

 Política de Segurança da Informação - PSI NÍVEL DE SIGILO: Público	CÓDIGO:	P.01
	SETOR:	TI
	PÁGINA:	Página 1 de 7
	REVISÃO:	01

1. Finalidade: estabelecer os princípios e as diretrizes gerais adotados pelo **ZOPONE** para a proteção de suas informações e ativos de informação, visando preservar sua confidencialidade, integridade, disponibilidade e, quando aplicável, autenticidade, em consonância com os riscos do negócio e com requisitos legais, regulatórios e contratuais aplicáveis.

2. Aplicabilidade: esta política aplica-se à **ZOPONE**, seus administradores, colaboradores, prestadores de serviços, fornecedores, parceiros e demais terceiros que, em razão de suas atividades, tenham acesso a informações, sistemas, ambientes ou outros ativos sob responsabilidade da **ZOPONE**, observadas as disposições contratuais e a aplicabilidade de cada diretriz.

3. Documentos Complementares: esta política estabelece diretrizes corporativas de alto nível. Regras técnicas, procedimentos operacionais, padrões, fluxos, critérios, parâmetros de configuração, matrizes de responsabilidade, evidências e demais controles específicos são disciplinados em documentos complementares, classificados conforme seu nível de sigilo e disponibilizados exclusivamente às pessoas que necessitem conhecê-los para o exercício de suas atribuições.

4. Definições:

- **Ativo de Informação:** qualquer informação, recurso, sistema, serviço, equipamento, ambiente ou elemento que possua valor para a organização e, por isso, necessite de proteção.
- **Autenticidade:** propriedade relacionada à comprovação de identidade, origem ou legitimidade de usuários, informações ou transações, quando aplicável.
- **Confidencialidade:** propriedade de que a informação não esteja disponível ou seja revelada a pessoas, entidades, processos ou sistemas não autorizados.
- **Integridade:** propriedade de preservação da exatidão, completude e consistência da informação, protegendo-a contra alterações indevidas ou não autorizadas.
- **Disponibilidade:** propriedade de assegurar que informações, sistemas e serviços estejam acessíveis às pessoas autorizadas quando necessários.
- **Dado Pessoal:** informação relacionada a pessoa natural identificada ou identificável, nos termos da Lei Geral de Proteção de Dados Pessoais - LGPD.

 Política de Segurança da Informação - PSI NÍVEL DE SIGILO: Público	CÓDIGO:	P.01
	SETOR:	TI
	PÁGINA:	Página 2 de 7
	REVISÃO:	01

- **Dado Pessoal Sensível:** dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.
- **Incidente de Segurança da Informação:** evento confirmado ou suspeito que comprometa ou possa comprometer a confidencialidade, integridade, disponibilidade ou autenticidade das informações ou dos ativos.
- **Risco de Segurança da Informação:** possibilidade de uma ameaça explorar vulnerabilidades e gerar impacto sobre informações, ativos, processos, pessoas ou negócios.
- **SGSI:** Sistema de Gestão da Segurança da Informação, compreendido como o conjunto de diretrizes, processos, responsabilidades e controles utilizados para gerir os riscos de Segurança da Informação.

5. Governança e Responsabilidades: a Segurança da Informação é responsabilidade compartilhada e deve ser incorporada aos processos de negócio, projetos, contratações, operações e decisões relevantes da ZOPONE.

- **Diretoria:** aprovar esta política, apoiar a governança de Segurança da Informação e assegurar, de forma compatível com os riscos e as necessidades do negócio, os recursos necessários à manutenção e à melhoria dos controles.
- **Tecnologia da Informação e Áreas Responsáveis por Segurança da Informação:** coordenar e apoiar a implementação das diretrizes, administrar os controles sob sua responsabilidade, acompanhar riscos e incidentes e propor melhorias.
- **Privacidade, Compliance, Jurídico, Recursos Humanos e demais Áreas de Apoio:** atuar, dentro de suas competências, na integração entre Segurança da Informação, proteção de dados pessoais, requisitos legais e contratuais, gestão de pessoas, terceiros e processos de governança.
- **Encarregado de Dados Pessoais:** prestar orientação e assistência nas matérias relacionadas à proteção de dados pessoais e atuar como canal de comunicação nos termos da legislação aplicável, sem assumir a responsabilidade técnica pelos controles de Segurança da Informação.

 Política de Segurança da Informação - PSI NÍVEL DE SIGILO: Público	CÓDIGO:	P.01
	SETOR:	TI
	PÁGINA:	Página 3 de 7
	REVISÃO:	01

- **Usuários e Terceiros Autorizados:** cumprir esta política e os documentos complementares aplicáveis, utilizar os ativos de forma responsável e comunicar prontamente situações suspeitas, vulnerabilidades ou incidentes.

6. Princípios e Diretrizes de Segurança da Informação: a ZOPONE adota abordagem baseada em riscos e busca promover melhoria contínua da Segurança da Informação, considerando a criticidade dos ativos, os impactos potenciais, os requisitos do negócio e as obrigações legais, regulatórias e contratuais.

6.1. Gestão de Riscos: os riscos de Segurança da Informação deverão ser identificados, analisados, avaliados, tratados e acompanhados de forma proporcional à criticidade dos ativos e processos. A metodologia, critérios, registros e planos de tratamento aplicáveis serão definidos em documentos internos.

6.2. Classificação e Tratamento da Informação: as informações deverão ser classificadas de acordo com sua sensibilidade, criticidade, requisitos legais, contratuais e de negócio. A ZOPONE adota, de forma geral, as classificações abaixo:

- **CONFIDENCIAL:** informação cuja divulgação, alteração, perda ou acesso não autorizado possa gerar impacto relevante jurídico, financeiro, operacional, estratégico, reputacional ou aos direitos de terceiros.
- **INTERNA:** informação destinada ao uso corporativo ou de pessoas autorizadas, cuja divulgação externa não autorizada possa gerar impacto operacional, administrativo ou de imagem.
- **PÚBLICA:** informação formalmente autorizada para divulgação ao público, observados os canais, finalidades e condições definidos pelo GRUPO ZOPONE e os direitos de terceiros.

Os controles aplicáveis a cada classificação, incluindo regras de acesso, armazenamento, transmissão, compartilhamento, retenção e descarte, serão definidos em normas e procedimentos internos.

6.3. Controle de Acesso e Autenticação: o acesso a informações, ambientes, sistemas e recursos tecnológicos deverá ser concedido de acordo com a necessidade de negócio, o princípio do menor privilégio e as responsabilidades de cada usuário. Mecanismos de autenticação e controle de acesso

 DESDE 1988 Política de Segurança da Informação - PSI NÍVEL DE SIGILO: Público	CÓDIGO:	P.01
	SETOR:	TI
	PÁGINA:	Página 4 de 7
	REVISÃO:	01

deverão ser compatíveis com o risco e a criticidade dos recursos protegidos. A concessão, revisão, alteração e revogação de acessos serão disciplinadas em procedimentos internos.

6.4. Proteção de Ativos e Uso Aceitável: os ativos corporativos deverão ser inventariados, protegidos, mantidos e utilizados de forma ética, segura e prioritariamente para finalidades profissionais, observadas as autorizações e regras internas aplicáveis. Não são admitidas alterações, instalações, conexões ou usos que comprometam a segurança, a legalidade ou a continuidade das atividades.

6.5. Monitoramento e Registros: a **ZOPONE** poderá registrar e monitorar o uso de seus ativos, sistemas, redes e serviços corporativos para finalidades legítimas de Segurança da Informação, prevenção e investigação de incidentes, proteção de ativos, continuidade dos negócios, auditoria e cumprimento de obrigações legais ou regulatórias, observados os princípios de necessidade, proporcionalidade, transparência e a legislação aplicável. Critérios técnicos, escopo, retenção e tratamento dos registros são definidos internamente.

6.6. Novas Tecnologias, Projetos e Mudanças: requisitos de Segurança da Informação e, quando aplicável, de privacidade e proteção de dados pessoais deverão ser considerados desde a concepção, aquisição, desenvolvimento, alteração e implantação de sistemas, produtos, serviços e projetos. Avaliações de risco, segurança, privacidade e impacto serão realizadas quando aplicáveis, conforme a natureza e a criticidade da iniciativa.

6.7. Terceiros e Cadeia de Fornecimento: a seleção, contratação e gestão de terceiros que tenham acesso a informações ou ativos relevantes deverão considerar requisitos de Segurança da Informação proporcionais aos riscos envolvidos. Contratos e instrumentos aplicáveis poderão estabelecer obrigações de confidencialidade, proteção de dados, controles de segurança, continuidade, subcontratação, comunicação de incidentes e demais responsabilidades pertinentes.

6.8. Continuidade, Resiliência e Cópias de Segurança: a **ZOPONE** mantém mecanismos de continuidade, recuperação e cópias de segurança compatíveis com a criticidade de seus processos, sistemas e

 Política de Segurança da Informação - PSI NÍVEL DE SIGILO: Público	CÓDIGO:	P.01
	SETOR:	TI
	PÁGINA:	Página 5 de 7
	REVISÃO:	01

informações, buscando reduzir os impactos decorrentes de indisponibilidades, falhas e incidentes. Estratégias, parâmetros, prioridades, responsabilidades e testes são definidos em documentos internos.

6.9. Gestão de Incidentes: a **ZOPONE** mantém processo estruturado para identificação, registro, classificação, análise, contenção, tratamento, recuperação e aprendizado decorrente de incidentes de Segurança da Informação. Pessoas abrangidas por esta Política devem comunicar prontamente situações suspeitas ou incidentes pelos canais definidos pela organização.

Quando houver envolvimento de dados pessoais, as áreas competentes deverão avaliar o incidente com assistência do Encarregado de Dados Pessoais e adotar as medidas previstas na LGPD, na regulamentação da Agência Nacional de Proteção de Dados - ANPD e nos procedimentos internos aplicáveis.

6.10. Privacidade e Proteção de Dados Pessoais: a proteção de dados pessoais integra as práticas de Segurança da Informação da **ZOPONE**. Medidas técnicas e administrativas apropriadas deverão ser adotadas ao longo do ciclo de vida do tratamento, considerando a natureza dos dados, as finalidades, os riscos aos titulares e os requisitos legais aplicáveis. As regras específicas de privacidade são complementadas pelo Programa de Privacidade e pelos documentos próprios da organização.

6.11. Conscientização e Capacitação: a **ZOPONE** promove ações periódicas de conscientização e capacitação em Segurança da Informação e proteção de dados, adequadas às responsabilidades e aos riscos associados às atividades desempenhadas.

6.12. Trabalho Remoto e Externo: o trabalho remoto ou externo deverá observar os mesmos princípios de Segurança da Informação aplicáveis ao ambiente corporativo, utilizando recursos e meios de acesso autorizados e adotando cuidados adicionais para proteção de credenciais, documentos, equipamentos e informações contra perda, exposição ou acesso indevido.

6.13. Segurança Física: o acesso físico a ambientes que abriguem ativos relevantes deverá ser controlado de acordo com sua criticidade e limitado a pessoas autorizadas. Medidas específicas de proteção

 Política de Segurança da Informação - PSI NÍVEL DE SIGILO: Público	CÓDIGO:	P.01
	SETOR:	TI
	PÁGINA:	Página 6 de 7
	REVISÃO:	01

ambiental, controle de visitantes, registro de acessos e movimentação de equipamentos são disciplinadas em procedimentos internos.

6.14. Retenção e Descarte Seguro: informações e mídias deverão ser mantidas somente pelo período necessário às finalidades autorizadas e aos requisitos legais, regulatórios, contratuais e de negócio. O descarte deverá utilizar métodos compatíveis com a natureza do suporte e a classificação da informação, de modo a reduzir o risco de recuperação ou acesso indevido.

7. Canais de Comunicação: dúvidas, suspeitas, vulnerabilidades ou violações relacionadas à Segurança da Informação deverão ser comunicadas pelos canais oficiais disponibilizados pela **ZOPONE**. Colaboradores e parceiros deverão utilizar também os canais definidos pela empresa. Questões específicas de privacidade e proteção de dados pessoais poderão ser direcionadas ao Canal de Privacidade disponibilizado no website.

7.1. Segue Rol de Canais:

- Incidente Informativo: incidentes.si@zopone.com.br
- Compliance: <https://zopone.com.br/compliance>
- Encarregado de Dados/Privacidade: <https://zopone.com.br/privacidade>

8. Violações: o descumprimento desta política poderá ser objeto de apuração e resultar nas medidas administrativas, disciplinares, contratuais ou legais aplicáveis, observados a legislação, os contratos e os normativos internos pertinentes.

9. Vigência e Revisão: esta política entra em vigor na data de sua aprovação e possui prazo de vigência indeterminado. Será revisada, no mínimo, anualmente e sempre que houver alteração relevante em riscos, processos, tecnologias, requisitos legais ou regulatórios, estrutura organizacional, modelo de negócio ou ocorrência de incidente significativo de Segurança da Informação.

 Política de Segurança da Informação - PSI NÍVEL DE SIGILO: Público	CÓDIGO:	P.01
	SETOR:	TI
	PÁGINA:	Página 7 de 7
	REVISÃO:	01

10. REFERÊNCIAS: as referências abaixo são utilizadas como fontes de orientação e boas práticas, sem que sua menção implique, por si só, declaração de certificação, conformidade integral ou auditoria independente da ZOPONE.

Código/Registro	Títulos/Referências
ABNT NBR ISO/IEC 27001:2022	Segurança da informação, segurança cibernética e proteção à privacidade - Sistemas de gestão da segurança da informação - Requisitos (Versão Corrigida:2023 e Emenda 1:2024).
ABNT NBR ISO/IEC 27002:2022	Segurança da informação, segurança cibernética e proteção à privacidade - Controles de segurança da informação.
ABNT NBR ISO/IEC 27005:2023	Segurança da informação, segurança cibernética e proteção à privacidade - Orientações para gestão de riscos de segurança da informação.
ABNT NBR ISO/IEC 27701:2026	Segurança da informação, segurança cibernética e proteção da privacidade - Sistemas de gestão da privacidade da informação - Requisitos e orientações.
Lei nº 13.709/2018	Lei Geral de Proteção de Dados Pessoais - LGPD.
Resolução CD/ANPD nº 15/2024	Regulamento de Comunicação de Incidente de Segurança.

11. Controle de Alteração (Natureza das Alterações):

- **criação:** em 30/01/2022;
- **Revisado:** em 12/08/2026 – adequação da PSI para publicação no website e segregação dos detalhes técnicos e operacionais em documentos internos classificados.