Política de Segurança da Informação

SILVIP, Sociedade Gestora de Organismos de Investimento Coletivo, S.A. (SILVIP)

Versão pública da Política de Segurança da Informação da SILVIP, que apresenta os principais compromissos e princípios adotados pela Sociedade em matéria de proteção da informação e de segurança dos sistemas e serviços tecnológicos. A versão integral da Política constitui um documento de uso interno.

1. Compromisso

A proteção da informação é essencial para a atividade da SILVIP e para a confiança dos seus participantes, clientes, parceiros, fornecedores e demais entidades com as quais se relaciona.

Neste contexto, a SILVIP adotou uma Política de Segurança da Informação, que estabelece os princípios e as orientações aplicáveis à proteção da informação sob a sua responsabilidade e dos sistemas e serviços tecnológicos que suportam a sua atividade.

Através desta Política, a SILVIP compromete-se a adotar medidas de segurança adequadas à natureza da informação e aos riscos associados, tendo em consideração os requisitos legais, regulamentares e contratuais aplicáveis, incluindo os relativos à resiliência operacional digital do setor financeiro.

2. A quem se aplica

A Política vincula todos os departamentos e colaboradores da SILVIP. Aplica-se igualmente aos parceiros e fornecedores que utilizem, administrem ou mantenham sistemas e serviços de tecnologias de informação e comunicação da Sociedade Gestora, ou que acedam a informação e a dados da organização, tanto em ambiente digital como em suporte físico.

A Política de Segurança da Informação orienta a atuação dos colaboradores da SILVIP e, sempre que aplicável, dos parceiros, fornecedores e prestadores de serviços que utilizem os seus sistemas ou tenham acesso a informação sob a sua responsabilidade.

A SILVIP procura assegurar que todas as entidades que intervêm no tratamento da sua informação adotam práticas de segurança adequadas e respeitam os requisitos aplicáveis.

3. Objetivos de segurança

A SILVIP protege a informação de acordo com quatro objetivos fundamentais:

- Disponibilidade: assegurar que a informação e os serviços indispensáveis à atividade permanecem acessíveis quando necessários;
- Confidencialidade: impedir o acesso ou a divulgação da informação por pessoas não autorizadas;
- Integridade: proteger a informação contra alterações indevidas e assegurar que permanece fidedigna e integral; e
- Autenticidade: permitir confirmar a origem da informação e a identidade de quem acede aos sistemas.

Estes objetivos orientam as medidas de segurança adotadas pela SILVIP e são considerados na gestão dos seus sistemas, processos e relações com terceiros.

4. Princípios

A atuação da SILVIP em matéria de segurança da informação baseia-se nos seguintes princípios:

- cumprimento dos requisitos legais, regulamentares e contratuais aplicáveis;
- proteção da informação de acordo com a sua importância e sensibilidade;
- consideração dos riscos de segurança na definição de processos, projetos e relações com terceiros;
- prevenção, deteção e tratamento adequado de incidentes;
- preparação para assegurar a continuidade e a recuperação dos serviços;
- acompanhamento regular da eficácia das medidas de segurança;
- melhoria contínua das práticas adotadas;
- formação e sensibilização dos colaboradores; e
- responsabilidade individual na utilização e proteção da informação a que tenha acesso.

A SILVIP adapta as suas medidas de segurança à evolução dos riscos, das tecnologias e dos requisitos aplicáveis à sua atividade.

5. Classificação da informação

A SILVIP classifica a informação de acordo com a sua sensibilidade e com o impacto que pode resultar da sua divulgação, alteração, perda ou utilização indevida.

Esta classificação permite aplicar medidas de proteção proporcionais ao risco, nomeadamente ao nível do acesso, armazenamento, partilha, conservação e eliminação da informação.

A informação pode ser classificada como:

- Pública: pode ser divulgada sem restrições, como a informação disponibilizada no sítio da SILVIP;
- Uso interno: destina-se aos colaboradores e a terceiros expressamente autorizadas;
- Confidencial: contém elementos sensíveis e está sujeita a medidas reforçadas de proteção e de controlo de acesso.

A SILVIP revê a classificação da informação sempre que a sua natureza, utilização ou grau de sensibilidade se alterem.

6. Medidas de segurança

A SILVIP adota medidas organizativas e tecnológicas destinadas a prevenir, detetar e responder a situações que possam afetar a segurança da informação ou o funcionamento dos seus sistemas.

Estas medidas incluem, designadamente:

- controlo do acesso à informação e aos sistemas;
- proteção dos equipamentos, sistemas e identidades digitais;
- acompanhamento de eventos relevantes de segurança;
- identificação e correção de vulnerabilidades;
- realização de cópias de segurança e testes de recuperação;
- gestão controlada das alterações aos sistemas;
- avaliação dos riscos associados a novos sistemas e serviços;
- adoção de medidas de continuidade e recuperação; e
- revisão periódica da eficácia dos controlos implementados.

As medidas adotadas são ajustadas à natureza da informação, aos sistemas utilizados e aos riscos identificados.

7. Fornecedores e prestadores de serviços de TIC

A SILVIP avalia os riscos associados à contratação de fornecedores e prestadores de serviços tecnológicos que possam ter acesso à sua informação ou suportar sistemas relevantes para a sua atividade.

Os requisitos de segurança aplicáveis são considerados na seleção, contratação e acompanhamento desses prestadores, tendo em conta a natureza dos serviços fornecidos e o respetivo nível de risco.

A SILVIP acompanha os serviços prestados e procura assegurar que os fornecedores adotam medidas adequadas de proteção da informação, comunicação de incidentes, continuidade e cumprimento das obrigações aplicáveis.

8. Gestão de incidentes

A SILVIP dispõe de mecanismos para identificar, analisar e tratar situações que possam comprometer a segurança da informação ou o funcionamento dos seus sistemas e serviços.

Sempre que ocorre um incidente, são adotadas medidas destinadas a:

- limitar os seus efeitos;
- proteger a informação e os sistemas afetados;
- recuperar o funcionamento dos serviços;
- apurar as respetivas causas;
- prevenir a repetição de situações semelhantes; e
- efetuar as comunicações legalmente exigidas.

Quando aplicável, a SILVIP comunica os incidentes às autoridades competentes e às pessoas ou entidades afetadas, nos termos legalmente previstos.

9. Formação e cultura de segurança

A segurança da informação depende não apenas das tecnologias utilizadas, mas também da atuação dos colaboradores.

A SILVIP promove ações de formação e sensibilização adequadas às funções desempenhadas pelos seus colaboradores, com o objetivo de reforçar:

- a utilização responsável da informação e dos sistemas;
- o reconhecimento de riscos e situações anómalas;
- a prevenção de incidentes;
- o conhecimento das regras e responsabilidades aplicáveis; e
- a adoção de comportamentos seguros no exercício da atividade.

A formação e a sensibilização são atualizadas em função da evolução dos riscos, dos sistemas utilizados e dos requisitos aplicáveis.

10. Governação e revisão

O Conselho de Administração da SILVIP aprova a Política de Segurança da Informação e assegura a existência dos recursos necessários à sua aplicação.

A Política é acompanhada pelas funções internas competentes em matéria de sistemas de informação, gestão de riscos, risco operacional e conformidade.

A SILVIP revê periodicamente a Política e adapta-a sempre que ocorram alterações relevantes nos riscos, na organização, nos sistemas utilizados ou nos requisitos legais e regulamentares aplicáveis.

11. Comunicação de vulnerabilidades e incidentes

Qualquer pessoa que identifique uma possível vulnerabilidade, ocorrência ou comportamento anómalo relacionado com os sistemas ou serviços da SILVIP pode comunicá-lo através do endereço: incidente@silvip.pt

A comunicação deve incluir, sempre que possível:

- uma descrição clara da situação observada;
- a data e a hora da ocorrência;
- o sistema ou serviço aparentemente afetado; e
- informação que permita compreender ou reproduzir a situação.

Não devem ser incluídos dados pessoais de terceiros, credenciais de acesso, informação confidencial ou elementos obtidos através de acesso não autorizado.

A SILVIP analisa as comunicações recebidas e trata a informação disponibilizada com adequada confidencialidade.

Versão pública n.º 2.0 | Aprovada em 29 de outubro de 2026.