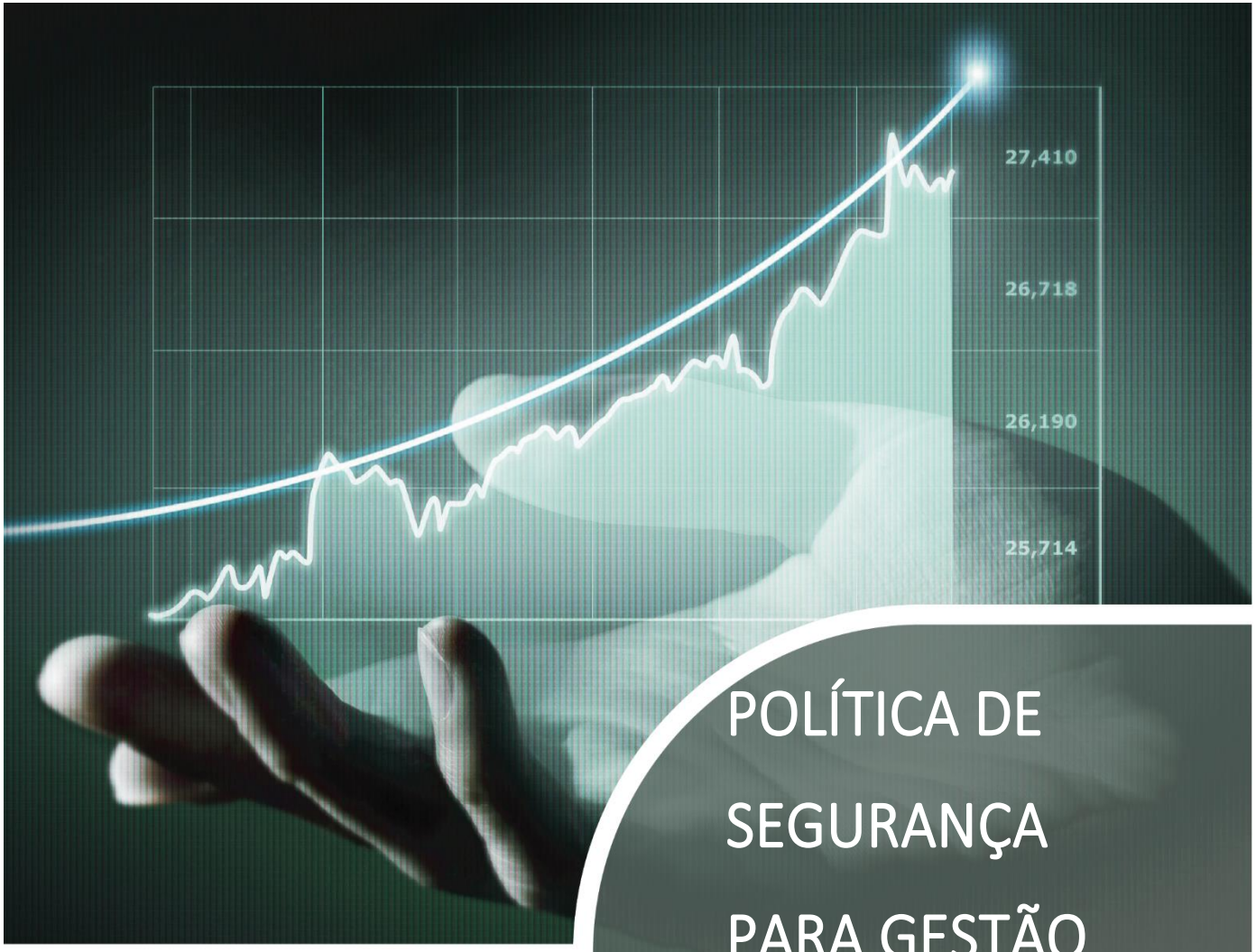

JULHO DE 2023

POLÍTICA DE SEGURANÇA PARA GESTÃO DOCUMENTAL

VERSÃO 1

Resultados SCVM S.A

Índice

Referência	PLT/RSCVM/SA/7	22/07/2023	versão	01
Responsável	Compliance			
Título	POLÍTICA DE SEGURANÇA PARA GESTÃO DOCUMENTAL			

1. OBJECTIVO

Estabelecer os princípios, directrizes e regulamentos que compõem a Política De Segurança Para Gestão Documental, a fim de garantir o tratamento seguro das informações, dos dados e comunicações da RESULTADOS SCVM SA, adiante designada por RESULTADOS ou CORRETORA.

2. ENQUADRAMENTO

A presente política foi elaborada com objectivo de definir directrizes, normas e procedimentos relativo a segurança e tratamento da informação, e tem fundamentação na Lei nº 14/21 de 19 de Maio - Lei Do Regime Geral Das Instituições Financeiras, e no Regulamento n.º 1/15 - Regula o processo de autorização para constituição e de registo dos agentes de intermediação, sem prejuízo de toda e qualquer outra regulamentação em vigor e de documentos legais que suportem essa actividade.

3. DEFINIÇÕES

- Activos: Tudo aquilo que tem valor para a RESULTADOS.
- Activos de informação: Todo e qualquer recurso que processe, manipule, armazene, transporte, transmita, descarte dados e informações que tenham valor para a RESULTADOS e precise ser protegido (por exemplo: computadores, servidores, banco de dados, smartphones, sistemas, ambientes e processos de trabalho, armários e arquivos).
- Autenticidade: Garantia da identificação do responsável por uma determinada acção. Desta forma é possível assegurar o não repúdio quanto a acção executada, onde e quando a mesma foi ocorrida.
- Ciclo de vida da informação: É o ciclo formado desde a criação ou obtenção da informação, passando por seu uso, manipulação, compartilhamento, armazenamento, transporte e descarte.
- Classificação da informação: Processo caracterizado pela definição do grau de sigilo da informação e os grupos de acesso à mesma. Visa assegurar que a informação receba um nível adequado de protecção, conforme seu valor, requisitos legais, sensibilidade e criticidade para a organização.
- Colaborador: Funcionário, associado, estagiário, fornecedor, prestador de serviço, estatutário ou agente económico, que tenha acesso a informações ou recursos da RESULTADOS.
- Comitê Estratégico de Segurança da Informação: Grupo da CORRETORA com a função de actuar como fórum para o debate, troca de informações e tomada de decisões.
- Confidencialidade: Propriedade de que a informação não esteja disponível ou revelada a indivíduos, entidades ou processos não autorizados.
- Disponibilidade: Propriedade de estar acessível e utilizável, sob procura, por uma entidade autorizada, quando necessário.

- Documento: Conjunto de informações ou instruções dispostas de forma ordenada, podendo estar na forma física ou eletrónica. Quando em forma eletrónica é também chamado “Documento Digital”.

- Evento de segurança da informação: Ocorrência identificada de um sistema, serviço ou rede, que indica uma possível violação da política de segurança da informação ou falha de controles, ou uma situação previamente desconhecida, que possa ser relevante para a segurança da informação.

- Gestão documental: Conjunto de procedimentos e operações técnicas referentes à produção, tramitação, uso, avaliação e arquivamento de documentos em fase corrente e intermediaria, visando sua eliminação ou recolhimento para guarda permanente.

- Incidente de segurança da informação: Um simples ou uma série de eventos de segurança da informação indesejados ou inesperados, que tenham uma grande probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação.

- Informação: É o conjunto de dados relacionados entre si que levam à compreensão de algo e que trazem um determinado conhecimento, podendo estar na forma escrita (Documentos), verbal ou de imagem, em meio digital ou físico. É considerada um activo que, como qualquer outro activo importante, é essencial para os negócios de uma organização e consequentemente necessita ser adequadamente protegida.

- Integridade: Garantia de que a informação esteja completa, íntegra e que não tenha sido modificada ou destruída de maneira não autorizada ou acidental durante o seu ciclo de vida.

- Nível de classificação: Categoria a ser definida para cada informação ou classe de informação. Estabelece a sensibilidade da informação em termos da preservação da sua confidencialidade.

- Proprietário da informação: Colaborador responsável por assegurar que as informações e os activos associados com os recursos de processamento da informação estejam adequadamente classificadas, realizando periodicamente análises críticas das classificações e restrições de acesso, levando em conta as políticas de controle de acesso aplicáveis.

- Segurança da informação e comunicações: Garantia de preservação da confidencialidade, disponibilidade, integridade e autenticidade da informação existente em quaisquer formas ou suportes, tais como impressa, armazenada, transmitida por meios físicos, electrónicos, divulgada em meio áudio visual, ou falada em conversação.

- Tratamento da informação: Conjunto de acções referente ao estabelecimento de directrizes de protecção da informação em função do seu nível de classificação,

envolvendo: a produção, recepção, utilização, acesso, reprodução, transporte, transmissão, distribuição, destinação, arquivamento, armazenamento e eliminação da Informação.

- Tratamento seguro da informação: Tratamento levando em consideração os critérios de Disponibilidade, Integridade, Confidencialidade e Autenticidade.

- Usuário: Colaborador autorizado a interagir com a informação. A definição do acesso deve ter como base a necessidade de conhecer a informação para a adequada execução das tarefas inerentes ao seu cargo ou função.

4. COMITÊ ESTRATÉGICO DE SEGURANÇA DA INFORMAÇÃO (CESI)

O Comitê Estratégico de Segurança da Informação da CORRETORA é constituído minimamente por colaboradores nomeados das áreas de Tecnologia da Informação, Jurídico, Capital Humano, Gestão de Riscos, Auditoria Interna e Administração, podendo ainda utilizar especialistas, internos ou externos, para apoiarem nos assuntos que exijam conhecimento técnico específico.

Deverá o CESI reunir-se formalmente pelo menos uma vez a cada doze meses, sendo que reuniões adicionais devem ser realizadas sempre que for necessário deliberar sobre algum incidente grave ou definição relevante para a CORRETORA.

Cabe ao CESI

Propor actualizações do modelo de conservação e arquivo da documentação, revisar e validar os documentos complementares, que tratem da segurança da informação, buscando a melhoria contínua das directrizes sobre segurança da informação na CORRETORA;

- Propor investimentos relacionados à segurança da informação visando a redução de riscos de segurança e conscientização dos colaboradores;
- Decidir sobre os incidentes de segurança, reportados pelo responsável de arquivos;
- Prestar suporte na elaboração de documentos complementares a esta Política, sobre classificação, guarda e manutenção da informação;
- Definir as medidas cabíveis nos casos de descumprimento da política;
- Difundir a cultura de Segurança da Informação na empresa.
- Aprovar a política de Segurança para gestão documental da CORRETORA;
- Prover os recursos humanos, materiais e financeiros necessários à segurança da informação e comunicações;

- Acompanhar periodicamente a evolução dos indicadores e resultados de segurança da informação, podendo ainda utilizar especialistas, internos ou externos, para apoiarem nos assuntos que exijam conhecimento técnico específico.

O Responsável de Segurança da Informação será responsável por:

- Responder, perante a Administração, por todos os aspectos de segurança e gestão de riscos da empresa em relação à Segurança das Informações;
- Responder por todos os eventos de segurança da informação (físicos ou electrónicos) e todas as perdas resultantes dos riscos não geridos ou não previstos;
- Liderar a elaboração da Política Corporativa de Segurança para gestão documental, bem como os anexos necessários para a adequação dos activos ao nível de Segurança pertinente ao bom desenvolvimento do negócio;
- Buscar e apoiar iniciativas de Segurança e gestão documental aplicáveis a toda a CORRETORA, como, por exemplo, o programa de conscientização de segurança, Governança da informação e gestão de identidades digitais;
- Garantir que a segurança seja parte do processo de planejamento da informação;
- Apoiar e validar as auditorias externas de Segurança da Informação realizadas por clientes ou órgãos reguladores;
- Manter contactos apropriados com autoridades relevantes, grupos de interesses especiais ou outros fóruns especializados de segurança da informação e associações profissionais;
- Coordenar as reuniões de trabalho do grupo técnico/operacional no tratamento de incidentes de segurança;
- Avaliar os incidentes de segurança da informação e propor acções correctivas, incluindo o direccionamento dos mesmos para o Comitê Estratégico de Segurança da Informação, quando aplicável;
- Assegurar que política de Segurança para gestão documental, regulamentos e procedimentos da CORRETORA sejam implantadas e mantidas de acordo com os preceitos definidos para sua área de actuação.

Os Colaboradores são responsáveis por:

Conhecer e cumprir as directrizes estabelecidas nesta política, bem como as boas práticas que contribuem para a segurança da informação e comunicações da CORRETORA.

Administrar os recursos, processos de negócios e informações sob sua responsabilidade conforme as directrizes desta política.

4.1. PRINCÍPIOS DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES

As acções de Segurança da Informação e Comunicações da RESULTADOS são norteadas pelos seguintes princípios:

- Alinhamento estratégico: deve haver um alinhamento entre a política, regulamentos e acções de Segurança da Informação e Comunicações da CORRETORA com a missão da Instituição e seu planejamento estratégico.
- Diversidade organizacional: a elaboração de regulamentos, controles e da Política da CORRETORA deve levar em consideração a diversidade das actividades da Empresa, respeitando a natureza e finalidade de cada Unidade Organizacional.
- Propriedade da informação: toda informação produzida ou armazenada na CORRETORA é de sua propriedade e não de seus Prestadores de Serviço, devendo seu uso ser destinado, exclusivamente, a atender os interesses da CORRETORA.

4.2. DIRECTRIZES DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES.

Para fins desta política ficam estabelecidas as seguintes directrizes gerais:

- A Segurança para gestão documental da CORRETORA deve ser apoiada por um Sistema de Gestão da Segurança da Informação e Comunicações (SGSI).
- Devem ser definidas métricas e indicadores que permitam controlar, auditar e elevar o nível de maturidade e conformidade da CORRETORA em segurança da informação.
- Comprometimento: Prestadores de Serviço da CORRETORA em qualquer vínculo, função ou nível hierárquico, são responsáveis pela protecção e salvaguarda dos activos tecnológicos e informações de que sejam usuários, dos ambientes físicos e computacionais a que tenham acesso, respeitando as políticas e mecanismos de controle e protecção implantados.
- Gestão de Riscos: Todos os processos, produtos e serviços desenvolvidos, que possam comprometer a segurança da informação, devem ser submetidos a um processo formal de análise, avaliação e tratamento de riscos, antes da sua aquisição, implementação e disponibilização, visando atingir o grau de segurança adequado para a CORRETORA.

- Gestão de Continuidade de Negócio: A CORRETORA deve estabelecer um conjunto de estratégias e planos de acção documentados, testados e revisados periodicamente, de maneira a garantir que os seus serviços essenciais sejam devidamente identificados, preservados e entregues, mesmo diante da ocorrência de um desastre até o retorno à situação normal de funcionamento da CORRETORA.
- Classificação e Tratamento da Informação: Todas as informações e os respectivos recursos tecnológicos que as suportam devem ser classificadas de acordo com seu grau de sigilo e receber o devido tratamento para assegurar sua protecção durante todo o ciclo de vida.
- Gestão de Acessos: O acesso aos ambientes físicos e tecnológicos da CORRETORA deve ser controlado, registrado e monitorado, com base nos princípios da necessidade de conhecer e do privilégio mínimo para o desempenho das actividades profissionais.
- Gestão de Incidentes: Os Colaboradores, e Prestadores de serviço da CORRETORA têm a obrigação de reportar imediatamente quaisquer incidentes de segurança a informação ou documentação que tomaram conhecimento, de modo que possam ser registados, avaliados e tratados.
- Auditoria e Conformidade: A CORRETORA reserva-se o direito de auditar periodicamente a prática de segurança da informação e comunicações, de forma a avaliar a conformidade das acções de seus Colaboradores e Prestadores de serviço em relação ao estabelecido pela Política de Segurança para Gestão documental da Informação da Empresa e pela legislação aplicável.
- Monitoramento: A CORRETORA reserva-se o direito de monitorar o acesso e utilização de seus ambientes físicos, assim como dos ambientes, equipamentos e sistemas tecnológicos, documentações produzidas por todos que nele actuam, de forma que acções indesejáveis ou não autorizadas sejam detectadas proactivamente.
- Treinamento e Conscientização: Todos os Colaboradores e Prestadores de serviço devem conhecer esta política e serem capacitados anualmente por meio de campanhas de conscientização e treinamentos de acordo com suas funções. Devem assinar o respectivo termo de aceite, garantindo assim maior efectividade e eficácia das acções de segurança para gestão documental na CORRETORA.
- Gestão de exceções/procedimentos de escalação: As necessidades válidas da CORRETORA decorrentes das suas operações podem eventualmente conflitar com algumas directrizes estabelecidas nesta política. Os procedimentos de gestão de exceções reconhecem que os conflitos de políticas são naturais e que a Empresa tem maturidade suficiente para poder geri-los. Ao estabelecer procedimentos de gestão de exceções, os colaboradores são encorajados a trabalhar com o sistema em vez de contorná-lo. Os responsáveis das áreas deverão ser consultados sobre os casos omissos para que sejam estabelecidos novos procedimentos para adequar as exceções.
- Gestão de Mudanças: O Gerenciamento de Mudança deve garantir que os métodos e procedimentos sejam aplicados de forma correcta para avaliar, aprovar, implantar e revisar todas as mudanças de acordo com o escopo estabelecido, de maneira eficiente, a fim de minimizar o risco e o potencial

impacto de tais mudanças para o negócio. Os processos e controles estabelecidos devem permitir a rastreabilidade das mudanças ocorridas em ambientes críticos da CORRETORA.

- Desenvolvimento Seguro: As aplicações desenvolvidas ou adquiridas pela CORRETORA, devem em todo o ciclo de desenvolvimento de sistemas utilizar metodologias que garantam a segurança das informações.
- A CORRETORA respeita a confidencialidade dos dados pessoais e toda a documentação dos seus colaboradores e clientes (tais como registros pessoais, fotografias e local de residência).
- Apenas os dados necessários ou legalmente exigidos para o desempenho eficaz da CORRETORA e cumprimento de obrigações legais são solicitados e retidos ou eventualmente divulgados em atendimento à legislação especifica.
- A CORRETORA se reserva o direito de monitorar o uso de computadores, telefones fixos, smartphones, tablets, celulares, e outros equipamentos disponibilizados e actividades de rede, incluindo, mas não se limitando a e-mail, correio de voz, uso da Internet e de qualquer informação armazenada em tais equipamentos, sistemas ou servidores, em circunstâncias apropriadas e com vista à protecção das informações e da segurança do tráfego de informação e conteúdo.

5. DEVER DE ARQUIVO

O arquivo pode ser substituído por processos de microfilmagem ou por qualquer outro processo tecnológico, nos termos a estabelecer pelo Organismo de Supervisão.

A CORRETORA compromete-se a cumprir as normas e orientações do Organismo de Supervisão quanto ao grau de exigência dos documentos e elementos e serem conservados.

6. PRAZO

A CORRETORA deverá manter em arquivo os documentos e registos referentes a:

a) Operações sobre instrumentos financeiros, pelo prazo de 10 (dez) anos após a realização da operação;

b) Contractos de prestação de serviços celebrados com os clientes ou os documentos de onde constam as condições com base as quais a CORRETORA presta serviços ao cliente, até que tenham decorrido 5 (cinco) anos após o termo da relação de clientela.

A CORRETORA deverá emitir certificados dos registos respeitantes às operações em que intervieram a pedido da CMC, bem como dos seus clientes.

Os Arquivos da Corretora são armazenados em duas formas, física e digital, sendo que a parte física conta com uma zona específica para arquivos e a digital em pasta de redes e nuvens cujo acessos são mediante autorização e permissões.

7. SUPORTE DOS REGISTOS

Os registos da CORRETORA serão conservados em suporte que permita o armazenamento de informação de forma acessível para consulta e de modo que:

a) Permita reconstituir cada uma das fases essenciais do tratamento de todas as operações;

b) Permita verificar quaisquer correcções ou outras alterações, bem como o conteúdo dos registos antes dessas correcções ou alterações;

c) Não permita manipular ou alterar de qualquer forma os registos.

8. APROVAÇÕES, REVISÕES E ANALISES CRÍTICAS

O conjunto de documentos que compõem a Política de Segurança para Gestão Documental deve passar por revisões anuais e análises críticas periódicas, ou sempre que ocorrer fato ou evento relevante que motive sua revisão antecipada.

9.VIOLAÇÕES DA POLÍTICA

Em caso de violação desta Política, a área de Segurança da Informação deve ser imediatamente notificada e em segunda instância o Comité Estratégico de Segurança da Informação.

O descumprimento das directrizes previstas nesta Política é passível de sanções administrativas, conforme regimento interno da área de Capital Humano, e legais, conforme legislação vigente.

ENTRADA EM VIGOR

A presente Política vigora a partir da data da sua publicação, podendo ser actualizada com base nas modificações inerentes a novos serviços, novas ameaças e alterações na Política Interna da RESULTADOS.

Luanda aos 22 de Julho de 2023.

Pelo Conselho de Administração.

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