Instituto Nacional de Estatística
Statistics Portugal

1935-2025

Política de Segurança da Informação

2025

2025

Política deSegurança de informação, última atualização: 2025/01/28

Política de Segurança da Informação do Instituto Nacional de Estatística, I.P.

Introdução

A Política de Segurança da Informação do INE, I.P. define os princípios gerais que orientam a proteção e a gestão dos ativos sob a responsabilidade do INE, I.P., no âmbito da sua Gestão de Segurança da Informação (GSI). Esta política integra-se no Sistema de Gestão Integrado (SGI), alinhado com as seguintes normas e requisitos:

// ISO/IEC 27001:2022 – Segurança da Informação, Cibersegurança e Proteção da Privacidade: Sistemas de Gestão da Segurança da Informação (Requisitos).

// ISO/IEC 27701:2019 – Extensão para Gestão de Informação Privada (Privacy Information Management).

// ISO 9001:2015 – Sistemas de Gestão da Qualidade (Requisitos).

// Legislação e regulamentação aplicáveis em matéria de segurança da informação, cibersegurança e proteção de dados.

// Recomendações do SEE (Sistema Estatístico Europeu) e do EUROSTAT relativas à Segurança da Informação, Cibersegurança e Proteção da Privacidade.

Ao integrar os princípios de qualidade e segurança, o INE, I.P. assegura uma abordagem sistemática e eficaz para garantir a confidencialidade, integridade, disponibilidade e qualidade dos dados e sistemas sob a sua gestão. O Conselho Diretivo do INE, I.P., ao estabelecer o Sistema de Gestão Integrado (SGI) e a Gestão de Segurança da Informação (GSI), assume os compromissos definidos na presente política. Este compromisso inclui a integração dos requisitos da GSI nos processos organizacionais e a garantia de que os recursos necessários para a sua implementação estão devidamente assegurados. Além disso, o Conselho Diretivo reconhece a sua responsabilidade perante as partes interessadas[1], comprometendo-se a:

//Adotar uma gestão adequada no âmbito da Segurança da Informação, Cibersegurança e Proteção da Privacidade;

//Monitorizar e avaliar continuamente a implementação da GSI, como parte integrante do SGI do INE, I.P.

Esta política está alinhada com os seguintes documentos estratégicos e normativos:

// Carta da Qualidade do INE, I.P.;

// Linhas Gerais da Atividade Estatística Oficial;

// Código de Conduta para as Estatísticas Europeias (princípios 2, 5 e 9);

// Outros documentos relacionados.

No contexto do GSI do INE, a gestão da Segurança da Informação, Cibersegurança e Proteção da Privacidade inclui, igualmente, a gestão de informação privada, em conformidade com os requisitos da norma ISO/IEC 27701:2019 (Gestão de Informação Privada).

O INE compromete-se a:

// Cumprir os requisitos normativos e legais: Garantir o cumprimento das normas nacionais, europeias (especialmente no âmbito do Sistema Estatístico Europeu – SEE) e internacionais aplicáveis à segurança da informação;

//Proteger a informação: Assegurar a confidencialidade, integridade e disponibilidade dainformação em todos os processos organizacionais;

//Promover a comunicação efetiva: Estabelecer e manter uma comunicação clara e eficiente das políticas e procedimentos de segurança da informação, assegurando que todas as partes interessadas compreendem as suas responsabilidades;

//Sensibilizar e formar continuamente: Implementar um programa contínuo de formação e sensibilização para reforçar a cultura de segurança da informação entre os colaboradores e demais partes interessadas;

//Evidenciar segurança organizacional: Demonstrar, de forma consistente, que o INE, I.P. éuma organização confiável e segura no âmbito da segurança da informação, adotando boas práticas e padrões reconhecidos internacionalmente.

Âmbito

A Política de Segurança da Informação do INE, I.P. aplica-se a todas as partes interessadas, incluindo colaboradores, fornecedores, parceiros e outras entidades que interajam com os ativos de informação da organização.

É responsabilidade de todas as partes interessadas:

// Conhecer e cumprir esta Política, bem como os documentos relacionados com a Segurança da Informação, de acordo com a sua aplicabilidade e contexto;

// Adotar comportamentos conformes às boas práticas e normas estabelecidas, contribuindo para a proteção da informação e a mitigação de riscos.

Qualquer violação deliberada desta Política ou de outros documentos associados sujeita os infratores a medidas disciplinares ou contratuais, podendo incluir:

// Cessação do contrato;

// Participação às autoridades policiais ou judiciais, em casos de indícios de prática de crime.

Este compromisso reforça a cultura de segurança da informação no INE, I.P., promovendo um ambiente seguro e alinhado com os requisitos legais e normativos..

Valor da informação

A informação é um ativo essencial para o INE, I.P., assumindo diversas formas, como documentos físicos, registos eletrónicos ou comunicações transmitidas por meios digitais. Independentemente do suporte, uso ou formato, é imprescindível garantir a proteção adequada da informação com base na sua relevância e valor.

A disponibilidade da informação e das infraestruturas tecnológicas que a suportam é vital para o funcionamento eficiente do INE, I.P., sendo a segurança no tratamento e transmissão de dados fundamental para o processo de produção das estatísticas oficiais.

Incidentes como interrupções de serviço, fugas de informação ou modificações não autorizadas podem comprometer a confiança dos cidadãos e empresas e violar obrigações legais e contratuais. Por isso, é responsabilidade de todas as partes interessadas colaborar ativamente na proteção da informação.

Adicionalmente, o EUROSTAT depende do funcionamento correto e esperado dos sistemas de informação e comunicação das Autoridades Estatísticas dos Estados-Membros. Essa colaboração só é possível com a identificação contínua de riscos associados aos ativos geridos pelo INE, I.P., e a implementação de controlos eficazes para assegurar a sua utilização segura e controlada.

Importância da Segurança da Informação

Os dados geridos pelo INE, I.P., juntamente com os processos, sistemas, aplicações e redes que os suportam, são ativos fundamentais para a sociedade. A proteção da confidencialidade,integridade e disponibilidade da informação é essencial para preservar a credibilidade e a confiança nos serviços prestados pela instituição.

A segurança da informação deve ser garantida em todas as etapas do ciclo de vida dos dados, desde a inserção/recolha até ao processamento, armazenamento, transmissão, pesquisa e eventual destruição. O controlo da segurança nessas operações é tão crítico quanto a funcionalidade dos sistemas que as suportam.

Para mitigar os riscos associados, o INE, I.P. compromete-se a manter um nível elevado e equilibrado de qualidade e segurança, prevenindo vulnerabilidades e incidentes que possam comprometer a organização.

Como as ameaças à segurança da informação evoluem continuamente, é necessário adaptar de forma constante as medidas de proteção, alinhando-as com os avanços tecnológicos e alterações legislativas ou regulamentares. Estas medidas devem ser:

// Tecnicamente eficazes;

// Economicamente viáveis;

// Não comprometer a produtividade e eficiência do INE, I.P..

Linhas orientadoras para a Gestão da Segurança da Informação

Gestão de pessoas

A Política de Segurança da Informação aplica-se a todos os utilizadores do INE, I.P. e deve ser implementada de forma transversal em todas as unidades orgânicas. Devem ser definidas responsabilidades específicas para funções críticas, assegurando o envolvimento e a colaboração de todos na proteção da informação.

Gestão do risco

Todos os sistemas, existentes ou planeados, devem garantir um nível de segurança da informação proporcional aos riscos identificados e assumidos pelo INE, I.P..

Definição de responsabilidades

O INE, I.P. é responsável pela qualidade, controlo de acessos, utilização e proteção da informação armazenada nos seus sistemas. Cabe à organização:

// Definir políticas e procedimentos que assegurem níveis adequados de segurança da informação;

// Monitorizar a sua implementação e eficácia.

Políticas de segurança da informação

Devem ser estabelecidas e mantidas políticas detalhadas de segurança da informação, aplicáveis a todos os sistemas, independentemente do seu ambiente ou infraestrutura.

Procedimentos de segurança da informação

Os procedimentos devem ser claros e detalhados, especificando:

// O que fazer e como fazer para alcançar os níveis desejados de segurança da informação;

// O grau de envolvimento humano necessário para a manutenção dos sistemas.

Rastreabilidade dos sistemas de informação

As operações realizadas nos sistemas de informação devem ser rigorosamente documentadas, permitindo identificar, a qualquer momento, quem realizou uma ação, quando foi realizada e o que foi feito.

Monitorização de controlos

A eficácia dos controlos implementados para mitigar os riscos depende de uma monitorizaçãocontínua. Isso inclui:

// Avaliar se os controlos estão alinhados com os objetivos organizacionais;

// Definir ações corretivas imediatas em caso de falha ou não operacionalidade dos controlos.

Modelo de Gestão de Segurança da Informação

O modelo de Gestão de Segurança da Informação (GSI) do INE, I.P. baseia-se em três pilares fundamentais, conhecidos como os princípios da confidencialidade, integridade e disponibilidade da informação:

// **Confidencialidade:** Garantia de que a informação esteja acessível apenas a utilizadores autorizados e entidades externas devidamente credenciadas, conforme as necessidades daorganização.

// **Integridade:** Assegurar a exatidão e confiabilidade da informação, protegendo-a contra modificações não autorizadas e garantindo que os métodos de processamento sejam corretos e consistentes.

// **Disponibilidade:** Garantir que a informação esteja acessível a utilizadores autorizados sempre que necessário, evitando interrupções que possam impactar o funcionamento da organização.

Todos os mecanismos de segurança da informação implementados no INE, I.P. são direcionados para a proteção da confidencialidade, integridade e disponibilidade da informação. Estes mecanismos são regidos por um conjunto normativo composto por:

// Políticas detalhadas de segurança da informação;

// Processos e procedimentos específicos para garantir a conformidade e a proteção da informação;

// Demais políticas e procedimentos integrados no Sistema de Gestão Integrado (SGI).

Este modelo é estruturado de forma a assegurar uma abordagem eficaz e contínua à gestão de segurança da informação em toda a organização.

Políticas detalhadas de Segurança da Informação

As políticas e procedimentos detalhados da Gestão de Segurança da Informação (GSI) do INE, I.P. estão estruturados de acordo com os requisitos da ISO/IEC 27001:2022 e abrangem as seguintes áreas:

1. Controlo de acessos
2. Confidencialidade estatística (pública)
3. Classificação de confidencialidade da informação
4. Segurança física e ambiental
5. Backups
6. Transferência da informação
7. Proteção contra malware
8. Zero trust
9. Controlos criptográficos
10. Segurança de comunicações
11. Privacidade e proteção de dados pessoais (pública)

Procedimentos

1. Gestão de utilizadores
2. Revisão e teste das palavras-passe
3. Acessos via VPN
4. Gestão de incidentes de segurança
5. Controlo de alterações
6. Gestão de riscos
7. Gestão de capacidade
8. Gestão de continuidade de negócio
9. Não conformidades e ações corretivas
10. Gestão documental
11. Auditorias internas
12. Operações ESS MDE e CDE
13. Revisão pela gestão

14. Procedimento de eliminação segura e reutilização de suportes de dados e equipamentos

15. Monitorização

Estas políticas e procedimentos são definidos e implementados para garantir que os controlos de segurança da informação estejam em conformidade com os requisitos da ISO/IEC 27001:2022, assegurando que todos os ativos de informação do INE, I.P. estejam protegidos contra ameaças e vulnerabilidades, e que a continuidade dos negócios seja mantida com a máxima segurança.

Organização da Segurança da Informação

A organização da segurança da informação no INE, I.P. tem como objetivo estabelecer, implementar, manter e melhorar continuamente a Gestão de Segurança da Informação (GSI), de acordo com as necessidades da organização. Este processo inclui a especificação de requisitos claros para a avaliação e tratamento de riscos relacionados com a segurança da informação.

Estrutura de Gestão da Segurança da Informação

A gestão do GSI é suportada por uma estrutura organizacional claramente definida, composta pelos seguintes elementos:

//O Conselho Diretivo - Responsável pela supervisão, controlo e avaliação da implementação do GSI, garantindo o alinhamento com os objetivos estratégicos do INE, I.P.SI;

// Responsável de Segurança da Informação (RSI) - Responsável pela gestão operacional do GSI, incluindo o desenvolvimento, implementação e monitorização contínua de políticas e controlos de segurança da informação;

// Responsável de Gestão da Qualidade - Gere o Sistema de Gestão Integrado (SGI), assegurando a integração eficaz da segurança da informação com os processos de qualidade e outros sistemas de gestão

// Encarregado de Proteção de Dados (EPD) - Participa ativamente no desenvolvimento e gestão do GSI, com especial foco na Política de Privacidade e na Proteção de Dados Pessoais, garantindo a conformidade com o Regulamento Geral sobre a Proteção de Dados (RGPD) e outras regulamentações aplicáveis;

// Equipa de Segurança da Informação - Inserida no Serviço de Infraestrutura Tecnológica e Segurança da Informação, do Departamento de Metodologia e Sistemas de Informação. É responsável pela implementação, monitorização e melhoria contínua dos mecanismos desegurança da informação;

// Responsáveis pelas Unidades Orgânicas e Trabalhadores - Colaboram como facilitadores em todas as unidades orgânicas do INE, I.P., assegurando a implementação das políticas de segurança da informação e o cumprimento das normas e procedimentos estabelecidos.

Manutenção e Comunicação das Políticas e Procedimentos de Segurança da Informação

As políticas e procedimentos de segurança da informação devem ser devidamente comunicados a todas as partes interessadas, no âmbito das suas responsabilidades e áreas de aplicação. A organização deve assegurar uma comunicação clara e efetiva, garantindo que todas as partes compreendem as suas obrigações individuais em matéria de segurança da informação.

Para assegurar a sua eficácia, as políticas e procedimentos de segurança da informação são regularmente revistos e atualizados, de forma a garantir que permanecem relevantes, adequados e alinhados com:

// Os requisitos organizacionais;

// A evolução das ameaças à segurança da informação;

// As mudanças nos requisitos legais e normativos.

A Gestão de Segurança da Informação (GSI) é regularmente avaliado através de auditorias internas e externas, realizadas por:

1. Entidades auditoras independentes, no âmbito do sistema "ESS[2]) IT Security Framework", abrangendo os processos de estatísticas de comércio internacional, incluindo:

// MDE (Micro-Data Exchange Intra-EU);

// CDE (Customs Data Exchange Extra-EU).

2. Entidades acreditadas ISO/IEC 27006, que certificam o GSI do INE, I.P., garantindo a conformidade com os requisitos da norma NP ISO/IEC 27001:2022 no contexto dos processos de estatísticas internacionais (intra e extra UE).

Este processo contínuo de comunicação, revisão e auditoria assegura que o GSI do INE, I.P. mantém elevados padrões de segurança da informação, protegendo os ativos críticos e promovendo a a confiança das partes interessadas.

[1]) Partes interessadas correspondem a todos os elementos (exemplo: cidadãos, empresas, entidades públicas e privadas) que de alguma forma afetam ou são afetados pela organização.

[2]) European Statistical System

contactos

Sede | Av. António José de Almeida 1000-043 LISBOA
Telefone geral: + 351 218 426 100* E-mail:ine@ine.pt

Apoio a Utilizadores I Serviço de Difusão
Telefone: + 351 218 440 695*
E-mail:info@ine.pt

Centro de Apoio em Portugal às Estatísticas Europeias
Telefone : + 351 218 440 447*
E-mail:ESDS@ine.pt

Horário de funcionamento:
9h00-17h00, nos dias úteis

Atendimento a Jornalistas | Serviço de Comunicação e Imagem
Telefone direto: + 351 218 426 110*
Telefone geral: + 351 218 426 100*
(ext:1248/1473)
E-mail:sci@ine.pt

Horário de funcionamento:
9h30-18h30, nos dias úteis

Biblioteca | Sede
Email: biblioteca@ine.pt
Horário de funcionamento:
9h00-12h30/14h00-17h00, nos dias úteis

Apoio a respondentes (empresas/ organizações ou famílias) | Departamento de Recolha e Gestão de Dados
Tel.: + 351 218 426 307*
E-mail: webinq@ine.pt

Horário: das 9h00 às 17h00, nos dias úteis.

Delegação do Porto | Edifício Scala Rua do Vilar, 235 – 4050-626 Porto
Telefone geral: + 351 226 072 000*
E-mail: dp@ine.pt

Horário de funcionamento da biblioteca: 9h00-12h30/14h00-17h00, nos dias úteis

Delegação de Coimbra | Rua Aires de Campos, Casa das Andorinhas
3000-014 COIMBRA
Telefone geral: + 351 239 790 400*
E-mail: dc@ine.pt

Horário de funcionamento da biblioteca: 9h00-12h30/14h00-17h00, nos dias úteis

Delegação de Évora | Rua Miguel Bombarda, 36
7000-919 ÉVORA
Telefone geral: + 351 266 757 700*
E-mail: de@ine.pt

Horário de funcionamento da biblioteca: 9h00-12h30/14h00-17h00, nos dias úteis

Delegação de Faro | Rua Cândido Guerreiro, 43-3ºFte
8000-318 FARO
Telefone geral: + 351 289 887 800*
E-mail: df@ine.pt

Horário de funcionamento da biblioteca: 9h00-12h30/14h00-17h00, nos dias úteis

Serviço Regional de Estatística dos Açores | Rua da Rocha, 26
9700-169 ANGRA DO HEROÍSMO
Telefone geral: +351 295 204 020*
E-mail: srea@azores.gov.pt

Direção Regional de Estatística da Madeira | Calçada de Santa Clara, 38
9004-545 FUNCHAL
Telefone geral: +351 291 720 060*
E-mail: drem@ine.pt

* Chamada para rede fixa nacional