Política de Segurança da Informação - PSI

Maio 2026

1. OBJETIVO

Esta Política de Segurança da Informação (PSI) é a declaração formal da Akiyama quanto ao seu compromisso com a proteção das informações e dos dados pessoais de sua propriedade ou sob sua guarda, controle e operação.

Seu objetivo é estabelecer as diretrizes gerais que asseguram a disponibilidade, a integridade, a confidencialidade, a legalidade, a autenticidade e a auditabilidade da informação, orientando o modelo de governança, os processos de negócio, a capacitação das pessoas e o uso dos recursos - tecnológicos ou não - da organização.

2. ABRANGÊNCIA

Esta Política aplica-se às seguintes empresas:

- AKIYAMA S.A. - Indústria e Comércio de Equipamentos Eletrônicos e Sistemas S.A. (Openbio) - CNPJ 02.688.100/0001-88;
- NAX ADMINISTRAÇÃO DE BENS E PARTICIPAÇÕES LTDA - CNPJ 17.809.418/0001-47;
- NATOSAFE TECNOLOGIA DA INFORMAÇÃO S.A. (Infant.ID) - CNPJ 17.908.486/0001-63;
- NEOYAMA INDÚSTRIA E COMÉRCIO DE ELETROELETRÔNICOS LTDA - CNPJ 15.806.916/0001-00;
- ANTHEUS TECNOLOGIA LTDA - CNPJ 01.167.328/0001-60.

Sujeitam-se às suas diretrizes todos os usuários da informação da Akiyama: colaboradores, estagiários, prestadores de serviço, fornecedores, parceiros e demais pessoas previamente e expressamente autorizadas a acessar informações da organização, independentemente do vínculo, do local de trabalho ou do dispositivo utilizado.

3. COMPROMISSO DA ORGANIZAÇÃO

A Akiyama reconhece a informação como um ativo essencial ao seu negócio e à confiança de clientes, parceiros e titulares de dados pessoais. Nesse sentido, a organização assume os seguintes compromissos:

- proteger as informações e os dados pessoais sob sua responsabilidade contra acessos não autorizados, divulgação indevida, alteração, perda ou destruição;

- manter e aprimorar continuamente um Sistema de Gestão de Segurança da Informação e de Privacidade, estruturado conforme as normas ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27701 e submetido a auditorias internas e externas independentes;
- cumprir os requisitos legais, regulatórios e contratuais aplicáveis, com destaque para a Lei nº 13.709/2018 - Lei Geral de Proteção de Dados Pessoais (LGPD);
- tratar dados pessoais de forma lícita e transparente, limitada às finalidades informadas aos titulares e respeitando os direitos que a legislação lhes assegura;
- prover os recursos humanos, tecnológicos e financeiros necessários à manutenção e à melhoria da segurança da informação e da privacidade;
- assegurar a continuidade dos produtos e serviços prestados aos seus clientes.

4. PRINCÍPIOS E DIRETRIZES

As diretrizes a seguir orientam todas as decisões, normas e procedimentos de segurança da informação e de proteção de dados pessoais da Akiyama:

- **Comprometimento:** a proteção da informação é responsabilidade de todos e é difundida em todos os níveis da estrutura organizacional.
- **Prevenção:** projetos, produtos, serviços e mudanças são planejados considerando, desde a concepção, a proteção da informação e dos dados pessoais.
- **Responsabilização e prestação de contas:** a organização mantém-se apta a demonstrar, a qualquer tempo, o cumprimento das normas de proteção de dados pessoais e a eficácia dos controles adotados.
- **Gestão de riscos:** riscos e vulnerabilidades são identificados, analisados e tratados periódica e sistematicamente, de modo que medidas preventivas sejam adotadas antes da ocorrência de incidentes.
- **Responsabilidade compartilhada:** todo usuário autorizado responde pela proteção dos ativos de informação a que tem acesso, pelo sigilo de suas credenciais e pela comunicação imediata de incidentes e fragilidades.
- **Conscientização e capacitação:** programas regulares de treinamento e campanhas de conscientização preparam as pessoas para reconhecer e tratar ameaças, entre elas as tentativas de fraude e de engenharia social.

- **Controle de acesso:** o acesso às informações e aos ambientes é concedido segundo a necessidade de uso e o menor privilégio, por meio de credenciais pessoais e intransferíveis, e é revisado periodicamente. Todo acesso que não for expressamente autorizado é proibido.
- **Proteção dos ambientes e dos ativos:** são adotados controles de segurança física e lógica, proteção das redes e dos equipamentos, defesa contra códigos maliciosos, criptografia, cópias de segurança, gestão de vulnerabilidades e de atualizações, além do monitoramento dos ambientes.
- **Uso dos recursos:** os recursos de informação e de tecnologia destinam-se às atividades da organização e devem ser utilizados de forma responsável e em conformidade com a legislação e com as normas internas.
- **Gestão de terceiros:** fornecedores e prestadores de serviço são avaliados quanto aos riscos que representam e assumem, em contrato, obrigações de segurança da informação, de confidencialidade e de proteção de dados pessoais.
- **Gestão de incidentes:** há processo formal para registro, avaliação, tratamento e comunicação de incidentes de segurança da informação e de privacidade, incluindo as notificações exigidas pela legislação.
- **Continuidade:** a organização mantém medidas para preservar a disponibilidade das informações e a continuidade de suas operações diante de eventos disruptivos.
- **Melhoria contínua:** controles, normas e procedimentos são reavaliados periodicamente e ajustados sempre que necessário.

5. RESPONSABILIDADES

As responsabilidades relativas à segurança da informação e à privacidade estão assim distribuídas:

- **Alta Direção:** aprovar as políticas organizacionais, prover os recursos necessários ao Sistema de Gestão e engajar lideranças e colaboradores no cumprimento dos objetivos definidos.
- **Área de Segurança da Informação e Privacidade:** conduzir a avaliação e o tratamento dos riscos, revisar periodicamente os controles, planejar e coordenar as auditorias internas, promover as campanhas de

conscientização e conduzir, junto à liderança, as análises críticas do Sistema de Gestão.

- **Encarregado pelo Tratamento de Dados Pessoais (DPO):** atuar como canal de comunicação entre a organização, os titulares de dados pessoais e a Autoridade Nacional de Proteção de Dados (ANPD), orientando sobre as práticas de privacidade adotadas.
- **Gestores:** cumprir e fazer cumprir esta Política e as normas dela decorrentes, assegurar o pleno conhecimento das regras por suas equipes, garantir a inclusão de cláusulas de segurança da informação nos instrumentos firmados com terceiros e comunicar os riscos e as vulnerabilidades identificados.
- **Usuários:** cumprir esta Política e as normas e procedimentos aplicáveis, firmar termo de responsabilidade, zelar pelas informações sob sua guarda, utilizar os recursos exclusivamente para as finalidades autorizadas e comunicar de imediato qualquer incidente ou suspeita de violação.

6. ESTRUTURA NORMATIVA E DIVULGAÇÃO

Esta Política é o documento de mais alto nível da estrutura normativa de segurança da informação e privacidade da Akiyama, sendo complementada por normas, procedimentos e instruções de trabalho internos que detalham a sua aplicação.

Esta Política é mantida permanentemente disponível ao público no sítio eletrônico da Akiyama e é divulgada a todos os colaboradores e prestadores de serviço, que recebem as informações e a capacitação necessárias ao seu cumprimento.

7. COMUNICAÇÃO DE INCIDENTES E CANAL DE CONTATO

Clientes, fornecedores, parceiros, titulares de dados pessoais e demais interessados podem comunicar incidentes, fragilidades ou suspeitas de violação de segurança da informação e de privacidade, bem como esclarecer dúvidas sobre esta Política, pelo canal:

comite.seguranca@akiyama.com.br

As comunicações recebidas são registradas, avaliadas e tratadas conforme o processo interno de gestão de incidentes, observadas, quando aplicáveis, as obrigações de comunicação aos titulares e à ANPD previstas na LGPD.

8. CONFORMIDADE E CONSEQUÊNCIAS DO DESCUMPRIMENTO

O descumprimento desta Política, das normas e dos procedimentos de segurança da informação e de proteção de dados pessoais é considerado falta grave e sujeita o infrator às medidas disciplinares, contratuais, administrativas e legais cabíveis, sem prejuízo da suspensão imediata dos acessos concedidos enquanto durar a apuração dos fatos.

A violação de leis, regulamentos ou obrigações contratuais aplicáveis pode, ainda, acarretar responsabilização civil, administrativa e criminal, nos termos da legislação vigente.

9. VIGÊNCIA, REVISÃO E APROVAÇÃO

Esta Política entra em vigor na data de sua publicação e permanece vigente por prazo indeterminado, até que seja revisada, substituída ou formalmente revogada.

A revisão ocorre, no mínimo, anualmente, ou sempre que houver mudança significativa no contexto, na legislação ou nos riscos da organização. As políticas são revisadas pela liderança da área relacionada e têm como aprovador final o responsável jurídico do Grupo.

As diretrizes aqui estabelecidas não constituem rol exaustivo: diante da contínua evolução tecnológica e do surgimento de novas ameaças, a Akiyama adota, sempre que necessário, medidas adicionais de proteção das informações e dos dados pessoais sob sua responsabilidade.