POLÍTICA DE SEGURANÇA DA INFORMAÇÃO - PSI

A **Associação dos Registradores de Imóveis do Paraná - ARIPAR** visando proteger e garantir a confidencialidade, integridade e disponibilidade das informações constantes nos sistemas utilizados, elaborou a presente política de segurança a ser observada por todos os profissionais que atuam na associação.

OBJETIVO

O objetivo da presente política de segurança é prevenir dados e padronizar procedimentos, sendo que no longo prazo, servirá como mecanismo de prevenção de incidentes relacionados às informações.

Através da orientação e do estabelecimento das diretrizes da ARIPAR para proteger seus ativos de informação, a presente política visa determinar os padrões de comportamentos relacionados à segurança da informação adequados às necessidades do negócio e os de proteção legal da entidade e de seus indivíduos.

Os riscos típicos que a aplicação deste Código pretende evitar são:

- Compartilhamento e uso indevido de dados pessoais;
- Alterações indevidas de dados e programas;
- Perda de dados e programas;
- Destruição ou perda de recursos e instalações;
- Roubo/furto de propriedade;
- Acessos não autorizados.

Estão sujeitos aos riscos citados através dos seguintes motivos:

- Negligência – atos não intencionais de usuários;
- Subversão – ataques disfarçados praticados por usuários;
- Acidente – ocorrências acidentais e por fatores alheios;
- Ataque furtivo – ataques praticados por pessoas estranhas;
- Ataque forçado – ataques às claras praticados por usuários ou estranhos;
- Ilícitas - ocorrências Ilícitas e por fatores alheios.

Rua Marechal Deodoro, nº 51, 18º andar, Conjuntos 1805-1810, Galeria Ritz, Centro, Curitiba - PR.
presidente@aripar.org

DIMENSÃO

Os termos constantes na PSI aplicam-se a todos os funcionários, estagiários, prestadores de serviços e a todo e qualquer profissional que possua acesso aos sistemas de informação da associação.

PRINCÍPIOS

a) CONFIDENCIALIDADE – todas as informações constantes nos sistemas de informação da associação só podem ser acessadas por pessoas devidamente autorizadas;
b) DISPONIBILIDADE – as informações dos arquivos da associação estão disponíveis para o correto tratamento a ser realizado pelas pessoas autorizadas;
c) INTEGRIDADE – as informações devem permanecer completas e íntegras, de forma a não serem modificadas ou destruídas de forma acidental.

CONCEITOS

1.1 Dados pessoais e informações

As informações e os dados pessoais são resultado da produção, manipulação, organização ou processamento de dados que represente uma modificação no conhecimento do sistema que a recebe. Um dado não é considerado informação quando, sem o devido processamento, for insuficiente para conferir sentido ou significado a uma determinada matéria. Porém, será considerado como informação o dado que, mesmo não processado, for suficiente para produzir modificações no conhecimento de sistemas humanizados ou informatizados.

1.2 Equipamento

O equipamento é todo dispositivo utilizado para processamento, produção, transformação, manipulação, organização ou transmissão de informações no ambiente da associação ou que seja de sua propriedade. Essa denominação engloba computadores, impressoras, scanners, smartphones, roteadores, switches, servidores, centrais telefônicas, aparelhos telefônicos, câmeras, monitores, dentre outros. No contexto desta política os equipamentos podem ser referenciados como hardware.

Rua Marechal Deodoro, nº 51, 18º andar, Conjuntos 1805-1810, Galeria Ritz, Centro, Curitiba - PR.
presidente@aripar.org

1.3 Empregado

É a denominação dada à pessoa contratada cujo vínculo de cunho empregatício é regido pela CLT - Consolidação das Leis do Trabalho.

1.7 Prestador de Serviço ou Terceiro

Parte contratada pela ARIPAR que tem acesso às instalações, recursos e informações necessárias para o cumprimento de suas obrigações profissionais.

REQUISITOS

Em busca da uniformização das práticas da associação, a PSI será comunicada a todos os funcionários, bem como fará parte dos documentos a serem entregues aos futuros profissionais que atuarem na associação, juntamente com o contrato de trabalho.

A PSI poderá ser alterada sempre que se fizer necessário, havendo fato relevante ou algum evento que motive sua retificação, total ou parcial.

Todos os funcionários devem ser orientados acerca de procedimentos de segurança, bem como correto uso dos equipamentos da associação, de forma a reduzir o acontecimento de incidentes.

Havendo qualquer incidente de segurança da informação, a associação está devidamente preparada para repará-lo ou reduzir os possíveis danos sempre que possível. O profissional que deve ser instado a manifestar-se é o encarregado de dados, no âmbito da Lei Geral de Proteção de Dados – LGPD.

A não obediência ao presente plano de segurança de informação acarreta a violação das normas internas e sujeitará o funcionário a responder pelas medidas cabíveis.

CLASSIFICAÇÃO DAS INFORMAÇÕES

As informações constantes na associação possuem os seguintes níveis de confidencialidade:

a) PÚBLICA – toda informação acessada pelos usuários em geral ou funcionários. Exemplo: informações constantes em murais, redes sociais ou sites.
b) INTERNA – informação interna é aquela que deve ser de conhecimento

Rua Marechal Deodoro, nº 51, 18º andar, Conjuntos 1805-1810, Galeria Ritz, Centro, Curitiba - PR.
presidente@aripar.org

somente dos agentes internos da associação (presidente e funcionários em geral). Exemplo: portarias internas ou circulares internas.

c) CONFIDENCIAL – é toda informação que pode ser acessada somente a pessoas previamente autorizadas, sendo que a publicidade destas informações pode causar impacto aos envolvidos.

d) RESTRITA – são informações que podem ser acessadas somente a determinadas pessoas, sendo que a divulgação não autorizada pode comprometer a estratégia organizacional da associação. Exemplo: folha de pagamento.

RESPONSABILIDADES

São responsabilidades de todos os agentes relacionados à associação:

- dar cumprimento à presente PSI;
- proteger as informações a que tiverem acesso, impedindo ou reduzindo o risco de perda, modificação ou destruição incidental;
- assegurar que os recursos e informações sejam utilizados somente para o fim específico;
- dar cumprimento a todas as leis e normas que tiverem conhecimento acerca de proteção de dados pessoais;
- não efetuar qualquer comentário que diga respeito às informações restritas, confidenciais ou internas, em ambientes públicos ou com pessoas diversas do ambiente organizacional;
- não compartilhar qualquer informação que tenha acesso em decorrência da função desempenhada na associação;
- comunicar ao responsável qualquer suspeita ou incidente que tiver conhecimento envolvendo informações.

CORREIO ELETRÔNICO

O correio eletrônico corporativo deve ser usado com base nas diretrizes a seguir.

É vedado aos funcionários da associação:

- remeter mensagens não requeridas, exceto para uso de atividade da associação;
- utilizar endereço eletrônico alheio para envio de mensagens, ou assinar em nome de terceiro;
- enviar qualquer informação por e-mail que possa ocasionar qualquer dado à

Rua Marechal Deodoro, nº 51, 18º andar, Conjuntos 1805-1810, Galeria Ritz, Centro, Curitiba - PR.
presidente@aripar.org

associação nas esferas cíveis ou criminais;

- enviar qualquer informação não autorizada, imagens, documentos, ou qualquer outro, sem a devida autorização;
- adulterar ou falsificar informações com objetivo de evitar punições;
- deletar informações ou mensagens de cunho corporativo sem a devida autorização;
- enviar mensagens que:

a) possuam conteúdos de ameaças como por exemplo spam ou vírus;
b) contenham qualquer arquivo que represente risco à segurança do destinatário;
c) possua como objetivo obter acesso não autorizado a outro computador;
d) possua como objetivo interromper serviço por meio de qualquer método ilícito;
e) possua como objetivo burlar qualquer sistema de segurança;
f) possua como objetivo assediar, ameaçar, vigiar ou intimar outro usuário;
g) possua como objeto acessar informações restritas;
h) possua qualquer conteúdo impróprio ou não relacionado à atividade;
i) possua conteúdos obscenos ou ilegais;
j) possua caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, entre outros da mesma natureza, ainda que não especificados;
k) contenha aspecto de perseguição moral ou preconceituosa relacionada à sexualidade, raça, incapacidade física ou mental, dentre outras na mesma natureza, ainda que não especificadas;
l) possuam fins políticos partidários;
m) possuam materiais protegidos por direitos autorais, sem a devida permissão para compartilhamento.

Todas as mensagens enviadas por correio eletrônico devem conter o nome completo e o departamento do subscritor.

DO USO DA INTERNET

O uso da internet nos equipamentos da associação deve obedecer aos presentes critérios de segurança. Toda informação acessada, transmitida, recebida ou produzida poderá ser objeto de monitoramento pelo responsável da associação.

Os equipamentos fornecidos são de propriedade da associação, que poderá, através do presidente ou pessoa por ele indicada, se necessário, bloquear acesso a sites que não dizem respeito à atividade desempenhada e estejam colocando em risco o correto funcionamento dos serviços inerentes.

O acesso a redes sociais é restrito às contas da associação. Toda tentativa de

Rua Marechal Deodoro, nº 51, 18º andar, Conjuntos 1805-1810, Galeria Ritz, Centro, Curitiba - PR.
presidente@aripar.org

alteração dos parâmetros de segurança, por qualquer colaborador, sem o devido credenciamento e a autorização para tal, será julgada inadequada.

Apenas os colaboradores autorizados pela instituição poderão copiar, captar, imprimir ou enviar imagens da tela para terceiros, devendo atender à norma interna de uso de imagens, à Lei de Direitos Autorais, à proteção da imagem garantida pela Constituição Federal e demais dispositivos legais.

Os downloads ou uploads de arquivos devem ser autorizados pelo responsável e possuir relação direta com a atividade desempenhada na associação, sendo que, em nenhuma hipótese, os computadores da associação poderão ser utilizados para disseminação de material ou programas pirateados.

O acesso a softwares de compartilhamento não é permitido. Já os programas de mensagens instantâneas poderão ser autorizados pelo controlador, desde que possuam finalidade com a atividade prestada.

IDENTIFICAÇÃO DOS EQUIPAMENTOS

Todos os equipamentos da associação são devidamente identificados, devendo possuir senha de acesso individual e de conhecimento restrito aos que o utilizam, estando cientes os funcionários que o uso dos dispositivos e/ou senhas de identificação de outra pessoa constitui crime tipificado no Código Penal Brasileiro (art. 307 – falsa identidade).

O usuário responsável pelo equipamento é única e exclusivamente responsável pelo seu uso correto. Assim, todo e qualquer dispositivo só poderá ser compartilhado com autorização do responsável.

Em caso de login compartilhado a responsabilidade é solidária dos que utilizarem da referida identificação, salvo se for possível identificar o autor do dano.

SEGURANÇA DOS EQUIPAMENTOS

As senhas de acesso ao computador e aos sistemas devem possuir caracteres de segurança, variando entre letras, números e caracteres especiais, sempre que possível, devendo ser evitadas senhas evidentes.

É de responsabilidade de cada usuário a memorização de sua própria senha.

As senhas não devem ser anotadas ou armazenadas em arquivos eletrônicos

Rua Marechal Deodoro, nº 51, 18º andar, Conjuntos 1805-1810, Galeria Ritz, Centro, Curitiba - PR.
presidente@aripar.org

(Word, Excel etc.), compreensíveis por linguagem humana (não criptografados); não devem ser baseadas em informações pessoais, como próprio nome, nome de familiares, data de nascimento, endereço, placa de veículo, nome da associação, nome do departamento; e não devem ser constituídas de combinações óbvias de teclado, como “abcdefgh”, “87654321”, entre outras.

Os usuários podem alterar a própria senha, e devem ser orientados a fazê-lo, caso suspeitem que terceiros obtiveram acesso indevido ao seu login/senha.

É proibido todo procedimento de manutenção física ou lógica, instalação, desinstalação, configuração ou modificação, sem o conhecimento prévio do responsável, ou de quem este determinar.

Todas as atualizações e correções de segurança do sistema operacional ou aplicativos somente poderão ser feitas após a devida validação no respectivo ambiente de homologação, e depois de sua disponibilização pelo fabricante ou fornecedor. Os sistemas e computadores devem ter versões do software antivírus instaladas, ativadas e atualizadas permanentemente. O usuário, em caso de suspeita de vírus ou problemas na funcionalidade, deverá acionar o departamento técnico responsável.

É expressamente proibido o consumo de alimentos, bebidas ou fumo na mesa de trabalho e próximo aos equipamentos.

BACKUP

A associação deverá possuir método eficaz de forma a garantir o correto backup dos dados, através de agendamento automatizado ou qualquer outra forma que garanta o funcionamento ininterrupto.

DISPOSIÇÕES FINAIS

A presente política de segurança da informação inicia sua vigência na presente data, podendo sofrer alterações sempre que se fizer necessário.

Curitiba, 09 de outubro de 2022.

Rua Marechal Deodoro, nº 51, 18º andar, Conjuntos 1805-1810,
Galeria Ritz, Centro, Curitiba - PR.
presidente@aripar.org