONOLOGIA E SEGURANÇA DA INFORMAÇÃO

1. OBJETIVO

O presente documento constitui uma declaração formal da Cooperativa de Economia e Crédito Mútuo dos Empregados das Empresas de Diversões do Estado de São Paulo acerca de seu compromisso com a proteção das informações de sua propriedade, estabelecendo diretrizes corporativas que permitam aos colaboradores e cooperados seguirem padrões de comportamento relacionados à segurança, adequados às necessidades de negócio e de proteção legal da empresa e do indivíduo Levou-se em consideração o porte e complexidade da COOPERPARQUES, cooperativa do segmento "capital x empréstimos" que opera apenas na modalidade de crédito consignado. Considera o volume de operações a complexidade de suas atividades, seus serviços e seus produtos, atendendo, assim, o princípio da proporcionalidade.

Esta política tem como guias principais os conceitos e orientações das normas ABNT ISO/IEC da família 27000, com suas alterações posteriores e as normativas do Banco Central.

2. RESPONSABILIDADE

É responsabilidade de cada colaborador da cooperativa manter-se atualizado em relação a esta política e aos procedimentos e normas relacionadas, buscando orientação do seu gestor ou da área de Tecnologia sempre que não estiver absolutamente seguro quanto a aquisição, uso e/ou descarte de informações. As diretrizes aqui definidas são extensíveis a prestadores de serviços da empresa, sendo responsabilidade da área contratante o repasse e respeito à política.

O Comitê Gestor da Segurança Cibernética, representado por um membro da Conselho de Administração, é responsável pela criação e atualização desta política, assim como normas e procedimentos derivados. A atualização ocorrerá anualmente ou sempre que algum fato relevante motive sua revisão antecipada.

Os colaboradores da COOPERPARQUES devem assinar um documento de responsabilidade (ou aceitar responsabilidade por algum meio eletrônico verificável) pelo cuidado físico e integridade dos equipamentos ou componentes de tecnologia designados pela COOPERPARQUES, incluindo

aqueles designados aos fornecedores ou terceiros sob sua responsabilidade.
Este documento deve incluir a assinatura do responsável pelo gestor responsável ao que foram designados os equipamentos. É obrigação dos referidos usuários informar ao gestor qualquer situação anormal ao respeito.

3. ÁREA GESTORA DA POLÍTICA DE SEGURANÇA

Responsável: Conselheiro responsável pela Política de Segurança
Atribuições: Responsável pela Política de Segurança

4. ESCOPO

As diretivas desta política visam proteger a informação de diversos tipos de ameaças, garantindo a continuidade dos negócios, minimizando os danos e maximizando as oportunidades de negócio.
A segurança da informação é aqui caracterizada pela preservação da:

Integridade – Garantia de que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas;

Confidencialidade – Garantia de que o acesso à informação seja obtido somente por pessoas autorizadas;

Disponibilidade – Garantia de que os usuários autorizados obtenham acesso às informações e aos ativos correspondentes sempre que necessário;

Quaisquer informações geradas ou recebidas por colaboradores como resultado da atividade profissional pertence a referida instituição, sendo que as exceções devem ser explicitamente formalizadas em contrato entre as partes. Os equipamentos de informática, comunicação, sistemas e informações utilizados pelos colaboradores são destinados à realização de atividades

profissionais, sendo o uso pessoal eventual permitido desde que não prejudique o desempenho dos sistemas e serviços.

A COOPERPARQUES poderá monitorar e registrar o uso dos sistemas e serviços visando garantir a disponibilidade e segurança das informações utilizadas.

Esta política se aplica a todas as áreas da COOPERPARQUES suas dependências e outras unidades que possam vir a ser constituídas.

5. DIRETRIZES

A seguir são listadas as diretrizes gerais dos assuntos relacionados com a segurança da informação:

Os colaboradores e prestadores de serviços, usando a infraestrutura de tecnologia, concedem sua conformidade absoluta com as políticas corporativas de tecnologia.

Incluindo, ilimitado, seu consentimento para investigações, leitura e/ou revisões que as áreas designadas fazem relativas às informações, dados, arquivos, conteúdo e mensagens que enviam, recebem, armazenam ou acesso, utilizando a infraestrutura de Tecnologia da COOPERPARQUES, incluindo informações, dados e documentos pessoais, sujeito a restrições provenientes de legislação aplicável e com conformidade com as diretrizes de gestão de dados pessoais de acordo à legislação do país.

Os colaboradores devem consultar com o gestor, quaisquer perguntas sobre o uso de qualquer componente da infraestrutura de tecnologia para fins pessoais.

Na COOPERPARQUES é considerado “PROIBIDO” os serviços de e-mail, mensagem instantânea e internet, aplicações e infraestrutura como segue:

a) Qualquer atividade que interfira com as funções ou demanda produtividade dos colaboradores da COOPERPARQUES, já estão quem faz isso ou quem são afetados pelo mesmo.
b) Busca, acesso, consulta, publicação ou transferência de conteúdo que não cumpre o código de ética do negócio COOPERPARQUES
c) Uso do software ou acesso aos sites da internet para conseguir o anonimato nas atividades realizadas e / ou na transferência de informação da internet.

d) Enviar mensagens, documentos ou bens da informação da COOPERPARQUES, dos colaboradores, dos seus cooperados ou dos seus fornecedores, a sites ou contas pessoais ou públicos sem haver a devida autorização do gestor da Cooperativa;
e) uso de e-mail, mensagem instantânea e internet como mídia de comunicação oficial a COOPERPARQUES por quem não está autorizado a fazer;

Em casos de violação desta política, a COOPERPARQUES reserva o direito de restringir ou cancelar o acesso a qualquer serviço mensagens instantâneas, e-mail, mídia social ou página de internet, total ou parcialmente, como determinado pela área de segurança.
Todas as conexões de rede de internet COOPERPARQUES deve ser feito por meio de mecanismos de segurança (por exemplo firewall), filtro de conteúdo e registro de atividade, de acordo com as normas de tecnologia, todo tráfego de mensagens, dados ou informações, de ou para qualquer equipe que está conectada às redes COOPERPARQUES deve seguir por tais mecanismos, ou o equipamento informático que este conecte à rede COOPERPARQUES em nenhum evento deve ser simultaneamente conectada às redes de terceiros.

5.1 Correio Eletrônico

A COOPERPARQUES através do pessoal designado, sem qualquer condição de privacidade para os colaboradores, podem monitorar, investigar, ler e/ou verifique toda a atividade que os colaboradores e prestadores de serviços, incluindo sem limite as informações, dados, conteúdo e mensagens ou arquivos enviadas, recebidas ou armazenadas, assim como sites da internet que visita e a atividade que faz nesses sites com o objetivo de garantir a integridade dos sistemas informação e redes, a qualidade de operação do mesmo e com o objetivo de verificar conformidade com os termos de utilização dos sistemas. Apresentados na política atual e cumprimento de outras políticas da COOPERPARQUES.

5.2 Acesso à Internet

A Internet deve ser utilizada para fins corporativos, enriquecimento intelectual ou como ferramenta de busca por informações, enfim, tudo que possa vir a contribuir para o desenvolvimento de atividades relacionadas à empresa. O uso da internet para assuntos pessoais (home banking, lojas virtuais e afins) é permitido desde que com bom senso e respeitando as demais diretivas de segurança estabelecidas.

É vedado o uso da Internet para:

i. Acesso a sites de relacionamento ou com conteúdo impróprio;
ii. Qualquer tipo de download e upload;
iii. Uso de softwares “peer-to-peer” (P2P);
iv. Acesso a computadores remotos.

Os acessos externos à rede interna, para fins de manutenção de infraestrutura ou sistemas, somente poderão ser realizados através de empresas formalmente contratadas pela COOPERPARQUES.

Os acessos à internet serão monitorados através de identificação do usuário, podendo ser bloqueados a qualquer momento pela equipe de tecnologia quando for identificado risco ao funcionamento do ambiente.

A estrutura de firewalls da empresa implementa o bloqueio de acesso a sites através do uso de blacklists de mercado. Qualquer exceção deve ser solicitada através de solicitação formal, identificando a exceção, o motivo e a vigência da liberação. A solicitação será analisada pelo Gestor.

5.3 Controle de Acesso Físico

Manter restrito, por controles físicos apropriados e proporcional à criticidade dos equipamentos, o acesso a todas as áreas onde serão processadas ou armazenadas informações pertinentes à operação da cooperativa, mantendo lista de acesso a estes ambientes.

5.4 Controle de Acesso (Lógico)

O colaborador é responsável por todos os atos executados com suas credenciais de acesso e, portanto, deve:

i. Manter a confidencialidade, memorizar e não registrar as senhas em qualquer lugar;
ii. Alterar a senha sempre que existir qualquer suspeita de comprometimento de sua confidencialidade;
iii. Selecionar senhas de qualidade, não triviais;
iv. Evitar o uso de seu equipamento por outros colaboradores enquantoeste estiver conectado com suas credenciais;
v. Bloquear sempre o equipamento ao se ausentar da estação (Ctrl+Alt+Del);
vi. Não transferir ou compartilhar a senha com ninguém. É terminantemente proibido o compartilhamento de login;
vii. Não habilitar logins automáticos utilizando o recurso de memorização de senhas.

A COOPERPARQUES implementa a rigidez de senha exigida pela regulação em seus sistemas nativos e nas ferramentas de terceirizadas (sempre que possível).
Para os logins de colaboradores (que possuem acesso a sistemas internos da empresa) estabelece-se os requisitos mínimos de senha a seguir:

i. Tamanho mínimo de 8 caracteres;
ii. Proibição de reuso das últimas 6 senhas utilizadas na alteração;
iii. Exigência de complexidade alta (maiúsculas, minúsculas, caracteres especiais, números);
iv. Expiração de senha a cada 90 dias;
v. Bloqueio de senha após 3 tentativas erradas;
vi. Desbloqueio de senha somente por acesso administrativo;
vii. Armazenamento em banco de forma criptografada.

A criação/uso de logins genéricos deve ser evitada, mas mesmo nos casos onde são imprescindíveis (logins de sistema, por exemplo), devem sempre estar associados a um responsável na empresa (planilha mantida com a Conselho de Administração).

Logins de visitantes, fornecedores, temporários (pessoas físicas ou jurídicas) devem ser claramente diferenciados dos logins de colaboradores.

A criação e bloqueio de logins são atribuições da equipe de tecnologia mediante fluxo aberto através de chamado aberto em ferramenta correspondente.

O fluxo compreende as seguintes etapas:

i. Solicitação da COOPERPARQUES de admissão/demissão;
ii. Ativação ou bloqueio do login do colaborador (rede, e-mail e demais plataformas integradas) pela equipe de tecnologia (suporte);
iii. Definição do permissionamento do colaborador pelo Gestor.

5.5 Backup

Todos os dados críticos da empresa são guardados em estruturas remotas com monitoração e procedimentos regulares de restauração. Maiores detalhes podem ser obtidos na Política de Backup.

5.6 Softwares

Somente softwares homologados poderão ser utilizados no parque tecnológico da COOPERPARQUES. Anualmente será realizado um inventário de software em todas as estações, sendo facultado a área de tecnologia a desinstalação de qualquer software não homologado sem aviso prévio ao colaborador. A presença de softwares não homologados será comunicada ao gestor da área, que tomará as medidas cabíveis.

5.7 Antivírus

Todos os equipamentos da empresa, sejam eles servidores ou estações, devem possuir antivírus instalados.

5.8 Classificação dos Dados

Conceder acesso aos dados com base no que somente será dado acesso à informação para a pessoa que tiver a necessidade de conhecer aquela informação;
Classificar os dados de forma a identificar seu nível de confidencialidade;
A classificação poderá ser:
Público: quando o conteúdo puder ser distribuído a qualquer pessoa interna ou externa e for de conhecimento geral;
Somente Interno: conteúdo produzido pela COOPERPARQUES para conhecimento exclusivo de seus colaboradores, terceiros e fornecedores;
Confidencial: conteúdo sensível e de acesso apenas as pessoas que devam conhecer seu conteúdo.

5.9 Chaves de Criptografia e Certificados Digitais

Manter de forma segura, a guarda das chaves de criptografia para acesso aos
recursos computacionais;
Manter registro de todas as chaves de criptografia e Certificados Digitais existentes, informando o dono e o mantenedor;
Documentar processo de guarda, renovação, revogação e inutilização de certificados digitais.

5.10 Testes de Invasão periódicos

Periodicamente executar rotinas para testar a defesa contra possíveis ataques aos seus sistemas de informação, rotinas estas denominadas de Penetration Test;
As rotinas deverão ser executadas por empresa especializada;
Estas rotinas serão realizadas em sistemas e ambientes que sejam acessíveis via internet.

5.11 Conscientização e Comunicação

Todos os colaboradores deverão receber periodicamente informações sobre potenciais ameaças à integridade dos sistemas de informação.

5.12 Rede Wi-fi

A empresa implementa redes sem fios segregadas, sendo a rede “Visitantes” usada basicamente para acesso à internet, sem acesso à rede corporativa e com menor rigidez e robustez. A rede “Corporativa”, entretanto, tem acesso normal aos recursos da rede, exigindo liberação prévia do equipamento com a equipe de tecnologia.

5.13 Descarte ou Armazenamento de Informação

Nenhuma informação confidencial deve ser deixada à vista, seja em papel ou em quaisquer outros dispositivos, eletrônicos ou não. Ao usar uma impressora coletiva, o colaborador deve recolher o documento impresso imediatamente.

6. DIVULGAÇÃO

Para uniformidade da informação, a PSI – Política de Segurança da Informação deve ser divulgada tão logo aprovada pela Conselho de Administração, seja na sua constituição ou em quaisquer atualizações que se façam necessárias.
Adicionalmente deve ser disponibilizada na empresa permitindo fácil acesso ou consulta a qualquer colaborador. A política também deve ser divulgada para novos colaboradores, no processo de integração.

7. VIOLAÇÕES DA POLITICA E SANÇÕES

O descumprimento das diretrizes desta política, mesmo que por mero desconhecimento, sujeitará o infrator a sanções administrativas, incluindo a aplicação de advertência verbal ou escrita, demissão por justa causa ou rescisão contratual, bem como sujeitará o infrator às demais penalidades administrativas, cíveis e penais previstas na legislação brasileira.

É dever de todo colaborador comunicar ao Gestor a ocorrência de incidente que afete a segurança da informação, que por sua vez escalará ao Conselho de Administração para análise quando assim for necessário.

8. REGULAMENTAÇÃO ASSOCIADA

Resolução Conselho Monetário Nacional - CMN nº 2.554/98

Resolução CMN nº 4.606/17

São Paulo, 10 de março de 2020.

ROBSON COELHO DA SILVA

Presidente

SHEILA MENDES OLIVEIRA

Tesoureira

FABIO FREIRE ROCHA

Secretário

COOPERATIVA DE ECONOMIA E CREDITO MUTUO DOS EMPRE:68314921000162

Assinado de forma digital por COOPERATIVA DE ECONOMIA E CREDITO MUTUO DOS EMPRE:68314921000162
Dados: 2020.07.07 12:20:07 -03'00'