PG.24.1 – Política de Segurança da Informação

Sistema de Gestão da Qualidade, Ambiente e Segurança

Edição 01
18 de janeiro de 2022

1. INTRODUÇÃO

A informação gerida pela SInASE, os seus processos de suporte, sistemas, aplicações e redes são ativos valiosos para a organização e, neste contexto, a segurança da informação deve ser uma prioridade, de forma a assegurar a continuidade da atividade da organização, minimizando os riscos e maximizando o desempenho e a prestação do serviço. A segurança da informação deverá ser aplicada em todas as fases do ciclo de vida da mesma, assegurando a manutenção, de forma permanente e equilibrada, de um nível de qualidade e segurança elevado, prevenindo a materialização de riscos inerentes, para mitigar os potenciais danos provocados pela exploração de vulnerabilidades e incidentes de segurança, e garantindo que o negócio opera conforme esperado ao longo do tempo.

2. OBJETIVO

Esta política pretende definir a finalidade e os princípios e regras fundamentais da gestão de segurança da informação, segundo as características e necessidades da sua atividade e das suas partes interessadas.

3. ÂMBITO/PÚBLICO ALVO

Aplicável a toda a organização incluindo todas as partes interessadas, entidades que mantenham qualquer tipo de relação comercial/contratual com a SInASE (colaboradores, clientes, fornecedores, prestadores de serviços) que tenham acesso, direito de uso ou controlo sobre ativos de informação titulados pela SInASE.

Todas as partes interessadas devem conhecer e agir em conformidade com esta Política e com os demais documentos relacionados com a Segurança da Informação, conforme aplicável e adequado.

4. INCUMPRIMENTO

Todas as partes interessadas abrangidas que, deliberadamente, violem esta política ficam sujeitas a sanções e outras ações, que podem ir até à cessação do contrato e/ou à participação às autoridades policiais ou judiciais das situações que indiciem a prática de crime.

5. POLÍTICA DE SEGURANÇA DE INFORMAÇÃO

A Política de Segurança da Informação expressa as considerações da SInASE no que respeita à segurança da informação sobre os seguintes aspetos:

1. **Aspetos elementares da Segurança da Informação** - A gestão da segurança da informação e dos sistemas que a suportam é realizada garantindo, através de uma abordagem baseada na gestão de risco e na melhoria contínua, a confidencialidade, a integridade e a disponibilidade da informação. Neste sentido a SInASE compromete-se a:
    - A garantir a segurança da informação, assim como de todos os recursos a ela associados, sejam eles processuais, tecnológicos ou humanos.

- Assegurar o estabelecimento e a prossecução dos princípios descritos nesta política, bem como a sua aprovação, publicação e comunicação a todos os colabores e entidades externas relevantes;

2. **Classificação e Manuseamento da Informação** - Definindo-se ativo de segurança de informação como qualquer recurso com valor para a organização, estes são classificados em função da sua sensibilidade relativamente aos seus atributos, designadamente a confidencialidade, integridade e disponibilidade, de modo a aplicar os controlos adequados para a sua salvaguarda.

3. **Utilização de dispositivos móveis e de acesso remoto-** São aplicadas medidas de segurança à utilização de dispositivos móveis para garantir a confidencialidade, integridade e a disponibilidade da informação de negócio para que possa ser acedida (de forma local ou remota) e/ou processada por estes dispositivos.

4. **Uso aceitáveis de ativos:**
   Os ativos de informação propriedade da SInASE são utilizados de forma a garantir a sua proteção, evitando a exposição dos mesmos a riscos de Segurança de Informação com potencial impacto de comprometerem a continuidade de negócio.

   A SInASE concede aos seus colaboradores e prestadores de serviços o direito de utilizar os seus próprios equipamentos, desde que sejam cumpridas as orientações internas.

5. **Relação com fornecedores e prestadores de serviços**
   Os fornecedores e prestadores de serviços são avaliados de forma a garantir relações contratuais com entidades que contribuem para a obtenção de acesso a matérias e serviços.

   Aquando da realização de acordos/ contratos de fornecimento/ prestação de serviços é entregue aos fornecedores/ prestadores serviços a Instrução de trabalho IT.29 – Requisitos de Qualidade, Segurança da Informação, SST e Ambiente, onde se encontram estabelecidos requisitos a ter em consideração aquando do fornecimento e/ou prestação de serviços.

6. **Controlos de acesso físico e lógico**
   Estão implementados controlos de acesso físico e lógico que permitem a gestão de identidades através de processos de identificação e autenticação do utilizador e que, por sua vez, permitem a implementação de regras de restrição baseadas em critérios de segurança.

7. **Mesa e ecrã limpo**
   A informação consideradas sensíveis, em formato físico ou digital, são devidamente protegidas sempre que não se encontram em uso.

8. **Cópias de Segurança**
   São efetuadas cópias de segurança, que ocorrem com uma periodicidade definida de forma a salvaguardar a informação.

   As mesmas são efetuadas pela equipa de TI.

9. **Transferência de Informação**
   A informação é trocada em canais de comunicação aprovados seguindo os requisitos de segurança definidos consoante a sua classificação de segurança.

10. **Segurança da Informação na Gestão de Projetos**
    A segurança da informação é endereçada na gestão de projetos através da identificação de possíveis riscos de segurança de informação associados ao projeto a implementar.

6. POLÍTICA DE PRIVACIDADE

A presente política da privacidade descreve o compromisso SInASE, com a proteção de dados pessoais e com a privacidade, nomeadamente a forma como são tratados os dados pessoais, como é garantida a respetiva segurança, para que tipos de entidades são transferidos e quais são os direitos dos titulares, bem como os contactos para efeitos de proteção de dados pessoais e de privacidade.

1. Enquadramento, âmbito de aplicação e princípios gerais

A SInASE é uma entidade consultora que atua na área da prestação de serviços de consultoria, formação e auditoria em sistemas de gestão, no âmbito de normas nacionais e internacionais de referência, em gestão de projetos cofinanciados (investimento, investigação e formação), em metodologias de gestão por objetivos, avaliação e melhoria do desempenho e em serviços de contabilidade e auditoria"

Para desenvolver a sua atividade empresarial a SInASE realiza geralmente operações de tratamento de dados pessoais de clientes ou potenciais clientes, de parceiros, de prestadores de serviços e de fornecedores. O tratamento de dados pessoais é suportado nos seguintes princípios:

- Transparência e comunicação – gerir a informação e os canais de comunicação com os titulares de dados pessoais, de forma acessível e simples.
- Legalidade, licitude e finalidade do tratamento – garantir o tratamento de dados pessoais de acordo com a legislação, com os regulamentos e com as normas em vigor e apenas para finalidades legítimas.
- Minimização, exatidão e conservação – tratar os dados pessoais necessários, exatos e atualizados, por quem necessita de intervir no processo; conservar e preservar os dados pessoais com base numa finalidade concreta.
- Segurança, confidencialidade e sigilo – consciencializar e formar os colaboradores para a adequada gestão dos dados pessoais, da segurança da informação, do dever de confidencialidade e de sigilo, quer em relação aos dados pessoais, quer à informação da atividade das empresas do grupo.

2. Conceitos

Dados pessoais, de acordo com regulamento geral de proteção de dados, em vigor, é a informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular.

3. Responsável pelo tratamento dos dados pessoais

A SInASE é a entidade responsável pelo tratamento dos dados pessoais, decidindo sobre os tipos e as categorias de dados pessoais e sobre qual o tratamento e as finalidades para que são utilizados, assim como sobre as transferências de dados pessoais para entidades terceiras, subcontratadas.

Estas, em seu nome, de acordo com a legislação / regulamentos em vigor, com a presente política da privacidade e com as regras e acordos específicos estabelecidos com esses terceiros, procederão ao respetivo ao tratamento de dados pessoais.

Podem ser transferidos dados pessoais para prestadores dos seguintes tipos de serviços: gestão de sistemas de informação, processamento, pagamentos e faturação eletrónica, consultores, consultoria, auditoria, formação, atividade bancária, seguros, e parceiros de negócio, serviços jurídicos, entre outros, à medida, que se possam revelar necessários para a atividade e desenvolvimento do negócio da empresa.

4. Que dados pessoais são tratados

De uma forma geral, a SInASE recolhe e trata dados pessoais para celebrar contratos relacionados com a prestação dos serviços, no âmbito da prestação de serviços e de acordo com o objeto de contrato, cumprir com obrigações legais e com requisitos de segurança, gerir serviços, fornecer informações e conteúdos em suportes físicos e digitais, acessos registados, contactos telefónicos, gerir o relacionamento com o cliente e as respetivas preferências, a experiência de cliente e gerir as ocorrências especificas durante a prestação de serviços, preservar o interesse vital do titular dos dados pessoais ou para garantia do interesse publico.

Os dados pessoais podem ser fornecidos pelo próprio titular, por telefone, presencialmente ou por meios digitais, ou recolhidos indiretamente através de entidades e autoridades oficiais, parceiros de negócio ou entidades com as quais a SInASE mantém contratos de prestação de serviços.

No âmbito da resposta às diferentes finalidades, podem ser tratadas as seguintes categorias de dados pessoais:

- identificação geral e contactos – nome, género, morada, endereço de correio eletrónico, contacto telefónico, numero de identificação civil e fiscal, informação familiar quando necessária;
- identificação e enquadramento profissional – função e dados curriculares, administrativos, fiscais, parafiscais, rendimentos, tipo de vínculo;

- dados pessoais relacionados com preferências, experiência de utilização, informação para faturação e para pagamento, bem como requisitos específicos do cliente, recolhidos e relacionados com o objeto de contrato e que sejam essenciais à prestação dos serviços contratualizados;
- dados pessoais constantes nos compromissos de confidencialidade e de sigilo profissional, nos acordos com fornecedores, parceiros e com subcontratantes, bem como dados de acesso e de utilização dos sistemas de informação da SInASE;
- podem ainda ser tratados dados relacionados com a avaliação da satisfação com os serviços prestados pela SInASE.

5. Finalidade, fundamento de licitude e prazo de conservação aplicáveis ao tratamento de dados pessoais

i. Finalidade: Execução dos contratos de trabalho, de estágio e gestão da relação de trabalho ou de estágio, com os colaboradores e estagiários

- Fundamento de licitude: Execução do Contrato; Cumprimento de obrigação legal.

Prazo de conservação: 12 anos após termino da relação contratual; posteriormente, arquivo histórico e interesse legítimo.

ii. Finalidade: Gestão de processos de recrutamento e de candidaturas espontâneas
- Fundamento de licitude: Diligências pré-contratuais.

Prazo de conservação: 2 anos; posteriormente, interesse legítimo ou oposição ao tratamento.

iii. Finalidade: Gestão comercial e Gestão do relacionamento com clientes, com fornecedores e com parceiros (exemplos: faturação, atividades e serviços prestados pela SInASE, compras, logística, ...)

- Fundamento de licitude: Diligências pré-contratuais ou Execução de Contrato;

Cumprimento de obrigação legal; Consentimento quando aplicável.

Prazo de conservação: 12 anos após termino da relação contratual; posteriormente, interesse legítimo, processo judicial, retirada de consentimento ou oposição ao tratamento.

iv. Finalidade: Gestão da relação com prestadores de serviços

- Fundamento de licitude: Diligências pré-contratuais ou Execução do Contrato;

Cumprimento de obrigação legal.

Prazo de conservação: 12 anos após termino da relação contratual; posteriormente, interesse legítimo, processo judicial.

v. Finalidade: Marketing, publicidade, organização de eventos, experiência de utilização
- Fundamento de licitude: Contrato; Interesse legítimo; consentimento quando aplicável.

Prazo de conservação: termino do contrato ou do interesse legítimo; retirada de consentimento.

vi. Finalidade: Avaliação da satisfação pelos clientes ou por outras partes interessadas; segurança da informação e auditoria;
- Fundamento de licitude: Interesse legítimo;

Prazo de conservação: termino do interesse legítimo; oposição ao tratamento; no caso da videovigilância, prazo legal.

6. Como e com que medidas são tratados os dados pessoais

O tratamento dos dados pessoais é realizado através de processos automáticos e manuais, com a adoção das medidas e dos controlos, tecnológicos e organizacionais, adequados e considerados proporcionais, para os proteger e preservar. Estas medidas incluem a gestão de autenticação e de acessos aos sistemas e às instalações, a monitorização da infraestrutura tecnológica, com o controlo de acessos, da utilização indevida e do tráfego anormal, a gestão de incidentes através de suporte técnico aos sistemas, o armazenamento de dados com regras de segurança especificas, a gestão de perfis de utilização dos sistemas, o acesso controlado à informação com caráter restrito, em qualquer suporte, a celebração de compromissos de confidencialidade e de sigilo profissional com todo o pessoal, bem como com estagiários, e a respetiva formação e consciencialização. Poderão, na medida das necessidades e requisitos específicos da gestão da informação, ser utilizadas técnicas mais robustas que visem a anonimização da informação ou a sua proteção acrescida, como a encriptação ou cifragem.

No âmbito do arquivo histórico e para fins estatísticos, os dados pessoais serão, sempre que possível, anonimizados, e podem ser preservados por períodos mais longos, bem como utilizados para as finalidades principais ou novas finalidades, se compatíveis.

Os dados pessoais podem ser transferidos, para as mesmas finalidades, para as entidades a que a Lei obriga ou para terceiros. A SInASE poderá ainda transferir dados para terceiros no âmbito de investigações, inquéritos e processos judiciais e/ou administrativos ou de natureza semelhante, desde que para tal seja devidamente ordenado por ordem judicial. Dada a natureza da SInASE, e para a execução dos contratos com os clientes, podem ser transferidos dados para parceiros ou para fornecedores, bem como para entidades públicas ou privadas, tendo em vista a preservação dos interesses vitais dos clientes ou dos colaboradores. No caso da partilha e do tratamento dos dados pessoais necessitar de transferências para terceiros fora do Espaço Económico Europeu, a SInASE compromete-se a atuar conforme estipulado pela legislação em vigor e pelo regulamento geral de proteção de dados, no âmbito aplicável às transferências de dados pessoais.

7. Direitos dos titulares dos dados pessoais

Será assegurada a resposta aos pedidos de acesso e informação, obtenção e consulta dos dados pessoais, atualização ou alteração, podendo ser solicitada a eliminação, a restrição e oposição ao tratamento e a cessação do tratamento automático dos dados pessoais para gestão de perfis, no caso de pedidos em conformidade com a legislação em vigor. Nos casos em que tenha sido dado consentimento, o mesmo poderá ser retirado, utilizando o contacto: qualidade.sinase@gmail.com

Poderá ainda contactar a autoridade nacional de controlo para a proteção de dados pessoais, caso entenda necessário e pertinente.

8. Alterações à política de privacidade

A SInASE reserva-se o direito de reajustar ou alterar a presente Política da Privacidade, sendo as mesmas publicadas no site da empresa.

7. RESPONSABILIDADES DA SEGURANÇA DA INFORMAÇÃO

A Política de Segurança da Informação é da responsabilidade da Administração em colaboração com a Direção Geral e equipa de qualidade, ambiente e segurança.

A Política de Segurança da Informação deve ser periodicamente revista, de forma a garantir que continua a ser adequada à SInASE e deve ser comunicada a todas as partes interessadas no âmbito da sua relação com a SInASE.

8. FALE CONNOSCO

Poderá contactar a SInASE para todos os assuntos relacionados com esta política através do seguinte endereço de email: qualidade.sinase@gmail.com ou enviar o seu pedido por carta para a morada Rua da Estrela n.º21 – 1200-668 Lisboa.