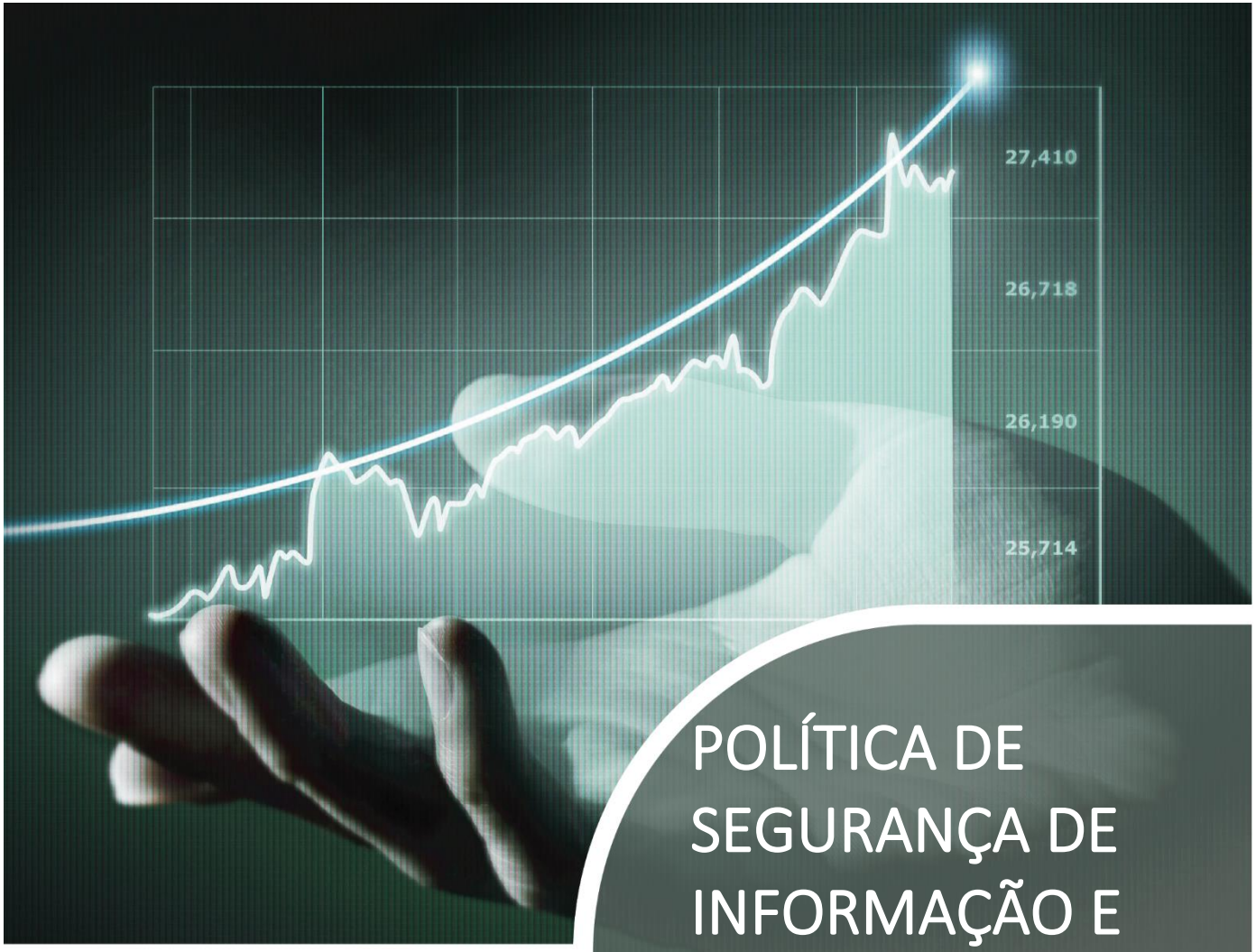

JULHO DE 2023

POLÍTICA DE SEGURANÇA DE INFORMAÇÃO E COMUNICAÇÃO

VERSÃO 1

Resultados SCVM S.A

Resultados SCVM S.A

ÍNDICE

Referência	PLT/RSCVM/SA/23	10/07/2023	versão	01
Responsável	Compliance			
Título	Política de Segurança de Informação e Comunicação			

1. ENQUADRAMENTO

A presente política enquadra-se na Lei nº 22/15 – Código de Valores Mobiliários, Lei nº 14/21 – Regime Geral das Instituições Financeiras, da Lei nº 22/11 de 17 Junho - Protecção de Dados Pessoais, da Lei nº 07/17 de 16 Fevereiro - Protecção das Redes e Sistemas Informáticos, da Lei nº 7/17 de 16 Fevereiro - Protecção das Redes e Sistemas Informáticos o Conselho de Administração, dentro das suas competências e atribuições, implementa a presente Política, como pilar de todo o processo de relacionamento institucional entre os Colaboradores da nossa Instituição, membros do Conselho de Administração, Conselho Fiscal, Partes Relacionadas, Contrapartes e outras partes interessadas.

2. ÂMBITO

A presente política aplica-se a todas as partes relacionadas e interessadas da Resultados SCVM, SA, em todas matérias relacionadas a protecção de dados, sistemas informáticos e informações.

3. DEFINIÇÕES

Segurança Cibernética: conjunto de políticas e controlos, meios e tecnologias que visam proteger programas, computadores, redes e dados de intrusão ilícita ou ataques digitais que provoquem danos aos mesmos.

Computação em Nuvem: modelo que permite o acesso e o fornecimento de forma conveniente e directa a um conjunto de recursos computacionais configuráveis e armazenamento de dados que podem ser rapidamente aprovisionados e acessíveis com o mínimo esforço de gestão ou interacção entre os prestadores de serviços.

Acesso condicionado: sujeição do acesso a um serviço mediante uma assinatura ou qualquer outra forma de autorização individual. Activos de informação: toda a informação com valor para a Organização, incluindo tecnologias de informação, instalações e pessoas que transmitam, armazenam e processam essa informação, independentemente do seu formato.

Resultados SCVM S.A

Cibercrime: crime cometido com recurso aos sistemas electrónicos e novas tecnologias de informação e comunicação.

Incidente de Segurança da Informação: qualquer ocorrência que afecte ou venha a afectar a confidencialidade, integridade e/ou disponibilidade da informação ou das tecnologias de informação, com prejuízo financeiro, reputacional ou operacional para a Corretora, incluindo qualquer acção ou omissão, deliberada ou não, que viole a regulação de segurança e privacidade da informação.

Código de acesso: dados ou senha que permite aceder, no todo ou em parte e sob forma inteligível, a um sistema informático

Segregação de Funções: separação efectiva entre actividades incompatíveis ou conflituantes entre si ou divergentes, visando o controlo no acesso a dados e informação.

Dados: qualquer representação de factos, vídeos, ou imagens, informações ou conceitos, incluindo de programas de computador, que são armazenados, transmitidos ou processados num sistema de informação.

Infraestrutura Tecnológica Crítica: sistemas e activos de informação, sejam físicos, virtuais e vitais para o funcionamento normal das Instituições Financeiras, cuja incapacidade ou destruição acarreta um elevado impacto na operacionalidade das Instituições.

Firewall: dispositivo de rede de computadores, utilizado para aplicar uma política de segurança a um determinado ponto da rede.

Virtual Private Network (VPN): acesso à rede corporativa, que possibilita a conectividade, via internet, de um equipamento externo à rede interna da corporação, provendo funcionalidades e privilégios como se o mesmo estivesse conectado física e diretamente à rede interna. Comumente é utilizado por funcionários em trânsito.

Software: unidade lógica (digital/comunicação), com instruções e dados processados nos servidores e computadores.

Backup: cópia de dados e informações de um dispositivo de armazenamento a outro para que possa ser restaurado em caso da perda dos dados originais, o que pode envolver apagamentos acidentais ou corrupção de dados.

Colaboradores: toda pessoa singular que presta serviços de natureza efectiva à Resultados SCVM, S.A, mediante contrapartidas pecuniárias decorrentes de um contrato de natureza laboral.

Activos: fundos, activos financeiros, recursos económicos ou outros bens de qualquer natureza, corpóreos ou incorpóreos, móveis ou imóveis, tangíveis ou intangíveis, documentos ou outros instrumentos legais que comprovem os direitos os bens relativos.

Due Diligence: procedimento sobre o qual é despoletado um conjunto de acções, preventivas, com vista a verificar e validar o conjunto de informações submetidas pelos

parceiros de negócio, clientes, accionistas e colaboradores da Resultados SCVM S.A, com vista a assegurar a idoneidade destas informações e entidades.

Partes relacionadas: sócios, accionistas com participações qualificadas, entidades pertencentes a grupos económicos, pessoas com relação de cônjuge, descendente ou ascendente, de primeiro e segundo graus, com membros dos órgãos de administração e fiscalização das instituições financeiras, considerados directamente ou como beneficiários últimos das transacções ou dos activos.

4. DIRECTRIZES OPERACIONAIS

No âmbito da presente política, os procedimentos abaixo descritos representam os critérios de segurança de dados e sistemas de informação implementados, de acordo com a dimensão, o perfil de risco, modelo de negócio e das operações da Resultados SCVM S.A, bem como em consideração aos produtos, serviços, actividades e processos, dando primazia ao registo e arquivo de informação.

Os procedimentos e os controlos adoptados permitem reduzir a vulnerabilidade da Resultados SCVM S.A, a incidentes de cibercrimes, com base no quadro regulamentar vigente.

5. ACESSO A DADOS E INFORMAÇÕES

Nos termos da presente política, o acesso aos sistemas e dados da Resultados SCVM S.A, estão condicionados a procedimentos que visam:

i. A autenticação, a autorização, a criptografia, a prevenção e a detecção de intrusão;

ii. A prevenção de fuga de informações;

iii. A realização periódica de testes e auditorias para detecção de vulnerabilidades;

iv. A protecção contra softwares maliciosos;

v. O controlo de acesso e de segmentação da rede de computadores;

vi. A manutenção de cópias de segurança dos dados e das informações;

vii. Controlos específicos para garantir a segurança das informações sensíveis, incluindo de rastreabilidade de informação;

viii. A prestação de informações a clientes e utentes, sobre precauções na utilização de produtos e serviços.

6. PROTECÇÃO DO CIBERESPAÇO

Os procedimentos de implementação da presente política respeitam as regras de protecção ambiental, conferindo uma gestão responsável dos controlos e transacções processadas nos servidores, conferindo confiança aos dados processados e a utilização racional e segura dos servidores e backups (de redes locais, internet, redes de comunicações e dados de computação em nuvem).

7. SEGURANÇA FÍSICA E LÓGICA

Todas as instalações e equipamentos de suporte ao processamento de informações e dados, nos sistemas informação e tecnologias de suporte encontram-se localizados em áreas seguras, protegidos contra situações de catástrofes naturais e cujo acesso encontra-se condicionado a procedimentos de comunicação prévia e autenticação da entidade.

Os critérios de implementação de qualquer tecnologia ou equipamento de suporte estão condicionados a apresentação de um plano de acção ao órgão de gestão, com a descrição detalhada dos objectivos e material ou tecnologia de suporte.

Toda a tecnologia ou material de terceiros só poderá ser utilizada/implementada nos sistemas da Resultados SCVM S.A, após a execução de testes de implementação, integridade e aceitação.

8. CONTROLO DE ACESSOS AOS SISTEMAS

1. Estão implementados procedimentos de controlo e monitorização dos acessos on job e remotos, com base em políticas de encriptação de palavras-passe e definição de privilégios com base nos limites e competências dos colaboradores.

2. O processamento, armazenamento de dados e computação em nuvem é feito com base em políticas de autenticação de acessos.

3. A subcontratação destes serviços fica condicionado a procedimentos de diligência legal, financeira e operacional.

9. CONTINUIDADE DE NEGÓCIOS

A gestão dos dados e sistemas informáticos é concebida com vista a gestão da continuidade das operações Resultados SCVM, SA, em caso de suspensão temporária ou definitiva dos serviços na sede, estando, por isso, implementados procedimentos de redundância e backup de informação, sendo possível continuar e recuperar os dados processados em menos de 24 horas.

Estão previstos, dentro da matriz de gestão dos sistemas da Resultados SCVM, SA, a realização de testes a integridade e fiabilidade dos sistemas, com vista a aferir a capacidade de resposta destes.

Para a implementação do referido processo, a par dos sistemas de suporte digitais, estão criadas equipas compostas por funcionários chave, capazes de dar continuidade as operações e transacções, incluindo um membro da função de auditoria interna, com o objectivo de auxiliar na salvaguarda dos procedimentos de controlo implementados.

10. RESPONSABILIDADES

O asseguramento da implementação e monitorização da presente política é da responsabilidade do Departamento da Sistemas de Informação e comunicação, a quem compete assegurar a aquisição dos equipamentos e softwares relevantes a operação da Resultados SCVM, SA, e verificar o estado e a qualidade dos critérios de segurança cibernética.

Cabe a função de auditoria interna realizar, dentro do apetite ao risco identificado, auditorias e inspecções aos controlos referentes a política de segurança cibernética e de informação e assegurar, no mínimo:

• A existência de uma base de dados sobre os riscos identificados e o devido acompanhamento do seu processo de saneamento.

• A existência de uma base de dados sobre todas as fraudes ocorridas e o processo de saneamento destas.

• Acompanhamento de todas as situações de violação dos princípios de compliance cibernético e prevenção de fraude, denunciados na Resultados SCVM, SA.

• Avaliar a compatibilidade entre os princípios do Código de Ética e Conduta Profissional e à presente política.

11. OBRIGAÇÃO DE NOTIFICAÇÃO DE INCIDENTES

No âmbito da presente política, a Resultados SCVM, SA, obriga-se a:

a. Comunicar a APD (Agência de Protecção de Dados), as violações das redes e dos sistemas de informação ou perdas de integridade com impacto significativo no funcionamento das referidas redes e serviços.

b. Comunicar sobre a detecção de incidentes, com intervalos de 4 horas, até à reposição normal dos serviços

c. Sem prejuízo do dever de sigilo profissional e de livre concorrência, sempre que necessário, a Resultados SCVM, SA, desenvolve iniciativas para a partilha de informações

sobre os incidentes relevantes, visando a mitigação do impacto e reforço da resiliência do mercado a ataques cibernéticos.

12. DÚVIDAS E OMISSÕES

As regras contidas na presente Política não podem estar em conflito com disposições internas e legislação vigente, nomeadamente a legislação financeira, sobre a protecção de dados e sistemas informáticos, laboral e criminal, sendo que, em caso de dúvida, aplica-se a legislação competente.

As dúvidas que surgirem na interpretação e aplicação desta Política serão esclarecidas pela função de Compliance.

13. ENTRADA EM VIGOR

A presente Política entra, imediatamente, em vigor após aprovação e publicação pelo Órgão de Gestão da Resultados SCVM, SA e, sempre que necessário, serão revistos os termos e condições de aplicação da presente política.

Luanda, 10 de Julho de 2023

O Conselho de Administração.

RESULTADOS SOCIEDADE CORRETORA DE VALORES MOBILIÁRIOS, S.A. NIF: 5001164678