Política de Segurança da Informação - PSI

Julho
2025

1. Objetivo

Este documento estabelece as diretrizes e as responsabilidades gerais para a proteção dos ativos de informação e dados pessoais sob controle e operação da Akiyama, que devem nortear seu modelo de governança, os processos de negócios implantados, as normas de segurança externas ou internas, capacitação dos usuários, características dos recursos utilizados - tecnológicos ou não, grau de Compliance atingido pela instituição e por terceiros prestadores de serviços que incluem tratamento de dados pessoais impactam diretamente no nível de segurança da informação na instituição.

2. Aplicação

A Política se aplica a todas as empresas abaixo expressas:

a. **AKIYAMA S.A. – INDÚSTRIA E COMÉRCIO DE EQUIPAMENTOS ELETRÔNICOS E SISTEMAS S.A (Openbio) –** CNPJ 02.688.100/0001-88;

b. **NAX ADMINISTRAÇÃO DE BENS E PARTICIPAÇÕES LTDA –** CNPJ 17.809.418/0001-47;

c. **NATOSAFE TECNOLOGIA DA INFORMACAO S/A (Infant.ID) –** CNPJ 17.908.486/0001- 63;

d. **NEOYAMA INDÚSTRIA E COMÉRCIO DE ELETROELETRÔNICOS LTDA –** CNPJ 15.806.916/0001-00;

e. **ANTHEUS-TECNOLOGIA LTDA –** CNPJ 01.167.328/0001-60

3. Corpo da política:

3.1 TERMOS E DEFINIÇÕES

●**Usuário:** pessoa que utiliza ou tem acesso a informações da Akiyama, inclusive terceirizados e outras pessoas prévia e expressamente autorizadas.

●**Colaborador:** empregado, estagiário ou voluntário que, formalmente vinculado à Akiyama, execute atividades no âmbito da instituição, de forma remunerada ou não;

- **Prestador de serviço:** pessoa física ou jurídica, vinculada a instituição mediante contrato formal ou tácito, que preste ou tenha prestado serviço à Akiyama;

- **Área de Segurança da Informação e Privacidade:** Setor interno responsável pelo acompanhamento e avaliação das políticas de segurança da informação e proteção de dados pessoais, a quem compete, ainda, sugerir normas e procedimentos que fortaleçam o controle da instituição.

- **Ativo de Informação:** Qualquer componente (seja humano, tecnológico, software ou etc) que sustenta um ou mais processos de negócio de uma unidade ou área de negócio.

- **TI:** Tecnologia da Informação

- **PSI:** Política de Segurança da Informação

- **Software:** Conjunto de instruções lógicas e codificadas que possibilitam o funcionamento de um sistema computacional. Os softwares podem incluir aplicativos, sistemas operacionais, utilitários e ferramentas, desempenhando um papel crucial na interação e no desempenho de hardware e usuários.

- **Firewall:** Medida de segurança em redes que monitora e controla o tráfego de dados com base em regras predefinidas. Funciona como uma barreira para proteger sistemas contra acessos não autorizados, malware e ataques cibernéticos, contribuindo para a segurança e integridade dos dados.

- **Malware:** Termo que se refere a software malicioso, como vírus, worms e trojans, criado para causar danos a computadores, redes ou usuários. Esses programas maliciosos podem infiltrar-se em sistemas, coletar informações confidenciais ou interromper operações normais.

- **Phishing:** Tipo de ataque online em que os criminosos tentam enganar os usuários, geralmente por e-mail ou mensagens, fazendo-se passar por entidades confiáveis.

- **Patches:** São atualizações de software que corrigem falhas, melhoram o desempenho ou abordam questões de segurança. São essenciais para manter a integridade dos sistemas, garantindo sua estabilidade e proteção.

- **Rack de Equipamentos:** Local físico onde são armazenados, gerenciados e processados os recursos de tecnologia da informação, incluindo servidores, sistemas de armazenamento, roteadores, switches de rede e outros componentes de infraestrutura de TI.

- **VPN:** Tecnologia que cria uma conexão segura e criptografada pela Internet, garantindo privacidade, segurança e acesso a recursos de rede.

3.2 INTRODUÇÃO

a) A Política de Segurança da Informação - PSI da Akiyama é uma declaração formal da organização acerca de seu compromisso com a proteção das informações de sua propriedade e/ou sob sua guarda, devendo ser cumprida por todos os seus colaboradores. Seu propósito é estabelecer as diretrizes a serem seguidas no que diz respeito à adoção de procedimentos e mecanismos relacionados à segurança da informação, e em garantir a disponibilidade, integridade, confidencialidade, legalidade, autenticidade e auditabilidade da informação, conforme indicativos nas metodologias ISO 27001 e na legislação da Lei 13709 - Lei Geral de Proteção de Dados Pessoais (LGPD).

b) É dever de todos considerar a informação como sendo um bem organizacional, um dos recursos críticos para a realização do negócio, que possui grande valor para a Akiyama e seus parceiros, e que deve sempre ser tratada profissionalmente para proteger a informação contra vários tipos de ameaças, garantir a continuidade dos serviços e produtos, maximizar o retorno sobre os investimentos e possibilitar a geração de novas oportunidades de negócio.

c) A violação desta política de segurança é qualquer ato que:

- Exponha a empresa a uma perda monetária efetiva ou potencial por meio do comprometimento da segurança dos dados ou de informações, ou ainda da perda de equipamento.

- Envolva a revelação de dados confidenciais, direitos autorais, negociações, patentes ou uso não autorizado de dados corporativos.

- Envolva o uso de dados para propósitos ilícitos, que venham a incluir a violação de qualquer lei, regulamento ou qualquer outro dispositivo governamental.

3.3 ESTRUTURA DAS NORMAS DA SEGURANÇA DA INFORMAÇÃO

a) A estrutura normativa da segurança da informação e proteção de dados pessoais da Akiyama é composta por um conjunto de documentos com níveis hierárquicos distintos, assim compreendidos:

b) Política de Segurança da Informação: representada por este documento, estabelece a estrutura e as diretrizes gerais concernentes à segurança da informação. É aprovada pela Diretoria da Akiyama e deve ser revisada anualmente;

c) Guias de Controles de Segurança da Informação (Normas): constituídas por definições táticas dos processos e orientações formais relacionadas a gestão de segurança da informação, exigem a aprovação por parte da Diretoria da Akiyama e revisão anual;

d) Procedimentos de Segurança da Informação: idealizados no âmbito das gerências e coordenações, cuidam de detalhar o exposto nas políticas e normas de segurança, devendo se apresentar de maneira objetiva, orientando, passo a passo, a atividade operacional. Sua implementação dependerá da aprovação da Diretoria da Akiyama.

3.4 DIVULGAÇÃO E ACESSO Á ESTRUTURA NORMATIVA

a) Esta Política Geral de Segurança da Informação, bem como toda e qualquer política complementar da informação implementada deverá permanecer disponível no sítio eletrônico da Akiyama - em local de fácil acesso ao público em geral - sendo seus conteúdos integralmente compartilhados em toda a rede interna da instituição, de maneira tal que qualquer cliente ou usuário interessado consiga acessar a informação com a máxima presteza possível.

b) Todos os colaboradores devem ser capacitados regularmente quanto às normas constantes na legislação nacional pertinente, nesta Política Geral e eventuais alterações posteriores, bem como em quaisquer outras informações necessárias para manutenção da eficácia na segurança da informação.

c) O objetivo da capacitação mencionada neste item é assegurar que cada colaborador possua o conhecimento atualizado da estrutura normativa, a fim de que possa executar suas tarefas de maneira segura e consciente.

d) Aos prestadores de serviços, devem ser fornecidas todas as informações necessárias para que eles tomem conhecimento do conjunto normativo aplicável à respectiva atuação.

3.5 DIRETRIZES GERAIS DE SEGURANÇA DA INFORMAÇÃO

a) As diretrizes a seguir listadas devem nortear todos os atos de gestão da

informação, incluindo toda e qualquer elaboração ou alteração de políticas, normas e procedimentos de segurança da informação e proteção de dados.

b) São diretrizes gerais de segurança da informação e proteção de dados pessoais na Akiyama:

- **Conscientização e Treinamento em Segurança:** Programas regulares de conscientização de segurança e sessões de treinamento são realizados para educar os funcionários sobre suas funções e responsabilidades na proteção de ativos de informações. O treinamento abrange tópicos como higiene de senha, engenharia social, conscientização sobre Phishing, Smishing e Vishing, e práticas recomendadas para uso seguro de tecnologia.

- **Responsabilidade compartilhada:** Todos os funcionários e indivíduos autorizados são responsáveis por proteger os ativos de informações em conformidade com esta política e procedimentos relacionados. Isso inclui proteger suas credenciais de login, relatar imediatamente quaisquer incidentes de segurança ou vulnerabilidades e usar os recursos com responsabilidade.

- **Comprometimento:** proteger os dados e as informações tratadas na instituição é fundamental para assegurar a continuidade de sua existência. Sendo assim, é necessário difundir, nos mais diversos níveis da estrutura hierárquica a necessidade e o desejo de colaborar com a implantação e manutenção de boas práticas;

- **Prevenção:** todo e qualquer projeto ou ação da Akiyama deve ser planejada levando em conta a necessidade de evitar vazamentos de dados pessoais e informações e assegurar a eficácia das estratégias de segurança da informação;

- **Responsabilização e prestação de contas:** é necessário manter-se capaz de demonstrar, a qualquer tempo, a observância e o cumprimento das normas de proteção de dados pessoais e a eficácia das medidas de controle adotadas;

- **Análise de riscos:** os riscos e vulnerabilidades institucionais devem ser analisados periodicamente e de forma sistemática, a fim de que medidas atenuantes possam ser tomadas antes que ocorram incidentes;

- **Inteligência de Ameaças:** a organização deve coletar, analisar e disseminar inteligência de ameaças a partir de fontes confiáveis, como feeds comerciais, OSINT e comunidades de segurança. As ameaças devem

ser classificadas conforme impacto e probabilidade, utilizando frameworks como MITRE ATT&CK.

c) As informações relevantes devem ser compartilhadas com as equipes de segurança e stakeholders, garantindo confidencialidade e conformidade. A inteligência deve ser integrada aos processos de resposta a incidentes, permitindo a aplicação de medidas preventivas e corretivas.

d) PI-058-00 - Inteligência de ameaças será revisada periodicamente para melhoria contínua, e todos os colaboradores devem estar cientes de suas responsabilidades na identificação e mitigação de riscos cibernéticos.

- **Resposta e relatórios de incidentes:** Implementado plano de resposta a incidentes de forma rápida e eficaz, do qual os funcionários devem relatar qualquer violação de segurança suspeita ou real, perda de dados confidenciais ou qualquer outro incidente de segurança ao departamento de TI ou equipe de segurança designada. Através de um procedimento claro para relatar, escalar e resolver incidentes sendo documentado e comunicado a todos os funcionários, a fim de minimizar seu impacto na organização.

- **Reavaliação:** todas as medidas adotadas devem ser, periodicamente, reavaliadas e ajustadas, sempre que necessário.

- **Uso Aceitável de Tecnologia:** Os funcionários devem usar os recursos de tecnologia da Akiyama com responsabilidade e em conformidade com as leis e regulamentos aplicáveis. Seguem as seguintes orientações: Atividades proibidas, como instalação não autorizada de software, acesso a sites inapropriados ou compartilhamento de informações confidenciais sem a devida autorização. O uso de recursos de tecnologia da empresa para fins pessoais é limitado de acordo com as políticas da organização. Os funcionários devem ter cuidado com tentativas de phishing por e-mail, links suspeitos e download de arquivos de fontes não confiáveis.

- **Proteção de Dados e Backup:** Medidas implementadas para proteger dados confidenciais de divulgação, modificação ou destruição não autorizada. Criptografia, prevenção contra perda de dados e backups regulares são empregados para garantir a integridade e a disponibilidade dos dados de acordo com o plano de execução de backup definido para o grupo.

- **Segurança de rede:** A infraestrutura de rede é protegida por firewalls, sistemas de detecção e prevenção de intrusão e avaliações regulares de vulnerabilidade. As configurações seguras e o gerenciamento de patches

são aplicados para reduzir o risco de acesso não autorizado e comprometimento do sistema.

- **Proteção contra malware:** Utilização de software antivírus atualizado e sistemas de detecção de malware, implementados para proteção contra ameaças de software malicioso. Verificação regular.

- **Senhas Rede / VPN:** Adotado como critério para criação de senhas a utilização de no mínimo 8 caracteres, letras maiúsculas e minúsculas, números ou caracteres especiais, e proibimos a inclusão nome, sobrenome ou a palavra "Akiyama". Além disso, não é permitido reutilizar as últimas senhas anteriores, as quais possuem um prazo para expiração de 4 meses. *Também implementamos um bloqueio do login após 3 tentativas indevidas.

- **Controle de acesso ao Rack de equipamentos:** O acesso ao Rack que está presente na empresa e é permitido somente para uma equipe pré-autorizada, composta pelo Gestor da Área de TI, pelo Analista de Infraestrutura (Pilgrims).

e) O acesso ao Rack localizado em Curitiba segue um processo de duas etapas. Primeiramente, se um colaborador ou terceiro não possui uma chave ou não possuir autorização, deverá solicitar o acesso ao Rack ao Gestor de TI, enviando um e-mail com nome completo, a empresa terceira se for o caso e o motivo.

f) Após essa solicitação, a segunda etapa consiste na validação realizada na entrada da empresa, que inclui a assinatura do Livro de Controle. Somente a equipe previamente autorizada, composta pelo Gestor da Área de TI, Analista de Infraestrutura, tem acesso a essa área. Qualquer pedido de novas autorizações deverá ser encaminhado ao Analista de Infraestrutura a responsável, juntamente com a aprovação do Gestor da Área de TI.

- **Redes sem fio (wireless) ou Wifi:** Adotado como critério a utilização de no mínimo 8 caracteres sendo eles letras, números e caracteres especiais. A senha padrão do Wi-Fi corporativo é fornecida exclusivamente aos colaboradores que utilizam notebooks. Para acessar, a senha deve ser autenticada através da rede, o acesso só será liberado seguindo alguns critérios como, estar com dispositivo ingressado no Domínio, e fazer parte do grupo que permite o acesso. O mesmo ocorre para as outras redes Wifi.

3.6 Comportamento íntegro e consistente

a) Não importando a forma com que se apresentam, informações estão presentes em cada decisão tomada e em cada atitude levada a cabo.

b) Assim, manter a informação segura no âmbito da instituição e fazer com que ela sirva, exclusivamente, aos propósitos pelas quais foram colhidas, representando um diferencial na qualidade dos serviços prestados, exige mais que a edição de normas e regulamentos de controle e a adoção de tecnologias de última geração em matéria de segurança.

c) Inicialmente, toda instituição é formada por pessoas e, para garantir a proteção das informações e dados pessoais sob controle e operação da Akiyama, faz-se necessário que os colaboradores e prestadores de serviço adotem comportamento íntegro e consistente com o objetivo de proteção das informações e dados pessoais na Akiyama com destaque para os seguintes itens:

- Colaboradores e prestadores de serviços devem assumir atitudes proativas em respeito à proteção dos dados pessoais e segurança da informação, buscando, dia a dia, a identificação de riscos e vulnerabilidades e a proposição de melhorias de controles e processos administrativos no tratamento destes dados;

- Os colaboradores devem ter sempre em mente que as operações da Akiyama estarão sempre sob ameaças externas à segurança dos dados, devendo permanecer alertas a quaisquer sinais de incidentes;

- Os colaboradores devem informar ao Comitê de Segurança da Informação e Proteção de Dados, formal ou informalmente, tão logo tomem conhecimento de qualquer falha de segurança ou vulnerabilidade na estrutura de informação da Akiyama;

- Todo acesso à informação e dados pessoais sob controle e operação da Akiyama que não for explicitamente autorizado está terminantemente proibido;

- A distribuição, divulgação, reprodução ou qualquer outra forma de compartilhamento de informação ou dado pessoal sob controle da Akiyama, ou mesmo de terceiros que a Akiyama seja, eventualmente, guardiã, confidencial ou não, está proibida, exceto quando houver autorização expressa do titular dos dados ou da gestão da Akiyama, nos termos da Lei Geral de Proteção de Dados;

- Arquivos confidenciais, documentos impressos e dados pessoais sob controle e operação da Akiyama devem ser adequadamente tratados, observando-se, com rigor, a legislação e as normas internas de proteção de dados;

- Computadores devem ser bloqueados com senha, impedindo a visualização de arquivos em uso, sempre que o usuário se afastar dos mesmos;

- Ao terminar o trabalho diário não deixar nenhum relatório e/ou mídia confidencial e/ou restrito sobre suas mesas (mesa e tela limpa);

- O uso de senhas de usuário é obrigatório, pessoal e intransferível para acesso às informações e ao ambiente computacional, ainda que estas venham a ser acessadas remotamente, em equipamentos particulares. Deve-se, ainda, evitar manter as senhas anotadas em papéis ou em outros sistemas visíveis e ao alcance de terceiros;

- É expressamente proibida a utilização de senhas ou identificação de outras pessoas;

- Cada vez que o usuário receber, da administração, uma nova senha de acesso a qualquer sistema da instituição, deverá alterá-la para outra de seu conhecimento exclusivo, se comprometendo, ainda, a substituí-la periodicamente ou na verificação de indícios de que ela tenha sido descoberta por outrem;

- É expressamente proibido desinstalar ou desativar recursos de proteção dos equipamentos da Akiyama;

- Nenhum software poderá ser instalado em equipamentos da Akiyama sem a expressa autorização da área de suporte;

- Não é permitida a utilização de softwares, aplicativos ou quaisquer outros documentos ou materiais sem o respectivo licenciamento ou autorização para uso

- Assuntos de trabalho devem ser evitados em eventos e ambientes públicos ou áreas expostas, de onde possam vir ao conhecimento de outras pessoas que não façam parte da instituição;

- Dúvidas sobre as Políticas e Normas de Segurança da Informação devem ser esclarecidas com o encarregado da área ou com algum membro do Comitê de Segurança da Informação e Privacidade da Akiyama. Caso prefira se comunicar via e-mail, devem enviar para o endereço comite.seguranca@akiyama.com.br.

3.7 Disposições normativas

a) A não conformidade com esta política pode resultar em ação disciplinar, incluindo rescisão do contrato de trabalho ou emprego. Violações de leis, regulamentos ou obrigações contratuais aplicáveis também podem levar a consequências legais.

b) Revisão e manutenção da política: Esta política será revisada anualmente ou conforme necessário para garantir sua relevância e eficácia contínuas, bem como a realização de auditorias internas e externas para verificar a conformidade com as políticas de segurança da informação. Quaisquer atualizações ou revisões serão comunicadas a todo o pessoal relevante.

3.8 Responsabilidades Gerais na Gestão da Segurança da Informação

a) Nesse documento, estão descritas as responsabilidades gerais no que tange à segurança da informação e dados pessoais sob controle e operação da Akiyama.

b) Para cada área ou atividade específica, estas responsabilidades serão elencadas nas respectivas políticas específicas ou normas criadas a partir das diretrizes apresentadas neste documento.

c) Cabe a cada colaborador e prestador de serviços da Akiyama:

- Manter-se constantemente atualizado em relação às normas de segurança da informação e proteção de dados pessoais publicadas pela Akiyama;

- Cumprir todas as políticas, normas e procedimentos de segurança da informação e proteção de dados pessoais da Akiyama;

- Solicitar ajuda ao superior hierárquico ou, em casos específicos, ao Comitê de Segurança da Informação e Privacidade ao Encarregado da Proteção de Dados (DPO), sempre que houver dúvidas quanto à segurança da informação e proteção de dados sob controle e operação da Akiyama;

- Assinar termo de responsabilidade, declarando ciência e aceitação das políticas, normas e procedimentos de segurança da informação e proteção de dados pessoais, e assumindo a responsabilidade pela realização de suas atribuições sempre em consonância com estas regras;

- Enviar todos os esforços no intuito de proteger as informações e dados pessoais, que estiverem sob sua guarda, contra tratamentos indevidos, alterações e supressão inadequadas, bem como acessos não autorizados;

- Garantir a estrita utilização dos recursos disponíveis, tecnológicos ou não, bem como das informações, para as finalidades decorrentes de suas atribuições funcionais, determinadas pela Akiyama;

- Observar com rigor a legislação pertinente à propriedade intelectual e à legislação de regência, no tocante à proteção de dados pessoais;

d) Cabe às Chefias, Gerências e Coordenações:

- Cumprir e fazer cumprir a política geral de segurança da informação, as políticas complementares (normas) e os procedimentos de segurança da informação e proteção de dados pessoais da Akiyama, bem como a legislação de regência pertinentes à segurança da informação e proteção de dados pessoais;

- Garantir às suas equipes o pleno conhecimento da política geral de segurança da informação, das políticas complementares (normas) e dos procedimentos de segurança da informação e proteção de dados da Akiyama, bem como o fácil acesso aos textos regulamentares do tema para eventuais consultas;

- Garantir a inclusão de cláusulas de segurança da informação nos instrumentos jurídicos firmados com outras instituições, bem como meios de garantir seu cumprimento ou a responsabilização em casos de incidentes;

- Propor a alteração ou criação de procedimentos de segurança da informação e proteção de dados pessoais, relacionados às suas respectivas áreas

- Manter os procedimentos referentes às suas áreas de atuação atualizados, dentro do cronograma de revisão periódica;

- Comunicar imediatamente ao Comitê de Segurança da Informação e Privacidade eventuais situações que possam representar risco e/ou vulnerabilidades relacionadas à segurança da informação e proteção de dados pessoais;

- Realizar constantemente o envio dos artefatos gerados em seu equipamento para os servidores de versionamento ou drives na nuvem para garantir proteção e backup.

e) Cabe a área de Segurança da Informação e Privacidade da Akiyama:
- Realizar o Planejamento de campanhas de conscientização e comunicação do Sistema de Gestão de Segurança da Informação;

- Conduzir avaliações e revisões de riscos de Segurança da Informação, estabelecendo as ações necessárias para tratamento dos riscos;
- Revisar periodicamente as medidas de segurança da informação;
- Planejar e coordenar auditorias internas do Sistema de Gestão de Segurança da Informação;
- Conduzir em conjunto com a Liderança as reuniões de Análise Crítica do SGSI.

f) Cabe à Liderança da Akiyama:
- Prover os recursos necessários para a manutenção e melhoria do Sistema de Gestão e da Segurança da Informação;
- Revisão e aprovação das Políticas Organizacionais;
- Engajar os demais líderes e colaboradores a respeito do cumprimento de processos e objetivos organizacionais.

3.9 Monitoramento e Controle

a) Todas as informações e dados controlados e operados pela Akiyama assim como seus arquivos físicos, equipamento diversos e todos os demais recursos estão destinados, exclusivamente, ao desenvolvimento de suas atividades, sendo vedado o uso para fins pessoais ou em favor de outras organizações, exceto quando pactuado com a direção da Akiyama.

b) A cada colaborador, independente do vínculo existente, deve ser dada ciência de que o tratamento desses dados pessoais ou uso das informações da Akiyama podem ser monitorados e que eventuais descumprimentos das políticas, normas e procedimentos de segurança serão detectados e utilizados para a instauração de procedimentos administrativos ou judiciais, dependendo do caso concreto, cabíveis.

c) No caso de procedimentos internos, as infrações serão submetidas ao rito administrativo vigente na Akiyama. Para as ações legais, serão observadas as normas de Direito aplicáveis à cada situação.

3.10 Respeito às políticas de segurança da informação e sanções

a) Além das penalidades aplicáveis aos atores que desrespeitarem as políticas, normas ou procedimentos de segurança da informação e proteção de dados, todo ato de infração será considerado grave e, tão

logo identificado, sem prejuízo do devido processo administrativo ou judicial, serão suspensas todas as autorizações para acesso aos equipamentos ou serviços de informática, bem como aos arquivos físicos de guarda dos dados, até que seja concluída a apuração dos fatos.

3.11 Casos Omissos

b) Os casos omissos serão avaliados pelo Comitê de Segurança da Informação e Privacidade para posterior deliberação. As diretrizes estabelecidas nesta política e nas demais normas e procedimentos de segurança, não se esgotam em razão da contínua evolução tecnológica e constante surgimento de novas ameaças. Desta forma, não se constitui rol enumerativo, sendo obrigação de todos os colaboradores da Akiyama adotar, sempre que possível, outras medidas de segurança além das aqui previstas, com o objetivo de garantir proteção as informações da Akiyama.

4. Vigência e Aprovação:

Esta política permanecerá vigente por prazo indeterminado, até que seja revisada, substituída ou revogada formalmente pela empresa.

Todas as políticas são revisadas pela liderança da área relacionada e o aprovador final é o responsável jurídico do Grupo.