POLÍTICA DE SEGURANÇA DA INFORMAÇÃO
ARCESP SEGURADORA S.A.

Com a finalidade de resguardar seus bens informacionais de forma segura e íntegra, a ARCESP Seguradora S.A. implementa esta política. O documento atua como um pilar de sua governança corporativa, direcionando a Companhia a operar em total conformidade com as diretrizes e padrões do mercado.

1. Objetivo e Abrangência

1.1. **Objetivo**

Esta política visa ser um conjunto de diretrizes que oriente e conscientize todos os envolvidos sobre o uso responsável e seguro da informação. Nosso objetivo é garantir a observância e aplicação dos princípios inerentes à segurança da informação.

1.2. **Abrangência**

Esta Política se aplica a todos os colaboradores, prestadores de serviço, terceirizados e qualquer pessoa com poderes de representação da Seguradora. É obrigação de cada um se manter atualizado sobre o conteúdo desta Política e as normas relacionadas, buscando orientação junto às áreas responsáveis sempre que houver dúvidas sobre as diretrizes apresentadas.

2. Governança e Responsabilidades

A Seguradora estabelece uma estrutura de governança clara para a segurança da informação, definindo responsabilidades em todos os níveis hierárquicos para garantir a eficácia desta política. Nela, a Diretoria Executiva é responsável por aprovar a política e garantir os recursos necessários; a área de TI e seus gestores, com o apoio do diretor de Controles Internos, supervisionam sua implementação e monitoram os controles.

3. Princípios e Diretrizes

3.1. Para a eficácia desta política, a Seguradora adota os seguintes princípios:

- Confidencialidade, Integridade e Disponibilidade: Assegurar que os dados da Companhia sejam acessados apenas por pessoas autorizadas (confidencialidade), que sua exatidão e completude sejam preservadas (integridade) e que os sistemas e informações estejam acessíveis quando necessário (disponibilidade).
- Conformidade Legal e Regulatória: Cumprir integralmente todos os requisitos de segurança da informação exigidos pela Lei Geral de Proteção de Dados (LGPD) — Lei nº 13.709/2018 —, pela Circular SUSEP nº 619/2020 e por outras leis e regulamentações aplicáveis, garantindo a existência de um sistema de controles internos eficaz.
- Gerenciamento de Riscos: Elaborar, implantar e seguir procedimentos de segurança da informação para mitigar riscos, garantindo que ameaças sejam identificadas, analisadas e tratadas de forma proativa.

- Educação e Conscientização: Promover uma cultura de segurança por meio da educação e conscientização contínua de todos os colaboradores e parceiros sobre as práticas de proteção da informação.
- Tratamento de Incidentes: Tratar todos os incidentes de segurança de forma completa e imediata, garantindo que sejam adequadamente registrados, investigados e corrigidos. As comunicações às autoridades competentes serão realizadas sempre que exigido.

4. Controles e Procedimentos de Segurança da Informação

4.1. A Seguradora adota um conjunto de controles e procedimentos para garantir a proteção e o sigilo de seus ativos de informação.

4.2. **Proteção de Dados e Privacidade**

A Companhia assegura que o tratamento de dados pessoais, desde a sua coleta até o descarte, é realizado em conformidade com a Lei Geral de Proteção de Dados (LGPD). Os direitos dos titulares dos dados, como o de acesso, correção e eliminação, são respeitados e podem ser exercidos por meio dos canais oficiais da empresa.

4.3. **Gestão de Acessos**

A gestão de acessos é um pilar da segurança e da privacidade. A identidades e os acessos aos sistemas e informações são controlados de forma rigorosa, baseados no princípio de que cada usuário deve ter acesso apenas ao que é estritamente necessário para realizar suas funções.

4.4. **Segurança de Infraestrutura e Aplicações**

Os sistemas, redes e softwares da empresa são submetidos a um processo contínuo de gestão de vulnerabilidades, que busca identificar e corrigir falhas de segurança proativamente. Medidas como a segurança de redes, segurança de software e a segurança física dos ambientes tecnológicos são implementadas para proteger os ativos.

4.5. **Resposta a Incidentes e Continuidade de Negócios**

A Companhia possui um plano de resposta a incidentes de segurança da informação, com o objetivo de identificar, conter, mitigar e erradicar ameaças de forma ágil e eficaz. Este plano se integra ao Plano de Continuidade de Negócios, garantindo que as operações críticas sejam restabelecidas rapidamente em caso de um evento adverso.

4.6. **Gestão de Terceiros**

A segurança da informação se estende a toda a cadeia de valor. A Seguradora exige que seus terceiros, prestadores de serviço e fornecedores sigam padrões de segurança compatíveis, garantindo que o tratamento de informações compartilhadas seja seguro e em total conformidade com esta política.

4.7. **Programa de Conscientização**

Um programa de conscientização em segurança da informação é promovido continuamente para que todos os colaboradores e parceiros entendam seu papel na proteção dos dados da empresa. O objetivo é fortalecer a cultura de segurança na instituição, garantindo que as práticas adequadas sejam adotadas no dia a dia.

5. **Vigência e Revisão**

Esta política tem vigência a partir do momento de sua publicação e aprovação pela Diretoria Executiva será revisitada periodicamente para análise e possível alteração, caso seja necessário.

Versão	Data de Aprovação	Responsável pela Elaboração	Instância da Aprovação	Natureza da Alteração
1.0	**15/12/2025**	**Controles Internos**	**Diretoria Executiva**	**Emissão Inicial**