POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

ANDERSEN®

INFORMAÇÃO PÚBLICA

Painel de controlo

Título:	Política de segurança
Tipo de documento:	Política
Nome do ficheiro:	PO-Política de Segurança da Informação
Classificação:	Público
Estado:	Aprovado
Autor:	Diretor de Cibersegurança

Análise e aprovação		
Avaliado por:	CIO	22/5/2025
Aprovado por:	Sócio-gerente	26/05/2025

Lista de distribuição	
Empresa	Pessoal da ANDERSEN e partes interessadas relevantes

ÍNDICE

Conteúdo

1 DECLARAÇÃO DA DA POLÍTICA DE POLÍTICA DE SEGURANÇA DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

O objetivo desta política é fornecer diretivas ou orientações a seguir para proteger a informação da organização contra uma vasta gama de ameaças, a fim de

- Garantir a segurança das operações efectuadas, através dos sistemas de informação.
- Atenuar os incidentes de segurança da informação.
- Gerir os riscos de segurança da informação.
- Assegurar o cumprimento dos objectivos da organização.

A ANDERSEN está empenhada em tornar os princípios da Política de Segurança da Informação parte da cultura da organização e implementou um Sistema de Gestão da Segurança da Informação baseado numa norma internacionalmente reconhecida.

Todo o pessoal da ANDERSEN, as partes interessadas relevantes e a direção devem ter conhecimento desta política e cumpri-la.

Esta política será desenvolvida através de regulamentos, procedimentos, instruções de funcionamento, guias, manuais e todos os instrumentos organizacionais considerados úteis para atingir os seus objectivos.

2 POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

2.1 ÂMBITO DE APLICAÇÃO

O âmbito da Política de Segurança da Informação coincide com o âmbito do Sistema de Gestão da Segurança da Informação (SGSI). Com este documento, são desenvolvidos os requisitos exigidos pela norma ISO/IEC 27001:2022 na sua secção: 5.2 "Política".

Esta política abrange toda a informação utilizada para o desenvolvimento das suas actividades pelas entidades que fazem parte do Sistema de Gestão da Segurança da Informação (SGSI).

2.2 DEFINIÇÕES E ACRÓNIMOS

Para efeitos da correta interpretação da presente Política, incluem-se as seguintes definições:

- **Informação:** dados que têm significado, em qualquer formato ou meio. Refere-se a qualquer comunicação ou representação de conhecimentos.
- **Sistema de Informação:** refere-se a um conjunto de recursos relacionados e organizados para o tratamento da informação, de acordo com determinados procedimentos, tanto informáticos como manuais.

2.3 OBJECTIVOS DO DA POLÍTICA DE SEGURANÇA DE SEGURANÇA DA INFORMAÇÃO OBJECTIVOS DA POLÍTICA DE

O principal objetivo da criação desta Política de Segurança da Informação, pelo Responsável do Sistema de Gestão de Segurança da Informação (SGSI), Gestor de Cibersegurança e Risco e pela Direção Geral da ANDERSEN, é garantir aos clientes e utilizadores de serviços o acesso à informação com a qualidade e o nível de serviço necessários para o desempenho acordado, bem como evitar perdas ou alterações graves da informação e o acesso não autorizado à mesma.

É estabelecido um quadro para a realização dos objectivos de segurança da informação da organização. Estes objectivos devem ser alcançados através de uma série de medidas e normas organizacionais claramente definidas e concretas.

A presente política de segurança deve ser mantida, actualizada e adaptada à sua finalidade.

Os princípios a respeitar, baseados nas dimensões básicas da segurança, são os seguintes

- **Confidencialidade**: propriedade pela qual a informação gerida pela ANDERSEN só pode ser acedida pelas pessoas autorizadas para o efeito, após identificação, no momento e pelos meios previstos.
- **Integridade:** propriedade que garante a validade, exatidão e exaustividade da informação gerida pela ANDERSEN, sendo o seu conteúdo o fornecido pelas pessoas afectadas sem qualquer tipo de manipulação e permitindo que seja modificada apenas pelas pessoas autorizadas a fazê-lo.
- **Disponibilidade:** propriedade de estar acessível e utilizável com a periodicidade acordada. A informação gerida pela ANDERSEN é acessível e utilizável pelos clientes e utilizadores autorizados e identificados em qualquer momento, sendo garantida a sua própria persistência perante qualquer eventualidade prevista.

Além disso, dado que qualquer sistema de gestão da segurança da informação deve respeitar a legislação em vigor, deve ser observado o seguinte princípio

- **Legalidade:** refere-se ao cumprimento das leis, regras, regulamentos ou disposições a que a ANDERSEN está sujeita, especialmente no que diz respeito à proteção de dados pessoais.

2.4 PLANEAMENTO

Para dar cumprimento à declaração da política de segurança, está previsto um conjunto de acções que incidem na implementação, gestão e manutenção de um SGSI, sempre em consonância com esta política. Como parte da fase de planeamento, considera-se essencial efetuar uma análise dos riscos relacionados com a segurança da organização. Com base em

Neste estudo, é elaborado um plano de tratamento específico para os riscos que a organização não considera aceitáveis.

2.5 IMPLEMENTAÇÃO

A implementação do SGSI é da responsabilidade principal do diretor de Cibersegurança e Riscos responsável pela segurança, apoiado em todos os momentos pelos restantes diretores de área e com o total apoio da Direção Geral.

Com base nos resultados obtidos durante a fase de planeamento, são implementados os controlos de segurança necessários e são postos em prática os procedimentos definidos no SGSI, tudo com o objetivo de cumprir os requisitos estabelecidos pelas normas ISO 27001.

2.6 REVISÃO

A política de segurança da informação e o SGSI são revistos regularmente a intervalos planeados ou se ocorrerem alterações relevantes, a fim de garantir a sua permanente adequação, eficácia e eficiência. De um modo geral, são revistos anualmente em conjunto com os processos de auditoria interna do SGSI.

2.7 MELHORIAS

Os possíveis melhoramentos da Política de Segurança da Informação e do SGSI são estabelecidos durante as fases de revisão ou com base nos contributos do pessoal da ANDERSEN e do pessoal externo.

Estas melhorias são avaliadas e, uma vez avaliada a sua viabilidade, são implementadas, exploradas e mantidas.

2.8 RECURSOS AFECTADOS AO SGSI

A ANDERSEN identificou e disponibilizou os recursos necessários para garantir o estabelecimento, a implementação, a manutenção e a melhoria contínua do seu Sistema de Gestão da Segurança da Informação (SGSI). Esta atribuição de recursos reflecte um compromisso organizacional para com a eficácia do sistema e para com a realização dos objectivos estratégicos e operacionais da organização.

Em termos de recursos humanos, a estrutura de gestão responsável pelo SGSI é composta essencialmente por duas figuras-chave: o Chief Information Officer e o Diretor de Cibersegurança e Risco, que lideram e supervisionam os processos relacionados com a gestão do sistema. Estas funções são complementadas com o apoio de uma consultoria externa especializada, cuja intervenção proporciona uma visão objetiva, bem como conhecimentos técnicos adicionais que reforçam a implementação e evolução do SGSI.

Em conjunto, estes recursos permitem à ANDERSEN manter uma gestão eficaz, assegurar a conformidade com os requisitos aplicáveis e promover a melhoria contínua em todas as áreas abrangidas pelo sistema.

3 GESTÃO DOS RISCOS

A gestão da segurança da informação na ANDERSEN baseia-se no risco, em conformidade com a norma internacional ISO/IEC 27001:2022.

Articula-se através de um processo geral de avaliação e tratamento dos riscos, que podem potencialmente afetar a segurança da informação dos serviços prestados, consistindo em

- **Identificar ameaças** que explorem vulnerabilidades nos sistemas de informação que suportam ou dos quais depende a segurança da informação.
- **Analisar o risco**, com base na consequência da materialização do perigo e na probabilidade de ocorrência.
- **Avaliar o risco,** de acordo com um nível pré-estabelecido e aprovado de risco amplamente aceitável, tolerável e inaceitável.
- **Abordar os riscos** inaceitáveis, através de controlos ou salvaguardas adequados.

Este processo é cíclico e deve ser efectuado com regularidade, pelo menos uma vez por ano. Para cada risco identificado, será atribuído um proprietário, podendo ser atribuídas várias responsabilidades à mesma pessoa ou comité.

4 OBJECTIVOS DE SEGURANÇA DA INFORMAÇÃO

De forma a contribuir para a minimização e controlo dos riscos da Organização, será definido um conjunto de objectivos reais e mensuráveis. Estes objectivos serão medidos, pelo menos, semestralmente e revistos anualmente, de forma a estarem alinhados com a estratégia da ANDERSEN.

A definição dos objectivos de segurança da informação é feita tendo em conta os seguintes elementos:

- Relatórios do Gestor de Cibersegurança e Risco e do Gestor do SGSI, aprovados pelo Sócio-Gerente da ANDERSEN.
- Oportunidades de melhoria encontradas durante o funcionamento do SGSI.
- Contribuições do responsável pela proteção de dados (RPD), que supervisiona e aconselha sobre o cumprimento da regulamentação em matéria de proteção de dados, bem como sobre a identificação e atenuação dos riscos associados ao tratamento de dados pessoais.

Ao definir os objectivos, há que ter em conta que estes devem ser mensuráveis e realizáveis, pelo que o planeamento para a sua consecução deve incluir

- O que deve ser feito
- Os recursos necessários
- Quem será responsável
- O prazo para a sua realização
- Como serão avaliados os resultados
- Se aplicável, o indicador associado a esse objetivo

O Sócio-Gerente, juntamente com o Gestor de Cibersegurança e Risco, será responsável pela definição dos objectivos de segurança da informação para a ANDERSEN. Estes devem ser específicos e coerentes com a sua Política de Segurança da Informação, missão, visão e valores.

5 ORGANIZAÇÃO E RESPONSABILIDADES

A organização da segurança da informação está organizada em torno de um Sistema de Gestão da Segurança da Informação (SGSI) e de uma série de comités e funções envolvidos no seu âmbito.

- O sócio diretor da ANDERSEN é responsável pela aprovação desta política.
- O Comité de Gestão do Risco da Informação é responsável pela revisão desta política.
- O Gestor de Cibersegurança e Risco é responsável pela manutenção desta política.
- O responsável pela proteção de dados supervisiona e aconselha sobre o cumprimento das medidas aplicadas.

6 APLICAÇÃO DAS POLÍTICAS

A ANDERSEN elaborou o presente documento que contém a Política Geral de Segurança da Informação, que foi aprovado pelo Sócio-Gerente e dado a conhecer a todo o pessoal da empresa.

7 FORMAÇÃO E SENSIBILIZAÇÃO

A forma mais eficaz de reforçar a segurança é proporcionar formação contínua e integrá-la nas tarefas diárias de trabalho.

Os programas de formação devem incluir cursos específicos sobre segurança da informação, adaptados à área correspondente e ao público-alvo, conforme considerado adequado. Além disso, devem ser realizadas regularmente campanhas de sensibilização para a segurança, dirigidas a todo o pessoal, utilizando os canais mais adequados.

O Gestor de Cibersegurança e Risco deve assegurar que todo o pessoal envolvido no SGSI tem conhecimento desta política, dos seus objectivos e processos, através da sua divulgação, formação e acções de sensibilização. No caso da formação em matéria de proteção de dados, deve ter em conta os requisitos do Delegado para a Proteção de Dados.

Deve também assegurar a distribuição dos documentos que se aplicam a cada nível, de acordo com os diferentes papéis definidos na empresa.

8 GESTÃO DA CONTINUIDADE DAS ACTIVIDADES

A ANDERSEN organizará os planos necessários para a implementação do processo de Análise de Impacto no Negócio (BIA) e do Plano de Continuidade do Negócio, bem como a ativação do Plano de Continuidade do Negócio quando necessário. O departamento de TI deve gerar um Plano de Continuidade do Negócio, documentando e implementando processos e procedimentos para garantir a continuidade tecnológica exigida pela empresa.

Todos os funcionários ajudarão a retomar atempadamente todos os serviços críticos para a ANDERSEN no caso de uma contingência importante, ajudando assim a garantir que a maioria dos serviços seja restabelecida no mais curto espaço de tempo possível.

9 AUDITORIA

A Direção Geral da ANDERSEN deve assegurar e verificar, através de auditorias internas e externas, o grau de cumprimento das diretrizes desta Política e que as mesmas são corretamente operadas e implementadas, responsabilizando-se pelo cumprimento das medidas corretivas que tenham sido determinadas com vista a manter a melhoria contínua.

10 VALIDADE E ACTUALIZAÇÃO

Esta política entra em vigor aquando da sua publicação e é revista pelo menos uma vez por ano.

O objetivo das revisões periódicas é adaptá-lo às mudanças no contexto da organização, com atenção às questões externas e internas, analisando os incidentes de segurança da informação ocorridos e as não-conformidades encontradas no SGSI. Tudo isto é harmonizado com os resultados dos diferentes processos de avaliação de risco.

Aquando da revisão da Política, serão também revistas todas as Normas e outros documentos que a desenvolvem, seguindo um processo de atualização periódica sujeito a alterações relevantes que possam ocorrer: crescimento da empresa e alterações organizacionais, alterações de infra-estruturas, desenvolvimento de novos serviços, entre outros.

Como resultado, será elaborada uma lista de objectivos e acções a realizar e implementar durante o ano seguinte para garantir a Segurança da Informação e a utilização adequada dos recursos que a suportam e processam na ANDERSEN.

11 SANÇÕES

O não cumprimento da Política de Segurança da Informação e demais regulamentos e procedimentos que a desenvolvem implicará a aplicação de sanções, de acordo com a magnitude e caraterísticas do aspeto não cumprido, nos termos da legislação laboral em vigor.

12 VALIDADE

A Política de Segurança da Informação entra em vigor na data da sua publicação.

13 RATIFICAÇÃO

Todos os abaixo assinados assumem e aceitam plenamente o conteúdo desta Política e comprometem-se a aplicá-la nas suas respectivas áreas, de modo a conseguir o correto funcionamento do Sistema de Gestão da Segurança da Informação.

Madrid, 26 de maio de 2025

29175499E JOSE VICENTE MOROTE (R: B46356481)
Assinado digitalmente por 29175499E JOSE VICENTE MOROTE (R: B46356481)
Data: 2025.05.26 20:39:08 +02'00'

José Vicente Morote
Sócio-Gerente

Assinado por ESPINOSA MARTINEZ JOSE MIGUEL - ***2268** o dia 27/05/2025 com um certificado

Miguel Espinosa
CIO

Assinado digitalmente por DELGADO MESA JONAS - 78562999J
Nome de reconhecimento (DN): c=ES, serialNumber=IDCES-78562999J, givenName=JONAS, sn=DELGADO MESA, cn=DELGADO MESA JONAS - 78562999J
Data: 2025.05.27 18:29:14 +02'00'

Jonás Delgado Mesa
Gestor de Cibersegurança e Risco