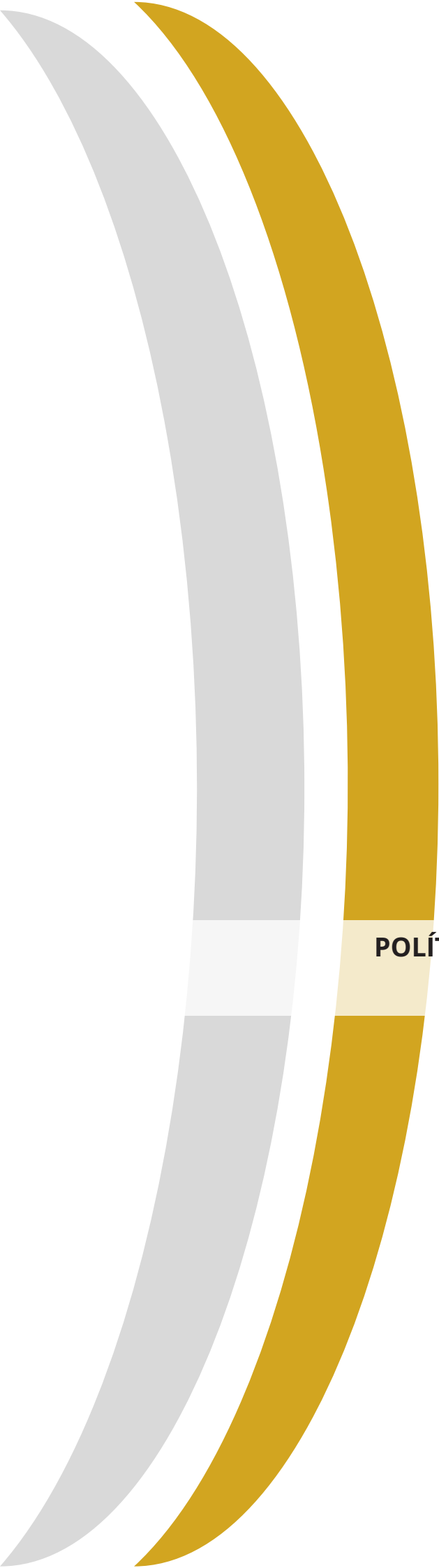




**POLÍTICA DE CÓPIAS SEGURANÇA
(BACKUP)**

Índice

1. Âmbito	3
2. Glossário	3
3. Objectivo	4
4. Funções e Responsabilidades	5
5. Comprometimento	5
5.1. Comprometimento dos Responsáveis Hierárquicos.....	5
5.2. Comprometimento dos Utilizadores	5
5.3. Comprometimento da Área de Tecnologia e Sistemas de Informação	6
6. Classificação da Informação para Efeitos de Backup	6
7. Tipos e Métodos de Cópias de Segurança	7
7.1. Ambiente On-Premise	7
7.2. Plataforma Bolsa Pro	8
7.3. Microsoft 365	9
8. Parâmetros de Backup.....	10
9. Retenção Legal de Registos	10
10. Armazenamento das Cópias de Segurança.....	11
11. Restauração e Testes	11
12. Segurança das Cópias de Segurança.....	12
13. Monitorização e Reporte de Falhas.....	12
14. Penalidades.....	13
15. Revisão e Gestão Documental	13
16. Nota de Propriedade e Distribuição	13
17. Outorgamento	Erro! Marcador não definido.

1. Âmbito

A Política de Cópias de Segurança (Backup) da Inovadora Capital (SDVM) estabelece as regras e os procedimentos aplicáveis à realização, armazenamento, protecção, retenção e restauração de cópias de segurança dos dados e sistemas de informação da Sociedade.

A presente Política desenvolve o disposto no Capítulo 8 da Política de Continuidade de Negócios e Recuperação de Desastres e articula-se com a Política de Segurança e Operação do Sistema de Informações e com o Manual de Procedimentos para o Sistema Informático da Inovadora Capital (SDVM), sendo elaborada em conformidade com o Regulamento n.º 2/25, de 24 de Junho, da Comissão do Mercado de Capitais (CMC), nomeadamente o Artigo 17.º, n.º 1, alínea e) cópias de segurança (back-ups) como meio informático obrigatório, o Artigo 23.º prazo de conservação de registos, e o Artigo 33.º, n.º 4 — dever de realizar ensaios periódicos dos sistemas de cópias de segurança. A Política observa ainda os deveres de segurança da informação pessoal previstos nos Artigos 30.º e 31.º da Lei n.º 22/11.

Aplica-se a toda a infra-estrutura tecnológica da Inovadora Capital (SDVM), incluindo o ambiente on-premise (servidores de virtualização, controladores de domínio e demais equipamentos próprios), a plataforma de negociação, custódia, compensação e liquidação Bolsa Pro (disponibilizada pela K-Solid – Soluções Tecnológicas) e o ambiente Microsoft 365 (correio electrónico, OneDrive e SharePoint), bem como a todos os colaboradores, prestadores de serviço e sistemas envolvidos na criação, processamento ou armazenamento de informação da Sociedade.

2. Glossário

Termos e Definições	Descrição
Backup [Cópia de Segurança]	Cópia de dados de um dispositivo de armazenamento para outro, permitindo que os mesmos possam ser restaurados em caso de perda dos dados originais.
Backup Completo, Full ou Total	Cópia integral de todos os ficheiros e directórios seleccionados para a média de backup.

Termos e Definições	Descrição
Backup Diferencial	Cópia cumulativa de todos os ficheiros criados ou alterados desde o último backup completo.
Backup Incremental	Cópia apenas dos ficheiros criados ou alterados desde o último backup completo ou incremental.
Snapshot	Imagem instantânea do estado de uma máquina virtual ou volume de dados num determinado momento, utilizada como ponto de restauro.
Período de retenção	Tempo durante o qual os dados de backup ficam guardados, findo o qual são descartados, libertando espaço para novas cópias.
Backup imutável / WORM	Cópia de segurança protegida contra alteração ou eliminação durante o período de retenção definido, mesmo por utilizadores com privilégios administrativos.
Restore / Restauração	Processo de recuperação de dados a partir de uma cópia de segurança, repondo-os no sistema de origem ou num sistema alternativo.
RPO [Recovery Point Objective]	Perda máxima tolerável de dados, medida em tempo, face ao último backup válido.
RTO [Recovery Time Objective]	Tempo máximo tolerável para restaurar um sistema a partir de uma cópia de segurança.
Data Center	Instalação que centraliza as operações e equipamentos de TI de uma organização, bem como o armazenamento, gestão e disseminação dos seus dados.

3. Objectivo

A presente Política tem como objectivo garantir que toda a informação crítica e relevante da Inovadora Capital (SDVM) é copiada, armazenada e protegida de forma adequada, permitindo a sua recuperação em caso de perda, corrupção, eliminação accidental, incidente de segurança ou desastre, minimizando o impacto na continuidade

das actividades da Sociedade e assegurando o cumprimento do Regulamento n.º 2/25, de 24 de Junho, da CMC.

4. Funções e Responsabilidades

- Administração do Topo – Aprovar a presente Política e assegurar a disponibilização dos recursos necessários à sua execução.
- Área de Tecnologia e Sistemas de Informação – Executar, monitorizar e testar as rotinas de backup, gerir o armazenamento das cópias de segurança e conduzir os processos de restauração, sendo a responsável formal pela execução e teste dos backups.
- Gabinete de Auditoria – Testar os controlos associados à presente Política, incluindo a verificação da realização efectiva dos backups e dos respectivos ensaios de restauração.
- Gabinete de Compliance – Verificar a conformidade da Política com as normas vigentes, nomeadamente as emitidas pela CMC.
- Todas as unidades de estrutura – Identificar e comunicar à Área de Tecnologia e Sistemas de Informação os dados e sistemas que consideram críticos para a sua actividade, para efeitos de classificação.

5. Comprometimento

5.1. Comprometimento dos Responsáveis Hierárquicos

- Assegurar que os dados críticos das respectivas áreas estão identificados e comunicados à Área de Tecnologia e Sistemas de Informação para efeitos de inclusão nas rotinas de backup;
- Sensibilizar os colaboradores sob a sua gestão para a correcta utilização dos repositórios de dados sujeitos a backup, evitando o armazenamento de informação crítica fora desses repositórios.

5.2. Comprometimento dos Utilizadores

- Guardar a informação crítica exclusivamente nos directórios de rede, sistemas ou repositórios abrangidos pelas rotinas de backup, evitando o armazenamento local ou em dispositivos amovíveis não autorizados;

- Comunicar prontamente à Área de Tecnologia e Sistemas de Informação qualquer perda, corrupção ou eliminação acidental de dados que necessite de restauração;
- Não desactivar, alterar ou contornar, por qualquer meio, os mecanismos de backup instalados nos equipamentos ou sistemas da Inovadora Capital (SDVM).

5.3. Comprometimento da Área de Tecnologia e Sistemas de Informação

- Administrar, proteger e testar as cópias de segurança dos programas e dados críticos do negócio, nos termos da presente Política;
- Manter actualizado o inventário dos sistemas, servidores e activos de informação sujeitos a backup;
- Configurar e manter os equipamentos e sistemas de backup de acordo com os parâmetros definidos no Capítulo 7;
- Executar e documentar os ensaios periódicos de restauração, nos termos do Artigo 33.º, n.º 4, do Regulamento n.º 2/25, de 24 de Junho, da CMC;
- Monitorizar a execução das rotinas de backup e escalar de imediato qualquer falha detectada;
- Reportar à Administração e ao Gabinete de Compliance os resultados dos testes de restauração e as eventuais deficiências identificadas.

6. Classificação da Informação para Efeitos de Backup

Toda a informação da Inovadora Capital (SDVM) deve ser classificada, para efeitos de backup, de acordo com a sua criticidade para o negócio, nos seguintes níveis:

Classificação	Descrição	Exemplos
Crítica	Informação indispensável à continuidade imediata das actividades de negociação, liquidação e relacionamento com clientes.	Base de dados da plataforma Bolsa Pro (ordens, posições, contas de clientes), registos de auditoria, contabilidade
Relevante	Informação de suporte às actividades operacionais e de controlo interno.	Correio electrónico e documentos no Microsoft 365, sistemas de compliance,

Classificação	Descrição	Exemplos
		documentos de auditoria e de gestão de risco
Padrão	Informação administrativa geral, sem impacto crítico imediato na actividade regulada.	Documentos administrativos, modelos, comunicações internas

7. Tipos e Métodos de Cópias de Segurança

A Inovadora Capital (SDVM) adopta, consoante o ambiente e o sistema em causa, os seguintes tipos de cópias de segurança:

- Backup completo — cópia integral dos dados, realizada com a periodicidade definida no Capítulo 8;
- Backup incremental — cópia apenas dos dados alterados desde o último backup completo ou incremental, reduzindo o tempo e o volume de cada execução;
- Snapshots de máquinas virtuais — pontos de restauro do ambiente de virtualização (VMware vSphere), utilizados como mecanismo complementar de recuperação rápida.

7.1. Ambiente On-Premise

Os servidores e máquinas virtuais geridos internamente pela Inovadora Capital (SDVM), incluindo os controladores de domínio, encontram-se virtualizados em ambiente VMware vSphere e são protegidos pela ferramenta Veeam Backup & Replication, instalada num servidor isolado dedicado exclusivamente a esta função.

Característica	Situação actual
Ferramenta	Veeam Backup & Replication
Versão instalada	13.0.1.180
Local de instalação	Servidor isolado, dedicado exclusivamente ao Veeam Backup & Replication
Estrutura dos jobs	Múltiplos jobs de backup (Backup Job 1 e Backup Job 2), repartindo as máquinas virtuais entre si

Característica	Situação actual
Âmbito de cobertura	Conjunto das máquinas virtuais do ambiente VMware vSphere, incluindo os controladores de domínio VMDCINC002) e servidores aplicacionais (VMINCPRIMAV001 — Primavera)
Local de armazenamento das cópias	No próprio servidor isolado de backup (armazenamento local)
Periodicidade dos jobs	Diária
Notificação e monitorização	Envio automático de relatório por correio electrónico para suporte.tecnico@inovadoracapital.ao após cada execução, com indicação de êxitos, avisos e erros
Retenção configurada	7 dias (confirmado para o Backup Job 2; sem GFS/retenção alargada configurada). Retenção do(s) job(s) adicionais (Backup Job 1" e Backup Job 2).
Cópia adicional	Inexistente — mantida apenas no servidor isolado de backup

A retenção de 7 dias configurada no "Backup Job 2" situa-se abaixo do valor de referência sugerido no Capítulo 8 para dados classificados como críticos (30 dias), pelo que se recomenda a revisão deste parâmetro pela Área de Tecnologia e Sistemas de Informação, tendo em conta a capacidade de armazenamento disponível no repositório (1,37 TB livres de 1,70 TB, à data de 22/08/2026).

7.2. Plataforma Bolsa Pro

A plataforma Bolsa Pro, disponibilizada pela K-Solid – Soluções Tecnológicas, dispõe de mecanismos de cópia de segurança e de recuperação de desastres geridos directamente pelo fornecedor, nos termos do contrato de prestação de serviço, do respectivo Acordo de Nível de Serviço (SLA) e da Documentação Técnica da Solução.

- A base de dados transaccional e o barramento de eventos (Kafka) dispõem de replicação síncrona, com objectivo de ponto de recuperação (RPO) de 5 minutos;
- As cópias de segurança da plataforma são cifradas e replicadas para uma região secundária;

- Os registos de auditoria de todas as operações de negociação, autenticação e administração são mantidos em suporte imutável (WORM), com retenção mínima de 7 anos; sempre que estes registos constituam registos de operações ou de contratos com clientes abrangidos pelo Artigo 23.º do Regulamento n.º 2/25, a respectiva retenção deve ser alargada para 10 anos, nos termos do Capítulo 9 desta Política;
- O fornecedor realiza testes de recuperação de desastres com periodicidade trimestral, incluindo simulação de falha total do centro de dados primário;
- A Área de Tecnologia e Sistemas de Informação deve obter e manter em arquivo evidência documental dos testes de disaster recovery realizados pela K-Solid, nos termos do Artigo 33.º, n.º 4, do Regulamento n.º 2/25, de 24 de Junho, da CMC;
- Deve ser confirmada, junto do fornecedor, a possibilidade de exportação periódica de cópias de segurança para um repositório sob controlo directo da Inovadora Capital (SDVM), como salvaguarda adicional face a uma eventual descontinuidade do serviço.

7.3. Microsoft 365

O correio electrónico corporativo e os documentos armazenados em OneDrive e SharePoint são geridos no ambiente Microsoft 365. Os mecanismos nativos do Microsoft 365 (lixeira, retenção de itens eliminados, versionamento de ficheiros) não constituem, por si só, uma solução de backup completa, apresentando limitações de prazo e de âmbito de recuperação.

- Deve ser implementada uma solução dedicada de cópia de segurança para o Microsoft 365 (por exemplo, através de ferramentas de backup específicas para Exchange Online, OneDrive e SharePoint), independente dos mecanismos nativos de retenção da Microsoft;
- Em alternativa ou em complemento, devem ser configuradas e documentadas as políticas de retenção do Microsoft Purview aplicáveis a correio electrónico e documentos, ajustadas às necessidades de retenção regulatória da Inovadora Capital (SDVM);
- A cópia de segurança do Microsoft 365 deve ser armazenada de forma independente do próprio tenant Microsoft 365.

8. Parâmetros de Backup

Os parâmetros mínimos de frequência e retenção das cópias de segurança, por classificação da informação, são os seguintes:

Sistema / Classificação	Tipo de backup	Frequência mínima	Retenção mínima
Plataforma Bolsa Pro (crítica)	Replicação síncrona + cópia cifrada em região secundária (gerido pela K-Solid)	Contínua (RPO 5 minutos)	7 anos (registos de auditoria, em suporte WORM); 10 anos para registos abrangidos pelo Artigo 23.º — ver Capítulo 9
Microsoft (relevante) 365	Backup dedicado (Exchange Online, OneDrive, SharePoint)	Diária	90 Dias
Servidores on-premise – crítica (Veeam)	Completo semanal + incremental diário	Diária	30 Dias diários +12 cópias mensais (GFS, 1 ano)
Servidores on-premise – relevante (Veeam)	Completo ou diferencial	Diária	14 Dias
Servidores on-premise – padrão (Veeam)	Completo	Diária	14 Dias

9. Retenção Legal de Registos

Em conformidade com o Artigo 23.º do Regulamento n.º 2/25, de 24 de Junho, da CMC, os registos das operações e dos contratos com clientes devem ser conservados pelo prazo mínimo de 10 anos.

- Os períodos operacionais de backup definidos no Capítulo 8 não prejudicam nem substituem este prazo legal de conservação: sempre que uma cópia de segurança integre registos de operações ou de contratos com clientes abrangidos pelo Artigo 23.º, deve ser assegurada a sua disponibilidade e integridade pelo prazo regulamentar de 10 anos, ainda que superior ao período de retenção operacional definido para o respectivo sistema;
- Em particular, a retenção mínima de 7 anos actualmente prevista para os registos de auditoria da plataforma Bolsa Pro (Capítulo 7.2) deve ser alargada para 10 anos relativamente aos registos que constituam registos de operações ou de contratos com clientes, devendo esta extensão ser confirmada e configurada junto da K-Solid – Soluções Tecnológicas;
- A Área de Tecnologia e Sistemas de Informação, em articulação com o Gabinete de Compliance, deve assegurar que os mecanismos de arquivo de longo prazo, distintos das rotinas de backup operacional de curto prazo, garantem o cumprimento deste prazo legal.

10. Armazenamento das Cópias de Segurança

A Inovadora Capital (SDVM) adopta como padrão mínimo a manutenção de cópias de segurança em, pelo menos, 2 suportes ou tecnologias distintas, reduzindo o risco de perda de dados por falha de um único ponto de armazenamento.

- Cópia primária — mantida no ambiente de produção ou no respectivo sistema de backup local (on-premise);
- Segunda cópia — mantida em suporte ou tecnologia distinta da cópia primária, reduzindo o risco de falha simultânea.

No ambiente on-premise, esta segunda cópia ainda não se encontra implementada: as máquinas virtuais são actualmente protegidas por uma única cópia, armazenada no servidor isolado de backup (Veeam Backup & Replication), sem réplica adicional. O Gabinete de Compliance recomendou, no seu parecer de 24 de Agosto de 2026, a implementação prioritária de uma segunda cópia independente, preferencialmente segregada do ambiente principal, como condição para a aprovação definitiva da presente Política.

11. Restauração e Testes

Em cumprimento do Artigo 33.º, n.º 4, do Regulamento n.º 2/25, de 24 de Junho, da CMC, a Área de Tecnologia e Sistemas de Informação deve realizar ensaios periódicos de restauração das cópias de segurança, com uma periodicidade trimestral.

Cada ensaio de restauração deve ser documentado, indicando, pelo menos: data do teste, sistema ou conjunto de dados testado, resultado (sucesso ou falha), tempo de restauração efectivamente alcançado e, quando aplicável, plano de acção para correcção de deficiências identificadas.

Os registos dos ensaios de restauração devem ser mantidos em arquivo e disponibilizados ao Gabinete de Auditoria e à CMC, sempre que solicitados.

12. Segurança das Cópias de Segurança

- As cópias de segurança devem ser cifradas, tanto em repouso como em trânsito, sempre que a solução técnica utilizada o permita;
- O acesso aos repositórios de backup deve ser restrito aos colaboradores da Área de Tecnologia e Sistemas de Informação devidamente autorizados, com registo (log) de todos os acessos;
- As cópias críticas devem, sempre que tecnicamente possível, ser mantidas em regime imutável durante o respectivo período de retenção, de modo a impedir a sua alteração ou eliminação, mesmo por utilizadores com privilégios administrativos;
- O descarte de suportes de backup obsoletos ou fora de uso deve seguir procedimento seguro de eliminação de dados, de modo a impedir a recuperação da informação neles contida.

13. Monitorização e Reporte de Falhas

A execução das rotinas de backup deve ser monitorizada de forma automática, com geração de alertas em caso de falha, atraso ou incompletude de uma cópia de segurança.

- As falhas de backup devem ser analisadas e corrigidas pela Área de Tecnologia e Sistemas de Informação no prazo mais breve possível, não superior a um dia útil, salvo impossibilidade técnica devidamente justificada;
- Falhas recorrentes ou não resolvidas devem ser reportadas à Administração;

- Deve ser mantido um registo histórico das execuções de backup, incluindo êxitos e falhas, para efeitos de auditoria.

14. Penalidades

O não cumprimento da presente Política constitui falta grave, ficando o utilizador que a viole sujeito a acção disciplinar, incluindo o despedimento, e/ou processo civil ou criminal, sem prejuízo das sanções regulatórias aplicáveis pela CMC.

15. Revisão e Gestão Documental

Este documento é válido a partir do momento da sua aprovação, devendo ser revisto com periodicidade não superior a um ano e sempre que se verifiquem alterações que o justifiquem, nomeadamente mudanças na infra-estrutura tecnológica ou na solução de backup utilizada.

O proprietário deste documento é a Área de Tecnologia e Sistemas de Informação, que deve garantir a sua revisão periódica.

- Comunicação interna na organização;
- Formação aos utilizadores;
- Revisão e auditoria periódica da Política;
- Elaboração da documentação de procedimentos técnicos associados.

16. Nota de Propriedade e Distribuição

Este documento é propriedade da Inovadora Capital (SDVM), podendo ser livremente copiado desde que sejam respeitadas as seguintes condições:

- É permitido fazer cópias inalteradas do documento completo ou em partes, desde que esta nota de distribuição seja mantida em todas as cópias, e que a distribuição não tenha fins comerciais;
- Se este documento for distribuído apenas em partes, devem ser incluídas instruções de como obtê-lo por completo;
- É vedada a distribuição de versões modificadas deste documento, bem como a comercialização de cópias, sem a permissão expressa da Inovadora Capital (SDVM).

18. Outorgamento

O Conselho de Administração

Ana Kainda da Silva Cazumbula

Presidente do Conselho de Administração

Márcia Cardoso Teixeira

Administradora Executiva

Edson Fortunato e Silva da Costa

Administrador Executivo

Elaborado por:	Área de Tecnologia e Sistemas de Informação
Aprovado por:	Conselho de Administração
Data de Aprovação:	02/09/2026