Sumário Executivo

Esta Política Pública de Segurança da Informação - PPSI formaliza o compromisso institucional da UmmA Seguros com a proteção das informações tratadas em sua operação, incluindo dados de clientes, proponentes, segurados, beneficiários, colaboradores, terceiros, seguradoras, operadoras e parceiros comerciais.

A política foi estruturada para ser publicável, sem exposição de dados confidenciais ou controles técnicos sensíveis, e para demonstrar maturidade, diligência e alinhamento ao negócio de seguros, à gestão de riscos da corretora, à LGPD, às boas práticas da ISO/IEC 27001, às diretrizes da ISO/IEC 27005:2022 e às exigências regulatórias e contratuais aplicáveis ao ecossistema segurador e de saúde suplementar.

A segurança da informação é tratada como extensão natural da atividade da corretora: uma organização que atua com proteção, mitigação de riscos e confiança deve aplicar internamente princípios equivalentes de cuidado, governança, prevenção e responsabilidade.

1. Introdução

A essência do mercado segurador é a mitigação de riscos, a proteção patrimonial, a proteção da vida, a continuidade das relações de confiança e a preservação da reputação das partes envolvidas. Na UmmA Seguros, compreendemos que a excelência na prestação de serviços de corretagem, intermediação, apoio comercial, gestão de propostas, relacionamento com clientes e suporte em sinistros depende da proteção adequada das informações que nos são confiadas.

Esta Política Pública de Segurança da Informação - PPSI expressa o compromisso da corretora com a confidencialidade, integridade, disponibilidade, autenticidade, rastreabilidade, prevenção, responsabilidade e uso adequado das informações, em linguagem pública e sem exposição de detalhes internos que possam comprometer a segurança da organização.

Protegemos informações porque protegemos pessoas, relações comerciais, expectativas legítimas, obrigações regulatórias, interesses de segurados, beneficiários e clientes, bem como a própria continuidade da corretora e de sua cadeia de confiança.

2. Objetivo

O objetivo desta PPSI é estabelecer as diretrizes públicas que orientam a proteção das informações tratadas pela UmmA Seguros, demonstrando à sociedade, aos clientes, às seguradoras, às operadoras, aos parceiros comerciais, aos colaboradores e aos demais terceiros o compromisso institucional da corretora com segurança da informação, privacidade, gestão de riscos, continuidade de negócios e conformidade.

São objetivos específicos desta política:

- declarar o compromisso da corretora com a proteção das informações e dos dados pessoais tratados em suas atividades;
- alinhar a segurança da informação à gestão de riscos corporativos e ao negócio de seguros;
- demonstrar aderência às boas práticas da ISO/IEC 27001 e da ISO/IEC 27005:2022, de forma proporcional ao porte, à complexidade e ao perfil de riscos da corretora;
- evidenciar o compromisso da corretora com seguradoras, operadoras e parceiros regulados, inclusive em razão dos reflexos contratuais e operacionais de normas setoriais como a Circular SUSEP nº 638/2021;

- orientar, em nível público, as práticas de classificação da informação, controle de acessos, compartilhamento seguro, gestão de incidentes, continuidade de negócios, temporalidade documental e conscientização de colaboradores;

- indicar a relação desta PPSI com a Política de Privacidade da corretora, que detalhará finalidades, bases legais, direitos dos titulares e canais de atendimento relacionados à proteção de dados pessoais.

3. Escopo e Abrangência

Esta PPSI aplica-se às informações tratadas pela UmmA Seguros no relacionamento com clientes, proponentes, segurados, beneficiários, dependentes, colaboradores, sócios, prestadores de serviços, seguradoras, operadoras de saúde suplementar, parceiros comerciais, fornecedores, correspondentes, consultores, escritórios de apoio e demais terceiros que participem ou interajam com suas atividades.

A política abrange informações em meio físico, digital, verbal, documental, sistêmico, contratual, operacional ou comercial, independentemente do local, sistema, plataforma ou canal por meio do qual sejam recebidas, armazenadas, acessadas, transmitidas, compartilhadas, processadas, arquivadas ou descartadas.

Por se tratar de documento público, esta PPSI não substitui políticas, normas, procedimentos, planos, matrizes de risco, manuais operacionais, instruções de trabalho e controles internos mantidos pela corretora em ambiente restrito.

4. Princípios de Segurança da Informação

A UmmA Seguros adota princípios de segurança da informação compatíveis com seu porte, suas atividades, seus riscos e as expectativas de clientes, seguradoras, operadoras e parceiros. A proteção da informação é orientada pelos seguintes princípios:

- Confidencialidade: informações devem ser acessadas apenas por pessoas autorizadas e para finalidades legítimas.

- Integridade: informações devem ser mantidas completas, corretas, confiáveis e protegidas contra alterações indevidas.

- Disponibilidade: informações e recursos essenciais devem estar disponíveis de acordo com as necessidades do negócio e os planos de continuidade.

- Autenticidade: a origem, a identidade e a legitimidade das informações e interações devem ser protegidas por mecanismos adequados.

- Rastreabilidade: acessos, operações críticas e eventos relevantes devem ser registrados na medida adequada ao risco, à finalidade e à viabilidade técnica.

- Necessidade e menor privilégio: o acesso às informações deve ser limitado ao necessário para o exercício da função ou execução da atividade.

- Prevenção e melhoria contínua: riscos devem ser identificados, avaliados, tratados, monitorados e revisados de forma contínua.

- Responsabilidade e prestação de contas: áreas, colaboradores, gestores e terceiros devem atuar de forma diligente, documentada e compatível com suas responsabilidades.

5. Governança, Gestão de Riscos e Melhoria Contínua

A segurança da informação é tratada pela corretora como responsabilidade institucional, integrada à governança corporativa, à gestão de riscos, à continuidade do negócio, à conformidade regulatória e à proteção da reputação da organização.

A corretora adota abordagem baseada em riscos, inspirada nas boas práticas da ISO/IEC 27001 e nas diretrizes da ISO/IEC 27005:2022, contemplando, de forma proporcional ao seu porte e à complexidade de suas atividades:

- identificação de ativos de informação, processos críticos e fluxos relevantes;
- identificação de ameaças, vulnerabilidades, eventos de risco e impactos potenciais;
- análise e avaliação de riscos considerando probabilidade, impacto, criticidade, sensibilidade das informações e dependência de terceiros;
- definição e priorização de medidas de tratamento de riscos;
- registro de decisões, responsáveis, prazos, riscos residuais e critérios de aceitação;
- monitoramento periódico da eficácia dos controles adotados;
- revisão da matriz de riscos diante de mudanças relevantes de processos, tecnologias, fornecedores, exigências contratuais, incidentes ou alterações legais e regulatórias.

O Comitê de Gestão de Segurança da Informação - GSI, ou instância equivalente designada pela Alta Direção, acompanha a evolução das diretrizes de segurança, promove revisões periódicas, apoia a priorização de medidas de proteção e reporta temas relevantes à Alta Direção.

6. Alinhamento com o Mercado Segurador, SUSEP, ANS e Parceiros Regulados

A UmmA Seguros reconhece que atua em uma cadeia de confiança composta por clientes, seguradoras, operadoras, prestadores de serviços, parceiros comerciais, plataformas tecnológicas e entidades sujeitas a diferentes exigências legais, regulatórias e contratuais.

Embora determinadas normas setoriais, como a Circular SUSEP nº 638/2021, sejam diretamente aplicáveis às sociedades supervisionadas pela SUSEP, a corretora reconhece seus reflexos na cadeia de valor do mercado segurador e mantém práticas de segurança compatíveis com as exigências contratuais, operacionais e reputacionais das seguradoras parceiras.

Nesse contexto, a corretora busca reduzir riscos em cascata, apoiar a continuidade da cadeia de confiança, demonstrar diligência em segurança da informação e cooperar, quando aplicável, com processos de due diligence, auditorias, avaliações de terceiros e exigências razoáveis de parceiros regulados.

Quando atuar na intermediação, apoio comercial ou relacionamento envolvendo produtos relacionados à saúde suplementar, a corretora observa as exigências contratuais e regulatórias aplicáveis ao setor, bem como os deveres de confidencialidade, segurança e proteção de dados pessoais, especialmente quanto a dados de saúde e demais dados pessoais sensíveis.

A atuação da corretora é orientada pela proporcionalidade, pela boa-fé, pela prevenção, pela necessidade e pelo compromisso institucional de proteger os dados de quem confia em seus serviços.

7. Classificação da Informação e Proteção de Dados

A corretora adota critérios internos de classificação da informação considerando sensibilidade, criticidade, finalidade, titularidade, risco, exigências legais, exigências contratuais, necessidade de acesso e impacto potencial em caso de acesso indevido, alteração, perda, indisponibilidade ou divulgação não autorizada.

As informações podem ser classificadas, conforme critérios internos, em categorias como pública, interna, confidencial e restrita. A classificação orienta o nível de proteção aplicável, incluindo regras de acesso, armazenamento, transmissão, compartilhamento, retenção e descarte.

Dados pessoais e dados pessoais sensíveis recebem tratamento compatível com a Lei Geral de Proteção de Dados - LGPD, com as finalidades informadas aos titulares e com os requisitos contratuais, regulatórios e operacionais aplicáveis ao mercado de seguros e, quando cabível, à saúde suplementar.

São exemplos de informações que podem exigir proteção reforçada, conforme o contexto: dados cadastrais, dados de contato, documentos de identificação, informações financeiras, propostas, apólices, boletos, comunicações comerciais, declarações pessoais de saúde, informações sobre beneficiários, dados de dependentes, dados de sinistros, informações de contratação e documentos comprobatórios.

Dados pessoais sensíveis, quando necessários à cotação, contratação, manutenção, execução, regulação, cobrança ou suporte de produtos securitários ou de saúde suplementar, são submetidos a controles adicionais de acesso, confidencialidade, compartilhamento e retenção.

8. Bases Legais e Relação com a Política de Privacidade

O tratamento de dados pessoais realizado pela corretora deve observar a LGPD, os princípios de finalidade, adequação, necessidade, transparência, segurança, prevenção, responsabilização e prestação de contas, bem como as bases legais aplicáveis a cada finalidade.

As bases legais poderão incluir, conforme o caso concreto e a finalidade do tratamento:

- execução de contrato ou procedimentos preliminares relacionados a contrato, tais como cotação, proposta, intermediação, contratação, renovação, endosso, assistência e suporte;
- cumprimento de obrigação legal ou regulatória;
- exercício regular de direitos em processo judicial, administrativo ou arbitral;
- consentimento, quando exigido ou adequado à finalidade específica;
- legítimo interesse, observados os direitos e liberdades fundamentais dos titulares e, quando aplicável, avaliação de balanceamento;
- proteção do crédito, conforme legislação aplicável;
- prevenção à fraude e segurança do titular, especialmente em processos de identificação e autenticação;
- tutela da saúde, quando aplicável e dentro dos limites legais;
- proteção da vida ou da incolumidade física do titular ou de terceiros, quando pertinente.

As finalidades específicas, bases legais, categorias de dados pessoais, compartilhamentos, direitos dos titulares e canais de atendimento serão detalhados na Política de Privacidade da corretora, documento complementar a esta PPSI.

Esta PPSI não tem por finalidade substituir avisos de privacidade, contratos, termos de consentimento, registros de operações de tratamento, relatórios de impacto ou demais documentos de governança em privacidade.

9. Controle de Acessos e Segregação de Funções

A corretora adota o princípio do menor privilégio e da necessidade de acesso, de modo que colaboradores, sócios, prestadores e terceiros autorizados tenham acesso às informações estritamente necessárias para o exercício de suas funções, execução de contratos, cumprimento de obrigações ou prestação de serviços.

Os acessos a sistemas, plataformas, bases de dados, documentos, e-mails, diretórios, repositórios físicos e digitais devem ser concedidos, alterados, revisados e revogados conforme critérios internos de segurança, segregação de funções, aprovação adequada e compatibilidade com as responsabilidades do usuário.

A corretora adota controles para evitar acessos generalizados ou incompatíveis com as atribuições funcionais, observando segregação de funções sempre que aplicável, especialmente em processos que envolvam dados pessoais de clientes, dados sensíveis, propostas, apólices, sinistros, documentos financeiros, informações estratégicas e dados de parceiros.

O desligamento, mudança de função, encerramento de contrato ou alteração de escopo de atuação deve ensejar revisão, revogação ou ajuste dos acessos concedidos, conforme procedimentos internos.

Credenciais de acesso são pessoais e intransferíveis. O compartilhamento de senhas, contas ou mecanismos de autenticação é vedado, salvo exceções formalmente tratadas em procedimento interno específico, quando tecnicamente inevitáveis e devidamente controladas.

10. Compartilhamento Seguro de Dados

O compartilhamento de informações pela corretora deve observar finalidade legítima, necessidade, segurança, base legal aplicável, compatibilidade contratual e pertinência operacional.

Dados de clientes, proponentes, segurados, beneficiários e demais titulares podem ser compartilhados, conforme a finalidade, com seguradoras, operadoras, estipulantes, plataformas tecnológicas, prestadores de serviços, assessorias, escritórios especializados, parceiros comerciais, autoridades públicas, órgãos reguladores ou terceiros necessários à prestação dos serviços, sempre observados os limites legais, contratuais e regulatórios aplicáveis.

A corretora busca manter instrumentos contratuais adequados com terceiros que tratem informações em seu nome ou em colaboração com suas atividades, contemplando, quando aplicável, cláusulas de confidencialidade, segurança da informação, proteção de dados pessoais, responsabilidade, cooperação em incidentes, subcontratação, retenção e descarte.

Não são realizados compartilhamentos incompatíveis com as finalidades informadas, com as bases legais aplicáveis ou com as expectativas legítimas dos titulares, salvo quando exigido por lei, regulamento, ordem de autoridade competente ou exercício regular de direitos.

Sempre que possível e adequado, a corretora adota medidas de minimização, restrição de acesso, registro, proteção de transmissão e limitação de uso das informações compartilhadas.

11. Gestão de Terceiros e Parceiros

A segurança da informação depende de uma cadeia de proteção que ultrapassa os limites internos da corretora. Por essa razão, fornecedores, prestadores de serviços, plataformas, parceiros comerciais e demais terceiros que tenham acesso a informações da corretora ou de seus clientes devem observar padrões mínimos de segurança, confidencialidade e proteção de dados compatíveis com a criticidade das atividades desempenhadas.

A corretora poderá realizar avaliações proporcionais de terceiros, considerando a natureza do serviço, o volume e a sensibilidade dos dados tratados, o grau de dependência operacional, a criticidade do fornecedor, a existência de subcontratações, a localização do tratamento, o histórico de incidentes e as exigências de seguradoras, operadoras ou parceiros regulados.

Contratações consideradas relevantes ou críticas podem demandar evidências adicionais, tais como políticas de segurança, acordos de confidencialidade, cláusulas de proteção de dados, comprovação de controles, certificações, relatórios, compromissos de notificação de incidentes, planos de continuidade ou outros documentos compatíveis com o risco.

A gestão de terceiros deve ser revisada periodicamente e sempre que houver alteração relevante no serviço, no risco, na criticidade do fornecedor, na legislação aplicável ou em exigências contratuais de seguradoras, operadoras e parceiros.

12. Conscientização de Colaboradores e Cultura de Segurança

A UmmA Seguros reconhece que tecnologia, processos e contratos somente produzem resultados efetivos quando acompanhados de comportamento responsável, cultura de segurança e consciência sobre riscos.

A corretora mantém programa de conscientização de colaboradores, proporcional ao seu porte e à natureza das informações tratadas, contemplando treinamentos, orientações, comunicações internas, cartilhas, termos de responsabilidade, políticas de uso aceitável e reforços periódicos sobre boas práticas de segurança e proteção de dados.

A comunicação de segurança deve ser séria, clara, educativa, objetiva e compatível com o ambiente corporativo da corretora, evitando informalidade excessiva e priorizando responsabilidade institucional, conformidade, prevenção, confiança e proteção das pessoas.

Os temas de conscientização podem incluir, entre outros:

- sigilo profissional e confidencialidade;
- proteção de dados pessoais e dados sensíveis;
- prevenção a phishing, engenharia social, fraudes e golpes digitais;
- uso adequado de e-mail, internet, dispositivos, sistemas e documentos;
- classificação, armazenamento, envio e descarte de informações;
- comunicação de suspeitas, fragilidades, perdas, acessos indevidos ou incidentes;
- responsabilidades individuais e consequências do descumprimento de políticas internas.

13. Gestão de Incidentes de Segurança

A corretora mantém diretrizes para identificação, comunicação, análise, classificação, contenção, tratamento, recuperação e registro de incidentes de segurança da informação, incluindo incidentes que possam envolver dados pessoais.

Suspeitas de acesso indevido, perda, indisponibilidade, alteração não autorizada, envio incorreto, vazamento, fraude, malware, comprometimento de credenciais, falha relevante de sistema, extravio de documentos ou qualquer evento que possa comprometer a segurança da informação devem ser comunicados pelos colaboradores e terceiros conforme canais e procedimentos internos.

A gestão de incidentes deve observar critérios de criticidade, impacto, urgência, dados envolvidos, titulares afetados, obrigações contratuais, exigências legais e necessidade de comunicação a clientes, seguradoras, operadoras, parceiros, autoridades ou titulares.

Quando o incidente envolver dados pessoais e puder acarretar risco ou dano relevante aos titulares, a corretora avaliará a necessidade de comunicação à Agência Nacional de Proteção de Dados - ANPD e aos titulares, observando os prazos, requisitos e critérios legais aplicáveis, incluindo a regulamentação vigente sobre comunicação de incidentes de segurança.

A corretora poderá cooperar com seguradoras, operadoras e parceiros regulados em processos de apuração, mitigação, comunicação e resposta a incidentes que envolvam informações compartilhadas no contexto da prestação dos serviços.

Informações detalhadas sobre procedimentos internos de resposta, equipes, contatos operacionais, fluxos de escalonamento, ferramentas, registros técnicos e lições aprendidas são mantidas em documentos internos de acesso restrito.

14. Continuidade de Negócios

A continuidade de negócios é componente essencial da confiança depositada na corretora. A organização mantém diretrizes para preservação de processos críticos, recuperação de atividades e manutenção de serviços essenciais diante de eventos adversos.

O Plano de Continuidade de Negócios - PCN, mantido em documentação interna, contempla estratégias proporcionais ao porte e ao risco da corretora para lidar com indisponibilidade de sistemas, falhas de fornecedores críticos, incidentes cibernéticos, perda de documentos, indisponibilidade de instalações, ausência de pessoas chave e outros eventos que possam comprometer a operação.

As estratégias de continuidade podem envolver, conforme aplicável, backups, procedimentos alternativos, priorização de processos críticos, comunicação com clientes e parceiros, recuperação de sistemas, acionamento de fornecedores, controles de contingência e revisões periódicas.

A corretora busca assegurar que atividades vitais, como atendimento a clientes, suporte em sinistros, comunicação com seguradoras e continuidade de obrigações relevantes, sejam retomadas em prazos compatíveis com sua criticidade e com os recursos disponíveis.

15. Temporalidade, Retenção e Descarte Seguro

A corretora adota critérios de temporalidade documental e retenção de informações, considerando exigências legais, regulatórias, contratuais, fiscais, securitárias, trabalhistas, contábeis, probatórias, operacionais e de exercício regular de direitos.

Informações e documentos devem ser mantidos pelo período necessário ao cumprimento de suas finalidades, à execução de contratos, ao atendimento de obrigações legais e regulatórias, à defesa de direitos e à preservação de interesses legítimos compatíveis com a legislação aplicável.

A Tabela de Temporalidade interna orienta prazos de guarda e critérios de eliminação de documentos físicos e digitais, incluindo, conforme o caso, propostas, apólices, endossos, comprovantes, documentos cadastrais, registros de atendimento, informações de sinistros, documentos financeiros, comunicações comerciais e documentos administrativos.

Atingido o prazo de retenção aplicável e inexistindo necessidade legítima de conservação, as informações devem ser descartadas de forma segura, proporcional ao suporte e à sensibilidade do conteúdo, buscando impedir recuperação, acesso indevido ou uso posterior incompatível.

A eliminação de documentos e dados deve observar procedimentos internos, responsabilidades definidas, registros quando aplicável e medidas compatíveis com o nível de risco da informação.

16. Uso Aceitável de Recursos e Ambiente de Trabalho

Os recursos tecnológicos, sistemas, e-mails, equipamentos, dispositivos, conexões, documentos e ambientes disponibilizados pela corretora devem ser utilizados de forma ética, profissional, segura e compatível com as atividades autorizadas.

É responsabilidade de cada colaborador, prestador ou terceiro autorizado proteger informações sob sua guarda, evitar exposição indevida, observar políticas internas, comunicar suspeitas de incidentes e utilizar recursos corporativos de acordo com as finalidades permitidas.

A corretora poderá estabelecer normas internas específicas sobre uso de e-mail, internet, dispositivos móveis, armazenamento em nuvem, senhas, autenticação, impressão, transporte de documentos, trabalho remoto, acesso a sistemas, instalação de softwares e uso de ferramentas de comunicação.

Por razões de segurança, conformidade e proteção de ativos, o uso de recursos corporativos poderá ser monitorado nos limites legais, contratuais e informados aos usuários, observados os princípios de necessidade, proporcionalidade, transparência e finalidade.

17. Segurança Física e Documental

A segurança da informação também abrange documentos físicos, ambientes de trabalho, arquivos, estações de atendimento, salas, armários, equipamentos, impressões, anotações, documentos de clientes e materiais recebidos de seguradoras, operadoras ou parceiros.

Documentos físicos contendo informações pessoais, confidenciais, comerciais ou estratégicas devem ser armazenados, manuseados, transportados, compartilhados e descartados com cuidado compatível com sua classificação e sensibilidade.

A corretora orienta seus colaboradores a evitar exposição desnecessária de documentos em mesas,

impressoras, áreas de circulação, salas de reunião, veículos, canais informais ou locais não autorizados.

As regras operacionais de guarda, arquivo, digitalização, circulação e descarte de documentos são definidas em procedimentos internos, observada a Tabela de Temporalidade e as exigências legais e contratuais aplicáveis.

18. Privacidade desde a Concepção e Minimização de Dados

A corretora busca incorporar segurança e privacidade desde a concepção de novos processos, produtos, fluxos, sistemas, parcerias e contratações que envolvam informações de clientes, colaboradores ou terceiros.

Sempre que possível, devem ser adotados critérios de minimização, limitação de acesso, redução de cópias, revisão de formulários, controle de compartilhamentos, descarte oportuno e coleta apenas dos dados necessários à finalidade legítima.

Mudanças relevantes em processos de tratamento de dados pessoais, tecnologias, fornecedores ou fluxos de compartilhamento devem ser avaliadas sob a perspectiva de riscos à segurança da informação e à privacidade dos titulares.

19. Responsabilidades

A Alta Direção é responsável por aprovar esta PPSI, demonstrar apoio institucional à segurança da informação e assegurar que a proteção das informações seja tratada como tema estratégico da corretora.

O Comitê de Gestão de Segurança da Informação - GSI, ou instância equivalente, é responsável por acompanhar a implementação das diretrizes, promover revisões, apoiar decisões de tratamento de riscos, avaliar incidentes relevantes e reportar temas críticos à Alta Direção.

Gestores são responsáveis por orientar suas equipes, zelar pelo cumprimento das políticas, solicitar acessos compatíveis com as funções, comunicar mudanças de pessoas ou processos e apoiar ações de conscientização e melhoria contínua.

Colaboradores, sócios, prestadores e terceiros autorizados são responsáveis por cumprir esta PPSI, observar políticas e procedimentos internos, proteger informações sob sua guarda, utilizar recursos adequadamente e comunicar suspeitas de incidentes ou fragilidades.

Fornecedores e parceiros que tratem informações da corretora, de seus clientes ou de terceiros devem observar obrigações contratuais, confidencialidade, segurança da informação, proteção de dados pessoais e cooperação em incidentes, conforme aplicável.

20. Revisão, Atualização e Publicidade

Esta PPSI será revisada, no mínimo, anualmente ou sempre que houver alteração relevante nos riscos, processos, tecnologias, serviços, fornecedores, estrutura organizacional, exigências legais, regulatórias, contratuais ou orientações de seguradoras, operadoras e parceiros regulados.

A versão pública desta política poderá ser disponibilizada em canais institucionais da corretora, como site, propostas, comunicações comerciais ou materiais de governança, conforme decisão da Alta Direção.

Atualizações relevantes poderão ser comunicadas aos públicos interessados por meio dos canais institucionais

apropriados. Versões internas, procedimentos operacionais e evidências de implementação permanecerão sob guarda da corretora e acesso restrito.

21. Canal Institucional

Dúvidas sobre esta PPSI, segurança da informação, proteção de dados ou exercício de direitos previstos na LGPD poderão ser encaminhadas ao canal oficial indicado pela corretora em seu site institucional ou em sua Política de Privacidade.

A Política de Privacidade complementará esta PPSI e apresentará informações específicas sobre finalidades de tratamento de dados pessoais, bases legais, direitos dos titulares, canais de atendimento, compartilhamentos e demais informações exigidas pela LGPD.

22. Disposições Finais

Esta PPSI reflete o compromisso público da UmmA Seguros com segurança, confiança, responsabilidade e proteção das informações que sustentam sua atividade no mercado de seguros.

A corretora reconhece que segurança da informação não é apenas requisito técnico ou regulatório, mas componente essencial da relação de confiança com clientes, seguradoras, operadoras, colaboradores e parceiros.

Nós atuamos com riscos todos os dias. Por isso, também os gerimos dentro de casa, com método, responsabilidade, proteção humana e compromisso institucional.

São Paulo, 25 de maio de 2026.

Anexo I - Referências Normativas e Boas Práticas

- Lei nº 13.709/2018 - Lei Geral de Proteção de Dados Pessoais - LGPD.
- Circular SUSEP nº 638/2021 - Dispõe sobre requisitos de segurança cibernética a serem observados pelas sociedades supervisionadas pela SUSEP e seus reflexos sobre prestadores e terceiros relevantes na cadeia do mercado segurador.
- Resolução CD/ANPD nº 15/2024 - Regulamento de Comunicação de Incidente de Segurança com Dados Pessoais.
- ISO/IEC 27001 - Sistema de Gestão de Segurança da Informação - requisitos.
- ISO/IEC 27002 - Controles de segurança da informação.
- ISO/IEC 27005:2022 - Diretrizes para gestão de riscos de segurança da informação.
- Lei nº 9.656/1998 e Lei nº 9.961/2000, quando aplicáveis a produtos e relações vinculadas à saúde suplementar, observadas as competências da ANS e as responsabilidades das operadoras reguladas.
- Contratos, orientações, exigências de segurança, requisitos de due diligence e políticas de parceiros regulados, seguradoras, operadoras e demais integrantes da cadeia de negócios, quando aplicáveis.

Anexo II - Quadro de Correspondência Temática

Tema da PPSI	Diretriz pública	Referência principal	Documento interno relacionado
Gestão de riscos	Identificar, avaliar, tratar, aceitar e monitorar riscos de segurança da informação.	ISO/IEC 27005:2022; ISO/IEC 27001	Matriz de Riscos; Plano de Tratamento de Riscos
Controles de segurança	Definir controles proporcionais ao risco, porte e criticidade dos processos.	ISO/IEC 27001; ISO/IEC 27002	PSI interna; normas técnicas; procedimentos operacionais
SUSEP e cadeia seguradora	Apoiar exigências contratuais e due diligence de seguradoras e parceiros regulados.	Circular SUSEP nº 638/2021; contratos de parceria	Gestão de Terceiros; Due Diligence de Fornecedores
ANS e saúde suplementar	Tratar dados de saúde e informações correlatas com confidencialidade e segurança reforçadas.	LGPD; normas setoriais aplicáveis; exigências contratuais	Política de Privacidade; Registro de Operações; Gestão de Consentimento quando aplicável
Segregação de acessos	Aplicar menor privilégio, necessidade de acesso e revisão periódica.	ISO/IEC 27001; LGPD art. 46	Política de Gestão de Acessos
Incidentes	Detectar, analisar, conter, tratar e comunicar incidentes quando aplicável.	LGPD; Resolução CD/ANPD nº 15/2024; ISO/IEC 27001	Plano de Resposta a Incidentes
Continuidade	Manter estratégias de continuidade e	ISO/IEC 27001; boas práticas de	Plano de Continuidade de Negócios

Tema da PPSI	Diretriz pública	Referência principal	Documento interno relacionado
	recuperação compatíveis com processos críticos.	continuidade	
Temporalidade	Reter dados pelo tempo necessário e descartar com segurança.	LGPD; obrigações legais, regulatórias e contratuais	Tabela de Temporalidade; Política de Retenção e Descarte
Conscientização	Capacitar colaboradores e reforçar cultura de segurança.	ISO/IEC 27001; boas práticas setoriais	Programa de Conscientização; Trilhas de Treinamento