POLÍTICA DE SEGURANÇA PARA A GESTÃO DOCUMENTAL

Índice

1. Introdução

A Política de Segurança para a Gestão Documental, foi elaborada ao abrigo da Lei nº 5/2020, de Prevenção e Combate ao Branqueamento de Capitais, do Financiamento do Terrorismo e da Proliferação de Armas de Destruição em Massa e da Norma ISO/IEC 27002:2022; que refletem as regras aplicáveis a Inovadora Capital, Sociedade e Distribuidora de Valores Mobiliários, de Segurança para a Gestão Documental.

1.1 Objectivo

O presente documento concretiza a Política de Segurança para a Gestão Documental adoptada pela Inovadora Capital, e estabelece os princípios gerais que esta deve aplicar aos activos por si geridos em matéria de segurança para a Gestão Documental.

A informação constitui um dos activos mais relevantes que uma organização tem ao seu cuidado. O desenvolvimento exponencial das tecnologias de informação a que temos assistido nos últimos anos, e, em particular da internet, tem contribuído para que diariamente sejam gerados grandes volumes de dados.

Por conseguinte, a Administração da Inovadora Capital considera crucial desenvolver e aplicar uma política que salvaguarde a integridade e confidencialidade de informação, com o intuito de proteger a informação seguindo as melhores práticas e garantir a eficácia do negócio.

1.2 Âmbito

A Política de Segurança para a Gestão Documental aplica-se a todas as actividades desenvolvidas pela Inovadora Capital, bem como a todas as partes interessadas, nomeadamente os colaboradores da Inovadora Capital, nos quais se incluem prestadores de serviços e entidades que processem informações da Inovadora Capital. Todas as partes interessadas que violem esta política ficam sujeitas a sanções e outras acções como por exemplo a cessão do contrato e/ou denúncias às entidades policiais ou judiciais de situações que possam suscitar a prática de crime.

2. Declaração de Compromisso

A Inovadora Capital está empenhada em garantir uma gestão eficaz da segurança de informação e dos activos à sua responsabilidade, pelo que se compromete a protegê-la, independentemente do seu formato, contra o acesso por pessoas não autorizadas, bem como a criar condições que garantam o acesso à informação sempre que necessário, e que essa informação seja fidedigna, transparente e autêntica. Essa garantia é reforçada pela aposta na melhoria contínua do Sistema de Gestão de

Segurança de Informação e realização de análises de risco regulares, implementação dos controlos necessários e ainda definição de responsabilidades.

3. Princípios Gerais

O Sistema de Gestão de Segurança de Informação da Inovadora Capital, apresenta um conjunto de princípios transversais a todos os domínios de Segurança de Informação:

- Assegurar a integridade, a confidencialidade e a disponibilidade da informação;
- Garantir e reforçar a conformidade com a regulamentação e exigências legais em vigor;
- Assegurar o desenvolvimento, implementação e reavaliação periódica das políticas, processos e controlos em alinhamento com as melhores práticas no âmbito da segurança;
- Avaliar e monitorizar regularmente os riscos associados à segurança;
- Reduzir os danos inerentes à ocorrência de incidentes de segurança da informação assim como garantir que os mesmos são reportados nos termos definidos para o efeito;
- Garantir que a Inovadora Capital tem capacidade de prosseguir com a sua actividade mesmo que ocorram incidentes de segurança graves;
- Promover uma cultura de sensibilização e compromisso para a segurança da informação.

4. Segurança para a Gestão Documental

4.1 Segurança

Consideram-se "activos de informação" os sistemas, portais, servidores, base de dados, equipamentos de comunicação, etc., que suportem a informação desde a recolha, processamento e armazenamento da informação, em qualquer formato. Dado o valor que estes representam para o negócio, devem ser protegidos. A Segurança da Informação consiste na protecção da informação e dos seus activos de suporte, nos seguintes pilares:

- **Confidencialidade**: Assegurar o acesso a informações apenas a pessoas com permissão para esse efeito;
- **Integridade**: Garantir a autenticidade da informação e dos métodos de processamento;
- **Disponibilidade**: Garantia do acesso à informação de pessoas ou processos autorizados, sempre que necessário:
- **Não repudiação**: Assegurar a existência de evidência inequívoca da identificação do originário de uma comunicação ou o responsável por uma operação;

- **Privacidade**: Engloba a protecção de dados pessoais de clientes e colaboradores, e da gestão de acesso aos mesmos.

4.2 Níveis de Segurança

A Política de Segurança de Informação engloba todas as normas e procedimentos no âmbito da segurança de informação, e encontram-se organizados de acordo com a seguinte estrutura hierárquica:

1. Política Geral de Segurança da Informação;
2. Políticas detalhadas, Normas e Regras;
3. Processos e Procedimentos.

4.3 Obrigação de Conservação

A Inovadora Capital deve conservar por um período de 10 (dez) anos, contados a partir do momento em que for efectuada a transacção ou após o fim da relação do negócio, no mínimo, os seguintes documentos:

- Cópias dos documentos ou outros suportes tecnológicos comprovativos do cumprimento da obrigação de identificação e de diligência, incluindo a conservação de registos sobre a classificação dos clientes;
- Registo de transacções, incluindo toda informação original e do beneficiário da transacção, para permitir a reconstituição de cada operação, de modo a fornecer o necessário, prova no âmbito de um processo criminal;
- Cópia de toda a correspondência comercial trocada com o cliente;
- Cópia das comunicações efectuadas pelas entidades sujeitas à Unidade de Informação Financeira e outras autoridades competentes;
- Registo dos resultados das análises internas, assim como o registo da fundamentação da decisão das entidades sujeitas no sentido de não cumprirem;

4.4 Políticas

Dado que a Inovadora Capital ainda se encontra num estágio inicial de desenvolvimento, irão começar a ser desenvolvidas um conjunto de políticas, procedimentos e controlos para os seguintes domínios:

- Política de Gestão de Activos de Informação;
- Política de Gestão de Risco de Segurança de Informação;
- Política de Segurança de Recursos Humanos;
- Política de Gestão de Acessos;
- Política de Gestão de Incidentes;
- Política de Segurança e Operação dos Sistemas e Instalações;
- Política de Gestão de Entidades Terceiras;

- Política de Aquisição, Manutenção e Desenvolvimento dos Sistemas de Informação;
- Política de Gestão de Operações e de Comunicações.

Qualquer uma das políticas a desenvolver será revista sempre que existirem mudanças técnicas ou organizacionais que o justifiquem, com o intuito de garantir a sua adequação. Qualquer actualização efectuada será do conhecimento de todos os colaboradores. Para além disso, à medida que forem criadas, estas políticas estarão permanentemente disponíveis para todos os colaboradores, em formato electrónico, na área partilhada.

4.5 Responsabilidades

É da responsabilidade da área de I.T. (Information Tecnology) desenvolver, melhorar e actualizar sempre que necessário a Política de Segurança de Informação, bem como solicitar a sua aprovação junto do Conselho de Administração, que por sua vez deverá aprovar estas políticas.

As principais responsabilidades da área de I.T. são:

- Desenvolver e actualizar sempre que necessário as políticas, procedimentos, processos e manuais relacionados com a segurança da informação;
- Organizar acções de consciencialização para a importância de adoptar comportamentos que não comprometam a segurança de informação;
- Promover acções de formação;
- Gestão da atribuição de acessos a colaboradores e utilizadores externos;
- Realizar avaliações de risco e desenvolver os respectivos planos de mitigação;
- Monitorizar eventos de segurança;
- Tratamento de incidentes de segurança;
- Acompanhamento, controlo e prevenção de actividades maliciosas;
- Análise, implementação e gestão ferramentas de segurança de informação;
- Estabelecer formalmente processos de cópia de segurança de informação (backup).

Já a área de Compliance é responsável não só por apoiar na implementação da regulamentação em matéria de Segurança de Informação como também assegurar a conformidade das Políticas de Segurança da Informação com as normas legais em vigor.

Compete à Unidade de Controlo Interno monitorizar os sistemas informáticos e garantir o seu alinhamento com a estratégia do negócio.

Porém, é transversal a todas as áreas que os respectivos colaboradores sejam responsáveis pelas suas acções, pelo que têm o dever de zelar pelo cumprimento das Políticas de Segurança de Informação.

4.6 Acordo de Confidencialidade

A fim de garantir a protecção, utilização e divulgação da informação serão estabelecidos com todos os colaboradores internos e externos, de forma individual, acordos de confidencialidade entre o colaborador e a Inovadora Capital. Estes deverão ser actualizados sempre que se observarem alterações relevantes no âmbito da Política de Segurança da Informação.

4.7 Relação com Terceiros

Sempre que qualquer área da Inovadora Capital tenha necessidade de recorrer a entidades externas que, no âmbito do projecto, acedam aos seus activos de informação, deverão ser feitas análises dos riscos de forma a assegurar a existência de controlos de segurança adequados. Uma vez garantidos esses controlos, deverão ser estabelecidos acordos com as entidades externas que assegurem a protecção dos activos de informação da Inovadora Capital.

5. Revisão e Actualização

A Inovadora Capital procederá à revisão anual da Política de Segurança para a Gestão Documental, procedendo à sua actualização sempre e quando ocorram alterações relevantes com impacto directo na Política.

6. Outorgamento