

DISTRIBUIDORA VALOR, S.D.V.M. (SU),S.A. Política					
Refª:	PL08	Versão:	2.0	Entrada em Vigor:	11-12-2023
Título:	Política de Segurança de Informação e Gestão Documental				
Processo Associado:	Indefinido				

Sumário

A presente Ordem de Serviço institui a Política de Segurança para a Gestão Documental da Distribuidora Valor, S.D.V.M. (SU), S.A. (Distribuidora Valor ou Distribuidora), no seguimento do estabelecido na regumanetação em vigor.

Alterações a versão anterior:

12.11.2024 - Adequação da Política, substituindo a denominação Corretora Valor - SCVM, (SU) S.A. por Distribuidora Valor - SDVM, (SU) S.A., em consequência da aprovação do processo de registo especial da Distribuidora Valor, S.D.V.M. (SU), S.A.

Documento atribuído a:

Conselho de Administração e Gabinete de Informática

Emitente(s)

Distribuidora Valor, S.D.V.M. (SU), S.A.

Índice

1. ÂMBITO E OBJECTIVO.....	2
2. RESPONSABILIDADES.....	2
3. ACESSO RESTRITO À COLABORADORES NÃO AUTORIZADOS	2
4. NÍVEIS DE ACESSO À INFORMAÇÃO E PROTECÇÃO DA INFRAESTRUTURA	3
5. SISTEMAS APLICATIVOS OU SOFTWARES INFORMÁTICOS E LOG OU HISTÓRICOS DE ACESSOS	3
5. DA GESTÃO DOCUMENTAL	5
6. COMPETÊNCIA PARA GESTÃO DOCUMENTAL	5
7. MODELO	5
8. TIPOLOGIA DE DOCUMENTOS	6
9. ACTUALIZAÇÃO	9

1. ÂMBITO E OBJECTIVO

A presente política resulta da obrigação regulamentar que incide sobre as instituições financeiras de implementar e manter políticas de segurança de informação nos seus regulamentos internos.

A presente política aplica-se a todos os aplicativos da Distribuidora, independentemente de se tratarem de aplicativos de abertura e movimentação de contas, contratação de operações e prestação de serviços aos clientes, custódia de títulos, os procedimentos e níveis de intervenção na elaboração, registo e controlo de documentos, estabelecendo os princípios de funcionamento da gestão documental e as regras para publicação dos documentos na pasta de normativos internos. Em suma estão afectos à presente política todos os aplicativos em utilização na Distribuidora para efeitos da sua realização enquanto instituição, bem como todas infraestruturas de rede da Distribuidora.

A política tem como objectivo definir as diretrizes que norteiam a elaboração das normas e padrões que tratam da protecção das informações detidas pela Distribuidora, abrangendo sua utilização, armazenamento, distribuição, confidencialidade, disponibilidade e integridade, bem como estabelecer os requisitos de:

- Autorização de acessos de colaboradores;
- Níveis de acesso claramente definidos, de acordo com a categoria dos trabalhadores que permitam aceder, modificar e/ou destruir a informação;
- Registo histórico que permita identificar quem teve acesso e/ou modificou a informação.

2. RESPONSABILIDADES

Todos os colaboradores são responsáveis por manter a segurança das informações sob sua ~~responsabilidade~~, posse ou guarda, assim como garantir o cumprimento desta Política e das demais normas da Distribuidora e da regulamentação aplicável.

3. ACESSO RESTRITO À COLABORADORES NÃO AUTORIZADOS

A informação sob custódia da Distribuidora, mesmo que pertencente à clientes ou fornecedores, é protegida contra o acesso de pessoas (colaboradores) não autorizadas.

A utilização de informação, destruição, armazenamento, manutenção e distribuição são feitos de acordo com as necessidades da Distribuidora nos termos da regulamentação. Estes processos devem estar devidamente documentados e serem passíveis de monitoração e auditoria.

Devem ser usados somente recursos autorizados ou equipamentos para garantir o compartilhamento seguro da informação, quando for necessário, além da identificação das pessoas que possuem acesso às informações confidenciais.

A informação custodiada pela Distribuidora é armazenada, pelo tempo determinado pela regulamentação ou legislação vigente. A Informação é protegida por backups e recuperável quando necessário. O local de armazenamento das informações deve ser apropriado e protegido contra sinistros e acessos de pessoas não autorizadas.

Para efeitos de segurança da informação, o Backups da Distribuidora deve ser situado em localização distinta da informação principal, no sentido do serem salvaguardados os riscos de inundação, vandalismo, incêndios que possam ocorrer em determinadas localidades geográficas.

Na sua estrutura, a Distribuidora adota mecanismos de acesso aos espaços da Distribuidora através de cartões de acesso, sendo por isso atribuído a cada colaboradores acesso específicos as estruturas da Distribuidora que sejam inerentes às suas funções.

4. NÍVEIS DE ACESSO À INFORMAÇÃO E PROTEÇÃO DA INFRAESTRUTURA

A Distribuidora tem definidos os níveis de acesso de acordo com o a categoria/funções dos colaboradores, tendo em conta as tarefas a serem desenvolvidas pelo colaborador, estando apenas disponível a informação para efeitos de desempenho das suas funções.

As redes externas de comunicação (Internet, redes privadas, etc.) devem ser monitorizadas através de Servidores de Firewalls, Servidores de Acesso à Internet, Servidores de AntiSpam, ferramentas ou softwares de Antivírus.

Devem ser realizados testes nos sistemas e dispositivos de rede e de segurança que visem identificar vulnerabilidades conhecidas, sendo que para os sistemas e dispositivos expostos à internet os testes devem ocorrer com frequência semanal.

A Distribuidora adota procedimentos que garantam o controle e a integridade dos dados e a legitimidade da informação.

A Distribuidora adota todas as medidas de segurança para proteção da sua infraestrutura de rede e software ou aplicativos informáticos, como ataques cibernéticos ou hackeamento.

5. SISTEMAS APLICATIVOS OU SOFTWARES INFORMÁTICOS E LOG OU HISTÓRICOS DE ACESSOS

Os aplicativos desenvolvidos pela área de desenvolvimento da Distribuidora e que se encontrem em produção devem ser documentados e controlados quanto às alterações ou correções feitas, com trilhas do que foi feito e guarda segura da biblioteca de fontes. Toda informação necessária para eventual reconstrução dos aplicativos deve constar de sua documentação.

Os aplicativos ou softwares desenvolvidos fora área de desenvolvimento da Distribuidora, ou seja, aqueles que a Distribuidora adquiriu uma licença de uso, devem ter a biblioteca de fontes e de recursos adicionais (bibliotecas adquiridas, componentes, etc.) monitorizada pela Distribuidora ou por entidade terceira contratada para o efeito. Tais fontes devem sempre ser atualizadas e verificadas quanto a sua validade e sincronização com a versão em uso no ambiente de produção.

O mau uso dos sistemas, feito de forma accidental ou deliberada, deve ser combatido pela segregação das funções de administração do sistema das funções de execução de certas actividades, ou entre áreas de responsabilidade. Tal segregação de funções visa criar controles para evitar fraudes ou conluios no desempenho de actividades críticas do sistema.

Quando for impraticável implantar a segregação, outros controles devem ser considerados, tais como o monitoramento das actividades, trilhas de auditoria e acompanhamento gerencial.

Os *software* e aplicativos em uso na Distribuidora, que tratam ou processem informação confidencial ou de elevado grau de criticidade devem ter *logs* diários, sobre todos utilizador. Nos respectivos *logs*, são registados os acesso que determinado utilizar efectou, todas actividades desempenhadas na aplicação pelo respectivo utilizador, em termos de quais informação acessou, qual informação mudou ou alterou, eliminou, trocou, substituiu, aprovou, cancelou, etc., entre outras actividades relevantes desenvolvidas pelos utilizadores.

Importa referir que o registo de *log* deve ser feito em todos os *user* e para todos *log in* ou início de sessão que o utilizador venha a realizar.

Para novos sistemas ou *softwares*, os requisitos operacionais devem ser documentados e testados antes da sua aceitação e uso.

Para sistemas já em uso devem ser feitas projeções da demanda de recursos e da carga da máquina futura a fim de reduzir o risco de indisponibilidade por sobrecarga (Capacity Planning) no decorrer da sua utilização.

Senhas de colaboradores

As senhas ou palavras passe para acesso aos aplicativos devem ser complexas e possuir quantidade de caracteres suficientes para que dificulte a quebra das mesmas, combinando entre Maiúsculas, Minúsculas e Caracteres Especiais.

Todos o softwares de processamento de operações ou softwares considerados críticos em termos de informação confidencial que processam, devem exigir a actualização de password no mínimo de 90 dias desde a última actualização da palavra passe/password.

Os softwares e aplicativos informáticos devem automaticamente bloquear o acesso aos utilizadores que introduzem três (3) vezes incorrectamente a respectiva palavra passe.

É Permitido o *resert* de palavras de passe de acesso dos colaboradores para execicio das suas actividades, mediante solicitação dos mesmos e sempre que as mesma forem perdidas ou bloqueadas.

Senha ou Palavras passe de Clientes

A Distribuidora adopta mecanismo de protecção de *reserts* de palavras passes de acesso à portais de realização de consulta ou realização de transacções na posição de ordenantes/clientes.

Excepcionalmente e, sempre que solicitado nos canais oficiais, a Distribuidora pode proceder aos desbloqueios de palavras passe de portais de realização de consultas ou transacções.

Contudo, por razões de segurança, nenhuma palavra passe de portais com acesso a realizar transacções pode ser reactivada ou desbloqueada mais de uma (1) vez por semana e três (3) vezes por mês. As contas e login de cliente com solicitações que ultrapassem o estabelecido acima devem ser suspensas e só podem ser reactivadas após contacto directo com o cliente ou presença do cliente nas instalações da Distribuidora para efeitos da correcta identificação.

5. DA GESTÃO DOCUMENTAL

Todos os aspectos de segurança da informação vertidos acima, contribuem para uma gestão documental eficiente da Distribuidora Valor.

Todos os suportes originais que contenham informações úteis ou evidências de interações relevantes, deverão ser arquivados e controlados por forma a poderem ser localizados e acedidos sempre que necessário.

As regras relativas aos registos em suporte informático e aos procedimentos associados à protecção e recuperação de registos, serão da responsabilidade do Gabinete de Informática.

6. COMPETÊNCIA PARA GESTÃO DOCUMENTAL

Na Distribuidora Valor, a Gestão Documental é da responsabilidade das diversas unidades orgânicas, sob coordenação da Direcção de Compliance.

- Unidade responsável por assegurar a divulgação pela Distribuidora da regulamentação emanada da Comissão Executiva é o Gabinete Jurídico;
- A Unidade responsável por assegurar a divulgação pela Distribuidora das alterações legislativas, demais regulamentação de carácter corporativo e da regulamentação que incida sobre a actividade corrente da instituição, é do Gabinete Jurídico;
- A Unidade responsável por assegurar a análise das alterações legislativas e suas implicações para a Distribuidora em matéria de processos e produtos, sugerindo às Unidades Orgânicas as alterações que a análise da nova legislação impuser, assegurando também a supervisão global da conformidade da organização com os requisitos legais e normativos, é do Gabinete de *Compliance*;

7. MODELO

No sentido de garantir a organização e a imagem nos actos internos da Distribuidora que dê origem a algum dos documentos tipificados, bem como, para efeitos de consolidação de todo

acervo documental da Distribuidora, os documentos estabelecidos pela presente política devem apresentar ainda os seguintes aspectos gerais:

7.1 TIPO DE LETRA E TAMANHO

Todos os documentos controlados ou tipificados na presente ordem de serviço devem ser redigidos com o estilo de letra “Trebuchet MS”, tamanho 11, tanto para palavras maiúsculas como para as minúsculas. Excepcionalmente, pode-se usar tamanho diferente do referido acima, em caso de preenchimento de tabelas/quadros ou em notas de rodapé.

7.2 USO DE LETRAS MAIÚSCULAS, NEGRITADAS, SUBLINHADAS, ITÁLICO E ASPAS

Apenas é permitido o uso de maiúsculas nos títulos, nos capítulos, nos artigos, nos temas e subtemas. O disposto anteriormente é aplicável ao uso de palavras em Negrito (N) e Sublinhadas (S).

O uso do itálico (i) e das aspas (“”) deve preferencialmente cingir-se às palavras estrangeiras. Excepcionalmente, podem essas duas funções serem utilizadas em números, ou seja, nos textos numéricos, quando a estrutura ou organização do documento exigir uma diferenciação da parte numérica do texto relativamente ao restante conteúdo.

8. TIPOLOGIA DE DOCUMENTOS

1ª - Regulamento

Sigla: RG

Âmbito: Utilizável para regular os órgãos colectivo da Distribuidora (Comissões, Comitês e Conselhos). Obrigatório a articulação/articulados na sua elaboração.

Hierarquia: Documento superior a todos os outros emitido pelo C.A.

2ª - Estatutos Orgânico

Sigla: EO

Âmbito: utilizável para definir as atribuições, competências, linhas de reportes e Dependência Hierárquica, estrutura das Unidades Orgânicas da Distribuidora, criadas pelo Conselho de Administração (Direcções, TaskForce, Núcleos, Áreas), Facultativo o uso de articulação, mas não recomendada.

Hierarquia: Documento imediatamente inferior ao RG em ao de conflitos de disposição.

3ª - Política

Sigla: PL

Âmbito: utilizável para definir as linhas mestras de actuação da Distribuidora sobre determinada(s) matérias. É permitida o uso de articulação.

Hierarquia: Documento imediatamente inferior ao RG e ao EO em caso de conflitos de disposição.

4ª - Normas de Procedimentos

Sigla: NP

Âmbito: utilizável para definir os circuitos, actos para a realização de actividades, tais como, realização de transferências sobre o estrangeiro, abertura de contas, etc. Não é permitida o uso de articulação, sendo obrigatório a definição dos processos e actos de forma sequencial.

Hierarquia: Documento imediatamente inferior ao RG e ao EO em ao de conflitos de disposição.

5ª - Circulares / Comunicados

Sigla: CIRC / COMUN

Âmbito: utilizável para difundir informações aos colaboradores que devam tomar conhecimento de determinada matéria, acto ou facto.

6ª - Despachos

Sigla: DPC

Âmbito: utilizável para tomada de decisão dos Órgãos de Administração sobre propostas advindas das demais unidades orgânicas.

7.ª - Manual do Produto

Sigla: MP

Âmbito: Definição do Produto ou Serviço e das suas características comerciais no repositório da Distribuidora (ex. intranet/pasta documentação) assegurando que o utilizador final fica habilitado a fazer a sua venda.

Considera-se o MP o conjunto de informação existente na área de Produtos divulgado no repositório/pasta de documentação, para as diversas Redes.

8.^a - Manual de Campanha

Sigla: MC

Âmbito: Sistematização de informação associada a uma campanha específica e considerada relevante à execução da mesma.

9.^a - Impressos

Siglas: T | M |

Âmbito: Documento pré-formatado para recolha de dados num circuito definido com vista à formalização de operações ou realização de actividades interdepartamentais.

Modalidade:

- a) Template - Impresso de circulação interna;
- b) Minuta - Impresso de circulação interna/externa;
- c) Formulários - Impresso de circulação externa.

10.^a Protocolos

Siglas: PT

Âmbito: Identificação das condições especiais de preço ou de remuneração bem como de acesso a produtos e serviços, que são atribuídas a universos restritos de clientes, por força da celebração de Protocolos e/ou Acordos Comerciais e/ou Contratos entre a Distribuidora e entidades externas.

11.^a - Publicações para Clientes

Siglas: CG - Condições Gerais | CE - Condições Especiais | FTI - Fichas técnicas | MT - Manual Técnico

Âmbito: Documentos de diferentes características elaborados por:

- (1) - Imposição legal ou normativa, obedecendo a conteúdos predefinidos e que devem, obrigatória ou facultativamente ser disponibilizados aos Clientes em determinadas interações comerciais na sua relação;
- (2) Por decisão comercial, visando uma melhor identificação e clarificação das características de um produto / serviço (p ex. apresentações comerciais para clientes utilizadas na dinamização da venda).

9. ACTUALIZAÇÃO

O Conselho de Administração e o Gabinete de Informática são encarregues de garantir a permanente actualização da presente política, sem prejuízo das diligências do Gabinete de *Compliance* de garantir que os normativos estejam sempre alinhados com a regulamentação e melhores práticas.

Documentos revogados

N/A

Documentos complementares

- Lei da Protecção de Dados Pessoais (Lei n.º 22/11, de 17 de Junho)
- Plano de Continuidade de Negócios - Distribuidora Valor
- Código de Governo Societário da Distribuidora Valor

Elaborado por: Gabinete de *Compliance*

- O Conselho de Administração -
DISTRIBUIDORA VALOR, S.D.V.M. (SU), S.A.