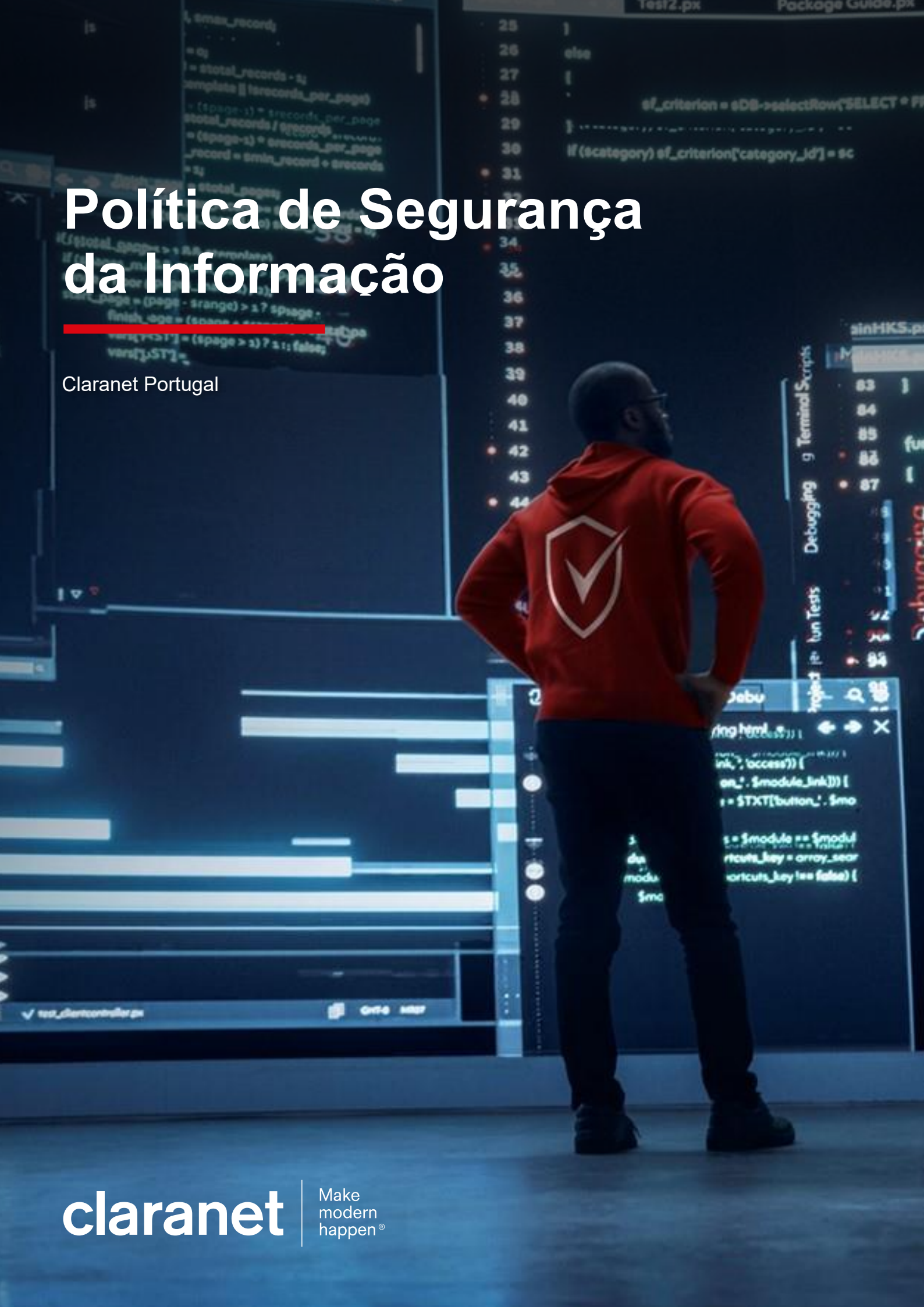
Política de Segurança da Informação

Claranet Portugal



claranet | Make modern happen®

Índice

1. Introdução

A Política de Segurança da Informação da Claranet Portugal constitui uma base comum a todos os Departamentos, permitindo a adoção de padrões de segurança organizacional, de práticas eficazes na Gestão de Segurança da Informação e fornecendo confiança nos intercâmbios inter-organizacionais que envolvam a Claranet.

A Política de Segurança da Informação pretende aplicar ao Sistema de Gestão Integrado a norma internacional ISO/IEC 27001, as normas comunitárias e a legislação e recomendações nacionais específicas em matéria de Segurança da Informação.

A equipa de Gestão da Claranet assume o duplo compromisso de:

- Adotar e manter todos os requisitos legais aplicáveis no contexto da Segurança da Informação;
- Assegurar as condições para a melhoria contínua do sistema, através da monitorização e revisões regulares das componentes relacionadas com a Segurança de Informação.

Este documento descreve os princípios gerais que devem ser aplicados por cada Departamento da Claranet aos ativos de informação por si geridos e encontra-se estruturado do seguinte modo:

- Audiência;
- Importância da informação e da Segurança da Informação;
- Política de Segurança da Informação;
- Responsabilidade na Segurança da Informação;
- Manutenção e comunicação das Políticas de Segurança.

2. Siglas e Definições

Sigla	Definição
Ativo	Qualquer recurso com valor humano ou tecnológico (quantificável ou não) que seja indispensável ao funcionamento da Claranet e que permita garantir os objetivos propostos
CISO	*Chief Information Security Officer*
Dados	Representação formal de matéria não trabalhada a partir da qual é gerada informação pelo seu processamento ou interpretação
Informação	Todos os dados passíveis de serem processados com o intuito de gerar conhecimento para o seu recetor
Segurança da Informação	Conjunto de medidas tendentes à proteção dos ativos de informação quanto à sua divulgação, alteração e acesso não autorizado
SGI	Sistema de Gestão Integrado
SGSI	Sistema de Gestão de Segurança da Informação
Sistemas de Informação	Expressão utilizada para descrever um sistema automatizado, ou mesmo manual, que considere pessoas, máquinas, e/ou métodos organizados para recolha, processamento, transmissão e disseminação de dados que representam informação para o seu utilizador

3. Audiência

A Política de Segurança da Informação da Claranet destina-se a todos os colaboradores, estagiários, consultores temporários, prestadores de serviços e outros *stakeholders* que, com esta, participem no tratamento de Informação. Todos têm de estar em conformidade com a Política de Segurança da Informação e com os demais documentos relacionados com a Segurança da Informação, em particular as "Políticas Detalhadas Segurança de Informação" (Pol.02).

Faz-se notar que qualquer utilização imprópria de equipamentos da empresa, equipamento pessoal ligado a recursos da empresa, rede da empresa, Sistema de email ou quaisquer outras aplicações de tratamento de informação ou recursos da empresa – bem como a utilização destes para fins ilícitos – tem o potencial de expor a empresa e o seu Grupo a consequências sérias. Tal inclui ações como o acesso não autorizado aos sistemas de computador, dados ou ativos, a introdução de vírus, roubo/divulgação de segredos da empresa/outras informações confidenciais e o roubo ou tratamento ilícito de dados pessoais.

Os colaboradores e outros prestadores que deliberadamente violem esta ou outras políticas ficam sujeitos a ações disciplinares/legais, que podem ir até à cessação do seu vínculo contratual e participação às autoridades judiciais das situações que indiciem a prática de crime.

4. Importância da Informação

A informação pode existir em diversos formatos ou meios de suporte (eletrónico, registada em papel ou outros média, conhecimento, etc.) e ser transmitida por correio, meios eletrónicos ou verbais, devendo ser adequadamente protegida independentemente do seu formato, utilização ou transmissão.

A preservação da confidencialidade, integridade e disponibilidade da informação depende de uma abordagem sistemática do risco de forma a minimizar os incidentes que ponham em causa a sua segurança.

O acesso à informação é um aspeto central do funcionamento da Claranet, dependendo da disponibilidade dos Sistemas e infraestruturas de informação a eficiência do serviço prestado aos seus Clientes. A segurança no tratamento e transmissão da informação é, assim, um fator vital para manter a sua eficiência.

Qualquer interrupção do serviço, fuga de informação para entidades não autorizadas ou modificação não autorizada de dados pode levar a uma perda de confiança e/ou violar as obrigações legais e regulamentares para com os Clientes, parceiros ou outras obrigações vigentes.

A mudança de sistemas de processamento clássicos – baseados em centros informáticos fechados – para as mais variadas formas de processamento distribuído de dados em ambientes abertos e heterogéneos cliente/servidor, traz riscos adicionais que necessitam de ser geridos, uma vez que a informação relevante e as aplicações que a tratam aumentam continuamente, a par com a sua utilização em locais de difícil controlo.

Para atingir os seus objetivos na vertente de segurança da informação, os Departamentos da Claranet estão dependentes do funcionamento correto dos seus sistemas de informação e comunicações. No entanto, tal apenas se torna possível com a identificação contínua dos riscos aos quais os ativos da Claranet se encontram expostos,

bem como, pela implementação de controlos e mecanismos de segurança que visem a utilização correta e controlada dos mesmos.

É da responsabilidade de todos os colaboradores da Claranet (bem como dos outros intervenientes da audiência desta política) contribuir proactivamente para a proteção da informação, inclusive aquando da partilha de informação sensível, mesmo na forma verbal. Da mesma forma cabe-lhes a responsabilidade de reportar qualquer ameaça, concretizada ou por concretizar, que possa ter qualquer impacto na disponibilidade, integridade ou confidencialidade da informação.

5. Importância da Segurança da Informação

A informação gerida pela Claranet, os seus processos de suporte, sistemas, aplicações e redes são ativos valiosos para a organização. Qualquer perda de confidencialidade, integridade e/ou disponibilidade podem levar à perda de credibilidade dos serviços prestados pela Claranet.

A Segurança da Informação deverá, portanto, ser aplicada em todas as fases do ciclo de vida da mesma. O controlo das operações de inserção/recolha, processamento, armazenamento, transferência, relacionamento, pesquisa e destruição da informação são tão importantes como a funcionalidade de uma aplicação. Deve assim ser assegurada a manutenção – de forma permanente e equilibrada – de um nível de qualidade e segurança elevado, prevenindo a materialização de riscos inerentes, com vista a mitigar / limitar os potenciais danos provocados pela exploração de vulnerabilidades e incidentes de segurança, garantindo que o negócio opera conforme esperado ao longo do tempo.

A Segurança da Informação deve ser um pressuposto fundamental para o sucesso dos serviços prestados pela Claranet, sendo, portanto, da responsabilidade de todos os colaboradores, fornecedores, parceiros ou outras entidades que, em cada momento, tenham acesso à informação.

As ameaças à Segurança da Informação estão em constante evolução, o que implica a adaptação contínua de medidas de segurança de modo a acompanhar as alterações tecnológicas, legislativas e/ou sociais. As medidas de segurança devem ser técnica e economicamente viáveis e não devem limitar de forma inadequada a produtividade e eficiência da Claranet. Os riscos residuais devem ser do conhecimento da Administração e dos Diretores que possuam responsabilidades operacionais sobre os ativos associados.

6. Política de Segurança da Informação

A Política de Segurança da Informação da Claranet assenta nos seguintes três pilares:

- **Confidencialidade:** garantia de que a informação está acessível apenas por pessoas e processos devidamente autorizadas para o efeito;
- **Integridade:** salvaguarda da exatidão da informação e dos métodos de processamento;
- **Disponibilidade:** garantia de que utilizadores e processos autorizados têm acesso à informação sempre que necessário.

E tem em conta as seguintes vertentes:

- **Gestão de pessoas:** a Segurança da Informação é aplicável a todos os colaboradores da Claranet em todos os Departamentos, de forma transversal, devendo ser atribuídas responsabilidades específicas a determinadas funções;
- **Gestão do risco:** todos os sistemas (existentes ou planeados) devem ter um nível de segurança adequado face ao risco que a Claranet está disposta a assumir. A análise de risco deve traduzir as preocupações de índole técnica de forma percetível;
- **Definição de responsabilidades:** a responsabilidade pela qualidade, acessos, utilização e salvaguarda da informação contida nos sistemas é dos seus Responsáveis. Cabe à Claranet definir as normas e procedimentos que implementem os níveis de segurança da informação definidos pelas entidades proprietárias da informação e vigiar a sua efetividade;
- **Regras de segurança:** devem existir políticas de segurança que definam os objetivos a atingir por todos os sistemas de informação, independentemente do seu ambiente;
- **Procedimentos de segurança:** devem ser o mais detalhados possível e definir claramente como atingir o nível de segurança pretendido e qual o envolvimento humano na manutenção dos sistemas de informação, não devendo ser deixado nada ao acaso;
- **Operação adequada dos sistemas de informação:** as operações dos sistemas de informação devem estar devidamente documentadas, assegurando que a qualquer momento é possível aferir “quem” e “quando” faz “o quê”;
- **Fazer o que está correto:** a segurança da informação é da responsabilidade da Gestão. A Administração da Claranet tem a responsabilidade de agir de forma prudente, fazendo uma adequada gestão da segurança de informação com base no conhecimento da situação;
- **Saber o que está a acontecer:** definir controlos e implementar uma adequada monitorização dos mesmos, de forma a avaliar se estes se encontram ajustados face aos objetivos definidos e definindo ações de resposta/mitigação atempadas quando se verifique a não operacionalidade dos controlos.

A Claranet assegura que não se pretende implementar, autorizar ou estabelecer qualquer monitorização remota dos sistemas ou instrumentos (abertos ou escondidos) relativamente a opiniões, hábitos ou atividades dos colaboradores – que aliás é estritamente proibida.

Esta política visa apenas criar meios para verificar se os recursos profissionais e/ou pessoais se encontram a ser corretamente utilizados, para necessidades organizativas e produtivas, segurança do local de trabalho, proteção dos ativos da Empresa e para a segurança desta (e, em particular, da sua rede, sistemas de informação).

7. Responsabilidades na Segurança da Informação

A Política de Segurança da Informação é da responsabilidade do CISO – *Chief Information Security Officer*, cabendo-lhe o controlo e a avaliação da implementação do Sistema de Gestão de Segurança da Informação (SGSI) – integrado no Sistema de Gestão Integrado (SGI), a comunicação à gestão de topo do seu desempenho e a garantia da conformidade do sistema com os requisitos da Norma.

8. Manutenção e Comunicação das Políticas de Segurança

A Política de Segurança da Informação deve ser periodicamente revista, de forma a garantir que continua a ser adequada à Claranet Portugal e deve ser comunicada a todos os colaboradores e *stakeholders* envolvidos no tratamento da informação.