DISTRIBUIDORA VALOR – S.D.V.M. (SU), S.A POLÍTICA					
Refª:	OS04	**Versão:**	3.0	**Entrada em Vigor:**	09-04-2026
Título:	Plano de Continuidade de Negócios – Distribuidora Valor				
Processo Associado:	Indefinido				

Sumário

Institui o Plano de Continuidade de Negócios da Distribuidora Valor

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.

09.04.2026 – Adicção do Ponto 12 sobre a componete do disaster recovery.

Documento atribuído a:

Gabinete de Gestão de Risco
Gabinete de Sistemas de Informação

Emitente(s)

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

Índice

1. ENQUADRAMENTO

1.1. A gestão da continuidade de negócio compreende o conjunto integrado de políticas e procedimentos que visam assegurar o funcionamento contínuo da Distribuidora, ou a recuperação atempada da sua actividade, no caso de ocorrência de eventos suscetíveis de desestabilizar o normal desenvolvimento do negócio, nomeadamente por implicarem a indisponibilidade das infraestruturas físicas, dos sistemas informáticos ou dos recursos humanos, de forma isolada ou em simultâneo. Este tipo de eventos abrange, entre outros, cenários como catástrofes naturais, pandemias, actos de terrorismo, falhas nos sistemas informáticos, incêndios, inundações ou falhas graves de energia.

1.2. Neste sentido a Distribuidora institui o presente plano de continuidade de negócio de forma a assegurar o funcionamento contínuo do seu negócio, e/ou a sua recuperação atempada, no caso de ocorrência de eventos suscetíveis de perturbar o seu normal funcionamento, tais como catástrofes naturais, pandemias, actos de terrorismo, falhas nos sistemas informáticos, incêndios, inundações ou falhas graves de energia

1.3. O PCN ora definido encontra-se ajustado às especificidades da Distribuidora e reflete os principais riscos que este se encontra exposto, bem como as vulnerabilidades inerentes ao seu negócio, estrutura organizativa, características das infraestruturas físicas, simplementação geográfica, entre outros aspetos.

2. CONTEXTO REGULAMENTAR

2.1. O presente plano resulta das obrigações regulamentares vertidas nos seguintes diplomas:

> Regulamento n.º 2/25, de 24 de Junho | Comissão de Mercado de Capitais | Agentes de Intermediação e Serviços de Investimento (alínea g do n.º 1 do artigo 10.º) estabelece que os agentes de intermediação devem adoptar uma política de continuidade das suas actividades, destinada a garantir, no caso de uma interrupção dos seus sistemas e procedimentos, a preservação de dados e funções essenciais e a prossecução dos seus serviços e actividades de investimento ou, se tal não for possível, a recuperação rápida desses dados e funções e o reatamento imediato dessas actividades.

3. ÂMBITO

3.1. O presente plano de continuidade de negócios, visa garantir que no caso de uma interrupção dos seus sistemas e procedimentos, a preservação de dados e funções essenciais e a prossecução dos seus serviços e actividades, bem como garantir a recuperação rápida desses dados e funções e o reinício rápido dessas actividades.

3.2. Plano de Continuidade que visa também, atender a uma série de situações projectadas que possam comprometer a prestação de serviços. Neste sentido, tem por objectivo garantir que a Distribuidora tem preparada as condições para continuar a oferecer seus serviços em situações de incidentes ou desastres que possam afetar sua infraestrutura técnica e física.

3.3. O presente plano não abrange o conceito de gestão de crises financeiras. Em geral, uma crise financeira – embora configure igualmente uma circunstância excepcional, susceptível de colocar em causa a sobrevivência da instituição, requer uma planificação de natureza distinta daquela que é exigida para as situações de desastre operacional.

3.4. O PCN abrange toda a organização e deverá ser do conhecimento dos colaboradores a eles respeitantes, de cumprimento obrigatório por todos.

4. OBJECTIVO

4.1. A gestão da continuidade de negócio tem como objectivo identificar as ameaças e os riscos a que a Distribuidora se encontra sujeita, analisar os impactos no negócio, caso essas ameaças se concretizem e tornar possível que o seu funcionamento alcance um nível aceitável no caso de ocorrência de eventos que perturbam o normal funcionamento do negócio, resguardando os interesses dos intervenientes, bem como a reputação da instituição e a respectiva actividade.

5. BENEFÍCIO DO PLANO DE CONTINUIDADE DO NEGÓCIO

5.1. A Adopção do plano de continuidade de negócios é imprescindível para assegurar a resiliência das instituições, e garante o seguinte:

a) Identificação de processos críticos e do impacto da roptura em todo a Distribuidora;
b) Conhecimento do grau de exposição ao risco de eventos adversos susceptíveis de causar uma interrupção na actividade da Distribuidora;
c) Resposta eficiente às interrupções;
d) Preservação da reputação da instituição; e
e) Mitigação de possíveis impactos às partes interessadas e ao património da Distribuidora.

6. DIRECTRIZES

6.1. **Plano de continuidade de negócio:** plano de acção detalhado que estabelece as medidas e os procedimentos necessários para a recuperação da actividade nos níveis e nos tempos definidos, devendo abranger os meios que permitam gerir uma eventual interrupção não planeada da actividade, incluindo o processo de retorno, com a maior brevidade possível a níveis de qualidade de serviço normais.

6.2. **Eventos:** acontecimentos susceptíveis de perturbar o normal funcionamento das Instituições, tais como catástrofes naturais, pandemias, actos de terrorismo, falhas nos sistemas informáticos, incêndios, inundações ou falhas graves de energia.

6.3. **Gestão de continuidade de negócio:** conjunto integrado de políticas, processos e procedimentos que visam assegurar o funcionamento contínuo de uma organização, ou a recuperação atempada da sua actividade operacional, no caso de ocorrência de eventos susceptíveis de perturbar o normal funcionamento do negócio.

6.4. **Infraestruturas Primárias:** local ou locais onde normalmente são executadas as funções de negócio críticas, abrangendo em simultâneo as infraestruturas de tecnologias de informação e os postos de trabalho, assim como as redes de fornecimento que permitam a sua operacionalidade ou acesso às mesmas (e.g., telecomunicações, energia, água, transportes).

6.5. **Infraestruturas alternativas:** infraestruturas que permitem a uma Instituição garantir a continuidade das suas funções de negócio críticas, ou a sua recuperação num espaço de tempo reduzido, no caso de uma situação emergente provocar a inoperacionalidade das infraestruturas primárias ou impossibilitar o acesso às mesmas.

7. GLOSSARIO

- AIN - Análise de Impacto para o Negócio
- OMC - Objetivo Mínimo de Continuidade
- PCN - Plano de Continuidade de Negócios
- PRI - Plano de Resposta a Incidentes
- PSI - Política de Segurança da Informação
- TRI – Tempo de Resposta a Incidentes

8. RESPONSABILIDADES

8.1. O Órgão de Administração da Distribuidora promove a resiliência da Distribuidora face à ocorrência de desastres e assegura o seu funcionamento contínuo, designadamente a recuperação do negócio em caso de perturbações na actividade. Neste contexto, o órgão de Administração considera a gestão da continuidade de negócio como parte integrante da gestão do risco, articulando-a também com as políticas de controlo interno da instituição, sendo responsável pela aprovação e implementação da política de gestão da continuidade de negócio.

8.2. A política de gestão da continuidade de negócio é objecto de aprovação em sede de órgão de Administração, ao qual compete também assegurar um acompanhamento assíduo do processo de implementação e desenvolvimento, bem como, e promover uma discussão regular sobre a gestão da continuidade de negócio nas reuniões ou sessões do conselho.

8.3. A competência pela implementação da política de gestão da continuidade de negócio pode ser delegada a um comité de Risco da Distribuidora, ou a outra unidade de estrutura adequada, no entanto, a responsabilidade deve permanecer sobre o Órgão de Administração.

8.4. O Órgão de Administração é o responsável pela activação dos procedimentos de continuidade de negócio, reflectidos no presente plano de continuidade de negócios, no caso de ocorrência de desastre, ou qualquer outra situação que outro evento que motive a activação do plano.

8.5. O Gabinete Jurídico é responsável pela gestão dos colaboradores através da realização de convocatórias a serem realizadas às áreas participantes para o devido planeamento e execução dos testes.

8.6. O Gabinete de Auditória é responsável pelo controlo sobre a realização dos testes definidos tendo em conta a sua calendarização.

8.7. O Gabinete de Gestão de Risco é responsável pela identificação e alerta dos riscos identificados durante e após a realização dos testes.

8.8. O Gabinete de *Compliance* é responsável por verificar se o plano cumpre com toda a regulamentação aplicável e garantir que seja feita a revisão do mesmo no mínimo anual.

8.9. O Gabinete de Sistemas de Informação é responsável por garantir que todos os sistemas se encontram operacionais para a realização de testes e executar o procedimento de restauração dos sistemas em caso de ocorrência de algum evento.

8.10. O Gabinete de Gestão de Risco é responsável por garantir que as instalações estão operacionais para a realização dos testes.

8.11. O Gabinete de Gestão de Risco é responsável por garantir a divulgação do plano de continuidade. A divulgação do documento será realizada através de comunicação interna, documento impresso e divulgação na Intranet com acesso ao documento em formato PDF.

9. GESTÃO DA CONTINUIDADE DO NEGÓCIO

9.1. Através do presente plano a Distribuidora implementa um processo de gestão de continuidade de negócio integrado no seu processo de negócio, que compreende as seguintes etapas:

a) Análise do impacto no negócio;
b) Definição de uma estratégia de recuperação;
c) Plano de continuidade de negócio,
d) Programas de testes, formação e sensibilização de todos os colaboradores, a todos os níveis da instituição.

10. ANÁLISE DO IMPACTO NO NEGÓCIO

10.1. Esta análise deve permitir identificar as funções de negócio críticas para a instituição, os principais factores dos quais depende a sua continuidade, tanto internos como externos, assim como os níveis de protecção adequados perante diferentes cenários, a análise do impacto no negócio é a base do processo de gestão de continuidade de negócio e consiste

em identificar as funções de negócio críticas para a instituição, ou seja, aquelas que, no caso de serem interrompidas, têm o potencial de gerar implicações mais significativas na continuidade da actividade, na reputação, na situação financeira e/ou nas contrapartes da instituição;

10.2. A análise do impacto no negócio deve contemplar as seguintes fases:

a) Identificação dos riscos susceptíveis de gerar uma interrupção da actividade e que possam originar um impacto material para a instituição;

b) Identificação dos cenários de interrupção plausíveis, incluindo estimativas das respectivas probabilidades de ocorrência, impactos e de duração dos seus efeitos. Não se afigurando razoável quantificar as probabilidades de ocorrência, a análise deve procurar definir uma escala qualitativa de probabilidades, o que permitirá identificar os cenários mais e menos prováveis. Para este efeito, as instituições devem considerar os riscos a que se encontram especialmente expostas (por exemplo, risco sísmico no caso dos edifícios que se encontram numa região de elevada actividade sísmica; risco de inundação, no caso de se encontrarem em regiões propensas a esses fenómenos);

c) Estimativa do período de tempo durante o qual a instituição pode suportar a interrupção de cada uma das suas funções de negócio críticas;

d) Cálculo do impacto da interrupção de funções de negócio críticas nos clientes finais; e

e) Previsão do impacto financeiro, legal e de reputação originado pela interrupção das funções de negócio críticas sobre a instituição, considerando períodos de tempo diversos.

10.3. Funções de Negócio Críticas para a Instituição:

#	Macroprocesso de Negócio	Infraestrutura Física de Suporte	Fornecedor / Entidade Externo (a)
1	Custodia	Negócio	Não
2	Abertura de Contas	Negócio	Não
3	Registo de Ordens	Negócio	Não
4	Transferência de Títulos	Negócio	Não
5	Atendimento Geral	Negócio	Não
6	CEVAMA	Negócio	Sim
7	Registos e Contabilidade	Suporte	Não
8	Produtos de Investimento (Mercado de Capitais)	Negócio	Não

10.4. A análise do impacto no negócio e os pressupostos que lhe estão subjacentes, devem ser revistos periodicamente e sempre que se verifiquem alterações relevantes ao nível operacional ou quando ocorram eventos externos que afectem significativamente a actividade da instituição.

10.5. As áreas de negócio relevantes devem participar na realização da análise do impacto no negócio, embora seja importante que todo o processo seja coordenado de forma centralizada e que, em especial, sejam definidos critérios uniformes para a identificação da importância crítica e consequente prioridade das funções de negócio.

10.6. Os resultados da análise do impacto no negócio devem ser claramente documentados e facilmente acessíveis a todos os intervenientes.

11 DEFINIÇÃO DE UMA ESTRATÉGIA DE RECUPERAÇÃO

11.1. A Distribuidora caracteriza os cenários de acordo com as probabilidades, impacto e duração, permitindo ter uma estratégia de recuperação incidam sobre os cenários mais relevantes para a instituição. Por outro, ainda no âmbito da Estratégia, a GSI enquanto *unidade responsável pela execução, revisão e testes do presente plano, procede da seguinte forma:*

1.º - Com base no Inventário de Activos mantidos na instituição, tal como, como determinado pela Política de Segurança Cibernética, é realizada a Análise de Impacto para o Negócio (AIN) dos processos de negócio cujo escopo é abrangido por este Plano de Continuidade Negócios

2.º - A Análise de Impacto para o Negócio (AIN) leva em consideração quais os activos de suporte e infraestrutura que mantém cada um dos processos de negócio avaliados. Também são determinados os tempos de indisponibilidade aceitáveis para cada processo e os recursos necessários para a activação do Plano de Continuidade Negócios (PCN).

11.2. Levando em conta os índices de disponibilidade apontados para cada um dos serviços, são estipulados tempos máximos de normalização do funcionamento, sempre levando em conta o índice mais alto em cada um dos cenários previstos, neste sentido, optou-se por adoptar o tempo de indisponibilidade por base mensal, tempo este que será o máximo objectivado, no mês em questão, para o reinício dos serviços.

11.3. Os procedimentos adoptados neste PCN visam atender ao Objetivo Mínimo de Continuidade (OMC), ou seja, o mínimo de serviços que deve estar operacional para a prestação dos serviços.

11.4. A partir dos resultados da análise de riscos e/ou por determinação do Conselho de

Administração e/ou Comissão Executiva, cada área identifica processos ou actividades críticas para os quais são definidas estratégias e construídos procedimentos de continuidade de negócios, considerando:

a) Ameaças e vulnerabilidades das situações analisadas;

b) Probabilidades e impactos que envolvam a indisponibilidade dos processos de negócio analisados, bem como a avaliação dos riscos;

c) Estratégias de continuidade e custos de implementação;

d) Consequências de não se implementar mecanismos de contingência (perdas potenciais);

e) Os recursos essenciais relacionados a pessoas, instalações, tecnologias, informações, suprimentos e partes interessadas (*stakeholders*) e serviços relevantes prestados por terceiros;

f) Para os recursos essenciais, são formalmente estabelecidos os planos com procedimentos alternativos para recuperação das actividades exigidas, no tempo desejado, observada a relação custo e/ou benefício e o impacto potencial.

11.5. Este PCN é aplicável as actividades de negócio consideradas críticos pelos órgãos de Administração das entidades da Distribuidora Valor, em função de potenciais impactos negativos, financeiros, patrimoniais, legais, regulatórios e de imagem.

11.6. Conforme o ponto anterior, como escopo deste PCN, os seguintes processos de negócio são por ele coberto:

a) Processos de Negócio; Processo de Cobrança; Processo de Repasses; Processo Administrativo Financeiro; Processo de Análise de Crédito;

b) Processamento de Dados; Processo de Recursos Humanos; Processo Cobrança Assessorias; Processo Vídeo Vigilância; Processo Departamento Pessoal.

11.7. Adicionalmente, também é levado em consideração neste escopo o funcionamento da operação da instituição em sua sede principal em caso de sua indisponibilidade (Perda da Sede Principal da Instituição).

i. Os procedimentos de continuidade de negócios, que estão apresentados neste plano,

são objectivos, concisos, prevendo o processo em que cada acto deve ser utilizado, os responsáveis pelos procedimentos de recuperação e os procedimentos que serão executados para a contingência ou a recuperação dos recursos que sofreram interrupção.

i. O Presente Plano deve ser impresso e entregue aos responsáveis pela sua implementação, bem como, por razões de perda do acesso digital, além de sua disponibilização em ambiente de nuvem seguro e acessível via VPN por todos os envolvidos.

ii. As situações de contingência por epidemias e surtos são tratadas em um plano de contingência próprio.

11.8. Com base no processo de gestão e avaliação de riscos (conforme a PSI), aquando da identificação de novas actividades ou implementação de novos activos que estejam relacionados ao escopo deste PCN, ele (o plano) deverá ser actualizado para fazer constar as actividades em causa.

11.9. A gestão da continuidade de negócios é objecto de acompanhamento sistemático por parte dos órgãos de administração da instituição.

12 DESCRIÇÃO DO PLANO DE CONTINUIDADE DE NEGÓCIO COM A COMPONETE DO DISASTER RECOVERY

12.1. A Distribuidora Valor tem um site alternativo, localizado a mais (+) 20 kilometros da zona da sede, com infraestrutura alternativa de contingência. O site foi criado e mantido com base na análise de risco realizada, neste site são feitos Back-up diários de todos os dados constantes servidor primário, no sentido, de o ambiente alternativo estar preparado e configurado com mecanismos de contingência, continuidade e *disaster recovery* com base neste PCN que inclui a recuperação de Desastres de Data Center, de serviços na nuvem.

12.2. Para efeitos de continuidade, deverão existir dois links de Internet na sede da instituição fornecidos por duas empresas com infraestruturas independentes.

12.3. Estão abrangidos pelo Backup da instituição, sumariamente:

Data Center da SEDE (Belas Business Park) - No âmbito do Plano de Continuidade de Negócio, a salvaguarda dos dados da infraestrutura do FileServer, Exchange Sever,Primavera e Sifox é assegurada através da solução **Veeam Software Backup & Replication**, a qual garante a execução automática de cópias de segurança periódicas, bem como a gestão e retenção dos respetivos pontos de recuperação, em conformidade com as políticas internas definidas.

Relativamente às máquinas virtuais, a solução encontra-se integrada ao hypervisor, permitindo a realização de backups ao nível de imagem e a replicação integral das VMs para infraestrutura de contingência, assegurando a capacidade de restabelecimento dos serviços dentro dos tempos e níveis de recuperação estabelecidos (RTO e RPO), suportando assim os mecanismos de continuidade e recuperação em cenário de desastre.

Teste de *Restore File Server*: Com periodicidade semanal, é realizada a validação do processo de restauração mediante a recuperação de ficheiros selecionados, com o objetivo de assegurar a integridade dos backups e o correto funcionamento do sistema de cópias de segurança.

Máquinas Virtuais (VMs): Com periodicidade trimestral, é efetuado o teste de recuperação integral de uma máquina virtual em ambiente isolado e sem ligação à rede produtiva, procedendo-se posteriormente à verificação dos sistemas e da integridade dos dados, de modo a garantir a eficácia e fiabilidade dos procedimentos de recuperação.

Bancos de Dados: Diariamente, é realizado o processo de restauração da base de dados de produção para o ambiente de testes e para o Site 2, sendo este procedimento considerado como uma validação integral da eficácia e consistência dos backups.

12.4. As medidas de contingência e continuidade aqui planejadas, em face da utilização de recursos de nuvem, podem ser activadas à distância, quando necessário. Para isso, há estrutura específica de VPNs para os acessos aos recursos necessários e os funcionários responsáveis sempre portam *notebooks* da instituição. Além do mais, A Distribuidora Valor possui uma sede alternactiva para situações de comprometimento de sua sede principal, localizada a uma quadra de distância. Neste sentido, acções de continuidade que envolvem o comprometimento da sede principal podem ser facilmente tomadas na sede auxiliar da instituição, **localizada na Marina Baia, Ilha de Luanda**

12.5 Como meio de controle de incidentes e possível escalação do PCN, a Distribuidora Valor mantém um TRI que realiza a categorização e classificação de incidentes. Além das tarefas gerais de resposta a incidentes, o referido time também pode escalar um incidente, visando a activação do plano de

continuidade, quando as primeiras respostas demonstrarem a sua necessidade.

12.6 Esta actividade utiliza sistemas específicos de registro de incidentes, categorização e classificação. Conforme o próprio Plano de Ação e Resposta a Incidentes, os incidentes de "Nível emergencial", quando não resolvidos no tempo previsto, ou seja, perdido o controle sobre o seu gerenciamento, devem ser escalados para situação de crise, que levará a activação do PCN, quando os serviços envolvidos estiverem cobertos por este plano.

13 ACTIVAÇÃO DO PLANO

13.1. O presente plano é activado nas seguintes situações:

a) Quando o incidente, pela sua gravidade e reconhecimento de complexidade, puder ser imediatamente reconhecido como apto a ser tratado diretamente pela PCN (como, por exemplo, um incidente grave que afete a sede da Distribuidora Valor.

b) Quando, por meio de entradas realizadas no TRI, detectar-se a afetação na disponibilidade de um recurso necessário para a prestação dos serviços da instituição, conforme a projeção da complexidade e afetação de activos que suportem os processos de negócio controlados por este plano.

c) Em tais casos, ao se detectar uma situação que não possa ser adequadamente controlada, levando em consideração os tempos aceitáveis de indisponibilidade para cada serviço, o TRI escalará o incidente para ser tratado por meio desta política.

d) Na situação acima, o plano somente será activado quando as medidas de contingência forem impossíveis de serem realizadas em tempo menor do que o aceitável da indisponibilidade do processo de negócio. Neste sentido, o TRI projetará o tempo de resolução do incidente.

e) Quando os mecanismos de monitoramento dos activos que mantém os serviços prestados pela instituição dispararem alertas que indiquem, pela sua gravidade, a impossibilidade de recuperação dos activos nos tempos esperados para o controle de incidentes.

f) Em todas as situações acima, a decisão sobre activar ou não a PCN cabe ao conselho de Administração ou ao órgão que o mesmo delegar esta função.

14 PROCEDIMENTOS DO PLANO DE CONTINUIDADE

14.1. Perda da Sede Principal da Instituição por Incêndios, Terramotos, Inundações, etc.

Resultado da Análise de risco		
Probabilidade: Baixa	**Impacto: Alto**	**Risco: Baixo**
Descrição da ameaça:	Situação gerada por qualquer evento que impeça a utilização da sede principal da instituição, tais como, incêndio na própria ou em prédios vizinhos, terramotos, inundações, desabamento, etc.	
Activos afetados pela ameaça:	Activos relacionados aos processos de negócio conforme o Inventário de Activos são: Data Center	
Processos de negócio afetados e índices de disponibilidade:	Processo de Risco: 98,8% Processo de Compliance: 98,8% Processo Administrativo – 100% Processo da Sala de Mercado: 99,4% Processamento de Dados: 99,4%	
Dono do processo:	Gabinete de Sistemas de Informação	
Responsáveis pela execução do plano de recuperação:	Dario Filipe +244 927 563 010 Director do Gabinete de Sistemas de Informação dfilipe@distribuidoravalor.ao	
Cargos ou pessoas a serem comunicados em caso da activação:	Gonçalo Madaleno PCA goncalo.madaleno@distribuidoravalor.ao Gabinete de Riscos laraujo@distribuidoravalor.ao E-mail de Grupo: info@distribuidoravalor.ao	

Recursos de Infraestrutura utilizados para o funcionamento do processo:	Servidor de VPN, Servidor de Arquivos, Links de Comunicação (Internet).
Recursos de Infraestrutura de contingência para o funcionamento do processo.	Servidor de Arquivos Conexão direta na Nuvem (VPN).
Procedimentos:	1. Preparação do espaço físico alterativo (sede alternativa) para receber os colaboradores essenciais à continuidade da actividade. 2. Conectar a rede ao Data Center da Marina Baia 3. Realizar conexão de VPN directa no Provedor de Nuvem, para acesso aos activos.
Tempos objetivados de recuperação (base mensal)	Processo Sala de Mercado: 4h22min Processo Administrato: 4h22min Processo de *Compliance*: 5h22min Processo de Gestão de Risco: 8h45m Processamento de Dados: 4h22min

14.2. Destruição/Falha/Defeito de Equipamentos ou Mídias Relevantes

Resultado da Análise de risco		
Probabilidade: Baixa	**Impacto: Baixo**	**Risco: Baixo**
Descrição da ameaça:	Comprometimento de equipamentos locais (ex.: servidores, roteadores, *switches*,...) ou mídias tanto por ação maliciosa quanto por eventos naturais como surto elétrico.	
Activos afetados pela ameaça:	Activos relacionados aos processos de negócio conforme o Inventário de Activos	
Processos de negócio afetados e índices de disponibilidade:	Processo Auditória: 90,8% Processo de Risco: 98,8% Processo de Compliance: 98,8% Processo Administrativo Financeira: 99,4% Processo de Registos e Contabilidade: 98,8% Processamento de Dados: 99,4%	

Dono do processo:	Gabinete de Sistemas de Informação
Responsáveis pela execução do plano de recuperação:	Dario Filipe +244 927 563 010 Director do Gabinete de Sistemas de Informação dfilipe@distribuidoravalor.ao
Cargos ou pessoas a serem comunicados em caso da activação:	Gonçalo Madaleno PCA goncalo.madaleno@distribuidoravalor.ao Gabinete de Riscos laraujo@distribuidoravalor.ao E-mail de Grupo: info@distribuidoravalor.ao
Recursos de Infraestrutura utilizados para o funcionamento do processo:	Servidor de Arquivos, Notebook, Desktop.
Recursos de Infraestrutura de contingência para o funcionamento do processo.	Backup - Equipamentos de Backup.
Procedimentos:	1. Realizar restore do backup do activo (*Veeam Backup*). 2. Substituir equipamento com defeito.
Tempos objetivados de recuperação (base mensal)	Processo de negócio: 8h45m Processo Sala de Mercado: 4h22min Processo de Auditória: 4h22min Processo de Compliance: 5h22min Processamento de Dados: 4h22min

14.3. Interrupção de Suprimento de Energia

Resultado da Análise de risco		
Probabilidade: Alta	**Impacto: Baixo**	**Risco: Médio**
Descrição da ameaça:	Risco de Corte prolongado de Energia, afectar a disponibilidade do Data Center da SEDE.	
Activos afetados pela ameaça:	Activos relacionados aos processos de negócio conforme o Inventário de Activos	
Processos de negócio afetados e índices de disponibilidade:	Processos da Comissão Executiva: 78% Processo de Negócio: 10,8% Processo de Risco 98,8% Processo de Compliance: 98,8% Processo Administrativo e Financeiro: 99,4% Processamento de Dados: 99,4%	
Dono do processo:	Gabinete de Sistemas Informação	
Responsáveis pela execução do plano de recuperação:	Dario Filipe +244 927 563 010 Director do Gabinete de Sistemas de Informação dfilipe@distribuidoravalor.ao	
Cargos ou pessoas a serem comunicados em caso da activação:	Gonçalo Madaleno PCA goncalo.madaleno@distribuidoravalor.ao Gabinete de Riscos laraujo@distribuidoravalor.ao E-mail de Grupo: info@distribuidoravalor.ao	
Recursos de Infraestrutura utilizados para o funcionamento do processo:	VPN, Servidor de Arquivos, Links de Comunicação (Internet).	
Recursos de Infraestrutura de contingência para o funcionamento do processo:	UPS de Capacidade de até 4 horas Data Center na Sede Alternativa da Distribuidora	

Procedimentos:	1. Preparação da troca da ligação para o Data Center da Marina Baia. 2. Faltando 1 hora para o fim da carga da UPS, testar a Disponibilidade da data Center alternativo. 3. Transferir a conexão dos balcões para o Data Center reserva
Tempos objetivados de recuperação (base mensal)	Processo de Negócio: 8h45m Processo Sala de Mercado: 4h22min Processo de Auditória: 4h22min Processo de *Compliance*: 5h22min Processamento de Dados: 4h22min Processo vídeo Vigilância: 8h45m

14.4. Saturação de Sistema

Resultado da Análise de risco		
Probabilidade: Baixa	**Impacto: Baixo**	**Risco: Muito baixo**
Descrição da ameaça:	Tendo em conta um aumento das operações já existentes ou mesmo a inclusão de novas operações, pode ocorrer saturação de recursos na nuvem ou no servidor físico, causando lentidão nas operações e, em casos extremos, parada de serviços. Nota: Não estão considerados aqui acções maliciosas que, causando o mesmo efeito, constituiriam ataques de negação de serviço.	
Activos afetados pela ameaça:	Activos relacionados aos processos de negócio conforme o Inventário de Activos	
Processos de negócio afetados e índices de disponibilidade:	Processo Gabinete Jurídico: 98% Processos da Comissão Executiva: 78% Processo Auditória: 90,8% Processo de Risco Global: 98,8% Processo de Compliance: 98,8% Processo Administrativo e Financeiro: 99,4% Processo de Registos e Contabilidade: 98,8% Processamento de Dados: 99,4% Processo de Recursos Humanos: 98,8% Processo Video Vigilância: 98,8%	
Dono do processo:	Gabinete de Sistemas de Informação	
Responsáveis pela execução do plano de recuperação:	Dario Filipe +244 927 563 010 Director do Gabinete de Sistemas de Informação dfilipe@distribuidoravalor.ao	
Cargos ou pessoas a serem comunicados em caso da activação:	Gonçalo Madaleno PCA goncalo.madaleno@distribuidoravalor.ao Gabinete de Riscos laraujo@distribuidoravalor.ao E-mail de Grupo: info@distribuidoravalor.ao	

Recursos de Infraestrutura utilizados para o funcionamento do processo:	VPN, Servidor de Arquivos, Links de Comunicação (Internet).
Recursos de Infraestrutura de contingência para o funcionamento do processo:	VPN, Servidor de Arquivos, Links de Comunicação (Internet) Activos de Suporte e Infraestrutura. "Inventário de Activos.xlsx
Procedimentos:	1. Intervenção directamente nos pedidos de informação no sentido de priorização a transmissão de dados. 2. Parar a transição de dados secundários ou não prioritários
Tempos objetivados de recuperação (base mensal)	Processo de Negócio: 8h45m Processo Sala de Mercado: 4h22min Processo de Auditória: 4h22min Processo de *Compliance*: 5h22min Processo de Registos e Contabilidade: 8h45m Processamento de Dados: 4h22min Processo Gabinete Jurídico: 4h22min Processo Vídeo Vigilância: 8h45m

14.5. Indisponibilidade de Acesso à Internet na Sede da Instituição

Resultado da Análise de risco		
Probabilidade: Baixa	**Impacto: Baixo**	**Risco: Muito baixo**
Descrição da ameaça:	Interrupção do acesso à Internet na sede da empresa, impedindo a interação com os serviços disponíveis na nuvem, com os demais serviços online e fundamentalmente com a rede agência e balcões.	
Activos afetados pela ameaça:	Activos relacionados aos processos de negócio conforme o Inventário de Activos	
Processos de negócio afetados e índices de disponibilidade:	Processo Gabinete Jurídico: 98% Processos da Comissão Executiva: 78% Processo de Negócio: 10,8% Processo de Risco Global: 98,8% Processo de *Compliance*: 98,8% Processo Administrativo e Financeiro: 99,4% Processo de Registos e Contabilidade: 98,8% Processamento de Dados: 99,4% Processo Video Vigilância: 98,8%	
Dono do processo:	Gabinete de Sistemas Informação	
Responsáveis pela execução do plano de recuperação:	Dario Filipe +244 927 563 010 Director do Gabinete de Sistemas de Informação dfilipe@distribuidoravalor.ao	

Cargos ou pessoas a serem comunicados em caso da activação:	Gonçalo Madaleno PCA goncalo.madaleno@distribuidoravalor.ao Gabinete de Riscos laraujo@distribuidoravalor.ao E-mail de Grupo: info@distribuidoravalor.ao
Recursos de Infraestrutura utilizados para o funcionamento do processo:	Link de Comunicação principal.
Recursos de Infraestrutura de contingência para o funcionamento do processo.	Link de Comunicação de Contingência VPN de Acesso a internet
Procedimentos:	1. Activar Link de Comunicação de Contingência (automático). 2. Se ocorrer queda dos dois links, o acesso aos sistemas poderá ser realizado de qualquer local com internet, através de VPN que será contratado para o efeito
Tempos objetivados de recuperação (base mensal)	Processo de Negócio: 8h45m Processo Sala de Mercado: 4h22min Processo de *Compliance*: 5h22min Processamento de Dados: 4h22min Processo Gabinete Jurídico: 4h22min Processo Vídeo Vigilância: 8h45m

14.6. Ataques de Ransonware

Resultado da Análise de risco		
Probabilidade: Alta	**Impacto: Alto**	**Risco: Crítico**
Descrição da ameaça:	Artefato de ransonware com acesso total à infraestrutura e aos dados da instituição, fruto de provável APT (Advanced Persistent Threat), que leva ao sequestro dos dados por meio de criptografia forte.	
Activos afetados pela ameaça:	Activos relacionados aos processos de negócio conforme o Inventário de Activos	
Processos de negócio afetados e índices de disponibilidade:	Processo Gabinete Jurídico: 98% Processos da Comissão Executiva: 78% Processo Auditória: 90,8% Processo de Risco Global: 98,8% Processo de Compliance: 98,8% Processo Administrativo e Financeiro: 99,4% Processo de Registos e Contabilidade: 98,8% Processamento de Dados: 99,4% Processo Vídeo Vigilância: 98,8%	
Dono do processo:	Gabinete de Sistemas de Informação	
Responsáveis pela execução do plano de recuperação:	Dario Filipe +244 927 563 010 Director do Gabinete de Sistemas de Informação dfilipe@distribuidoravalor.ao	
Cargos ou pessoas a serem comunicados em caso da activação:	Gonçalo Madaleno PCA goncalo.madaleno@distribuidoravalor.ao Gabinete de Riscos laraujo@distribuidoravalor.ao E-mail de Grupo: info@distribuidoravalor.ao	
Recursos de Infraestrutura utilizados para o funcionamento do processo:	Activos de Suporte e Infraestrutura. Data Center; Servidores Windows	

Recursos de Infraestrutura de contingência para o funcionamento do processo.	Ambiente de Disaster Recovery (Marina Baia – Ilha de Luanda - Angola). Backup (Recovery Services vaults)
Procedimentos:	1. Realizar restore do backup do activo afetado (Recovery Services Vaults). 2. Activar o Plano de Recuperação de Desastre (DR). a. Start de Banco de Dados no ambiente de DR b. Garantir o processo de conectividade no ambiente de DR c. Alterações de DNS Externo para Ambiente de DR d. Alterações em Servidores WEB para Ambiente de DR e. Alterações em Servidores RDS para ambiente de DR f. Alterações em Servidores APP para ambiente de DR g. Alterações no Servidor de Arquivos para ambiente de DR h. Start de Banco de Dados no ambiente de DR - POSTGRESQL i. Validação de Sistemas para ambiente de DR j. Validação de Sistemas para ambiente de DR k. Alterações ConnectDirect
Processos de negócio afetados e índices de disponibilidade:	Processo de Negócio: 8h45m Processo Sala de Mercado: 4h22min Processo de Auditória: 4h22min Processo de *Compliance*: 5h22min Processamento de Dados: 4h22min Processo Gabinete Jurídico: 4h22min Processo Vídeo Vigilância: 8h45m

14.7. Ataque de Negação de Serviço Contra a Infraestrutura do Provedor

Resultado da Análise de risco		
Probabilidade: Média	**Impacto: Médio**	**Risco: Médio**
Descrição da ameaça:	Ataque de negação de serviço contra a infraestrutura do provedor de nuvem via Internet, tipicamente DDoS (Distributed Denial of Service). Não são considerados ataques à estrutura física do provedor.	
Activos afetados pela ameaça:	Activos relacionados aos processos de negócio conforme o Inventário de Activos	
Processos de negócio afetados e índices de disponibilidade:	Processo Gabinete Jurídico: 98% Processos da Comissão Executiva: 78% Processo de Negócio: 10,8% Processo de Risco Global: 98,8% Processo de *Compliance*: 98,8% Processo Administrativo e Financeiro: 99,4% Processo de Registos e Contabilidade: 98,8% Processamento de Dados: 99,4%	
Dono do processo:	Gabinete de Sistemas de Informação	
Responsáveis pela execução do plano de recuperação:	Dario Filipe +244 927 563 010 Director do Gabinete de Sistemas de Informação dfilipe@distribuidoravalor.ao	
Cargos ou pessoas a serem comunicados em caso da activação:	Gonçalo Madaleno PCA goncalo.madaleno@distribuidoravalor.ao Gabinete de Riscos laraujo@distribuidoravalor.ao E-mail de Grupo: info@distribuidoravalor.ao	
Recursos de Infraestrutura utilizados para o funcionamento do processo:	Acesso ao Data Center 2	

Recursos de Infraestrutura de contingência para o funcionamento do processo:	Ambiente de Disaster Recovery (Marina Baia – Ilha de Luanda).
Procedimentos:	Activar o Plano de Recuperação de Desastre Plano de Recuperação de Desastre de Data Center.docx" levando em consideração os seguintes procedimentos: 1. Start de Banco de Dados no ambiente de DR 2. Garantir o processo de conectividade no ambiente de DR 3. Alterações de DNS Externo para Ambiente de DR 4. Alterações em Servidores WEB para Ambiente de DR 5. Alterações em Servidores RDS para ambiente de DR 6. Alterações em Servidores APP para ambiente de DR 7. Alterações no Servidor de Arquivos para ambiente de DR 8. Start de Banco de Dados no ambiente de DR 9. Validação deSistemas para ambiente de DR 10. Validação deSistemas para ambiente de DR 11. Alterações ConnectDirect
Tempos objetivados de recuperação (base mensal)	Processo Negócio: 8h45m Processo Sala de Mercado: 4h22min Processo de Auditória: 4h22min Processo de *Compliance*: 5h22min Processo de contabilidade: 8h45m Processamento de Dados: 4h22min Processo Gabinete Jurídico: 4h22min

14.8. Ataque de Negação de Serviço Contra um Activo Específico

Resultado da Análise de risco		
Probabilidade: Alta	**Impacto: Médio**	**Risco: Alto**
Descrição da ameaça:	Ataque de negação de serviço contra servidores/serviços da Distribuidora Valor hospedados no provedor em nuvem. São considerados ataques direcionados visando esgotar capacidade dos servidores ou ainda esgotar limites de serviços das aplicações.	
Activos afetados pela ameaça:	Activos relacionados aos processos de negócio conforme o Inventário de Activos	
Processos de negócio afetados e índices de disponibilidade:	Processo Gabinete Jurídico: 98% Processos da Comissão Executiva: 78% Processo de Negócio: 10,8% Processo de Risco Global: 98,8% Processo de *Compliance*: 98,8% Processo Administrativo e Financeiro: 99,4% Processo de Registo e Contabilidade: 98,8% Processamento de Dados: 99,4% Processo Video Vigilância: 98,8%	
Dono do processo:	Gabinete de Sistemas de Informação	
Responsáveis pela execução do plano de recuperação:	Dario Filipe +244 927 563 010 Director do Gabinete de Sistemas de Informação dfilipe@distribuidoravalor.ao	
Cargos ou pessoas a serem comunicados em caso da activação:	Gonçalo Madaleno PCA goncalo.madaleno@distribuidoravalor.ao Gabinete de Riscos laraujo@distribuidoravalor.ao E-mail de Grupo: info@distribuidoravalor.ao	

Recursos de Infraestrutura utilizados para o funcionamento do processo:	Activos de Suporte e Infraestrutura.
Recursos de Infraestrutura de contingência para o funcionamento do processo:	Os servidores/serviços possuem recursos de contingência. Ambiente de Disaster Recovery (Marina Baia – Ilha de Luanda – Angola).
Procedimentos:	1 - Activar servidores/serviços de contingência. 2 – "Plano de Recuperação de Desastre de Data Center" levando em consideração os seguintes procedimentos: a. Start de Banco de Dados no ambiente de DR b. Garantir o processo de conectividade no ambiente de DR c. Alterações de DNS Externo para Ambiente de DR d. Alterações em Servidores WEB para Ambiente de DR e. Alterações em Servidores RDS para ambiente de DR f. Alterações em Servidores APP para ambiente de DR. g. Alterações no Servidor de Arquivos para ambiente de DR h. Start de Banco de Dados no ambiente de DR – SQL i. Validação de Sistemas para ambiente de DR j. Validação de Sistemas para ambiente de DR k. Alterações ConnectDirect
Tempos objetivados de recuperação (base mensal)	Processo de Negócio: 8h45m Processo Sala de Mercado: 4h22min Processo de Auditória: 4h22min Processo de *Compliance*: 5h22min Processo de Registo e Contabilidade: 8h45m Processamento de Dados: 4h22min Processo Gabinete Jurídico: 4h22min Processo Vídeo Vigilância: 8h45m

14.9. Destruição de Activos na Nuvem

Resultado da Análise de risco		
Probabilidade: Média	**Impacto: Alto**	**Risco: Alto**
Descrição da ameaça:	Perda causada por destruição de activos hospedados no provedor de nuvem. Embora a ameaça possa ser causada por ações acidentais, considera-se primordialmente a realização de ações maliciosas no sentido de causar a referida destruição.	
Activos afetados pela ameaça:	Activos relacionados aos processos de negócio conforme o Inventário de Activos	
Processos de negócio afetados e índices de disponibilidade:	Processo Gabinete Jurídico: 98% Processos da Comissão Executiva: 78% Processo Auditória: 90,8% Processo de Risco Global: 98,8% Processo de *Compliance*: 98,8% Processo Administrativo e Financeiro: 99,4% Processo de Registo e Contabilidade: 98,8% Processamento de Dados: 99,4% Processo Vídeo Vigilância: 98,8%	
Dono do processo:	Gabinete de Sistemas de Informação	
Responsáveis pela execução do plano de recuperação:	Dario Filipe +244 927 563 010 Director do Gabinete de Sistemas de Informação dfilipe@distribuidoravalor.ao	

Cargos ou pessoas a serem comunicados em caso da activação:	Gonçalo Madaleno PCA goncalo.madaleno@Distribuidoravalor.ao Gabinete de Riscos info@Distribuidoravalor.ao E-mail de Grupo: info@Distribuidoravalor.ao
Recursos de Infraestrutura utilizados para o funcionamento do processo:	Activos de Suporte e Infraestrutura de rede, servidores.
Recursos de Infraestrutura de contingência para o funcionamento do processo.	Ambiente de Disaster Recovery (Marina Baia – Ilha de Luanda). Backup (Recovery Services)
Procedimentos:	1. Realizar restore do backup do activo destruído (Recovery Services). 2. Activar o Plano de Recuperação de Desastre (DR), ou seja, "iniciar o Plano de Recuperação de Desastre de Data Center: a. Start de Banco de Dados no ambiente de DR b. Garantir o processo de conectividade no ambiente de DR c. Alterações de DNS Externo para Ambiente de DR d. Alterações em Servidores WEB para Ambiente de DR e. Alterações em Servidores RDS para ambiente de DR f. Alterações em Servidores APP para ambiente de DR g. Alterações no Servidor de Arquivos para ambiente de DR h. Start de Banco de Dados no ambiente de DR - i. Validação de Sistemas para ambiente de DR j. Validação de Sistemas para ambiente de DR k. Alterações ConnectDirect

Tempos objetivados de recuperação (base mensal)	Processo de Negócio: 8h45m Processo Sala de Mercado: 4h22min Processo de Auditória: 4h22min Processo de *Compliance*: 5h22min Processo de Registos e Contabilidade: 8h45m Processamento de Dados: 4h22min Processo Gabinete Jurídico: 4h22min Processo Vídeo Vigilância: 8h45m

15 PROJECTO DE IMPLEMENTAÇÃO DO DISASTER RECOVERY

Fase	Actividade	Descrição	Duração	Período
1	Planeamento e Análise	Levantamento de requisitos, análise de risco (BIA), definição de RTO/RPO	1 mês	Mês 1
2	Desenho da Solução	Arquitetura do DR, escolha tecnológica (on-premise/cloud), dimensionamento	1 mês	Mês 2
3	Aquisição	Compra de equipamentos, licenças e contratação de serviços	2 meses	Meses 3-4
4	Implementação de Infraestrutura	Setup de servidores, storage, rede e segurança no Site B	2 meses	Meses 5-6
5	Configuração de Replicação	Implementação de replicação de dados e sincronização	2 meses	Meses 7-8
6	Implementação de Sistemas	Instalação de aplicações e serviços no DR	2 meses	Meses 9-10
7	Testes de DR	Testes técnicos e funcionais (failover e fallback)	1 mês	Mês 11
8	Formação e Go-Live	Formação das equipas, documentação e entrada em operação	1 mês	Mês 12

16 FORMAÇÃO, TESTES E REVISÃO DO PLANO

16.1. Esta política é revisada, no mínimo, anualmente ou, ainda, por proposta da área responsável pelo gerenciamento do risco operacional da Distribuidora Valor ou em decorrência de factos relevantes que demonstrem sua ineficácia.

16.2. Pelo menos uma vez por ano, os procedimentos previstos nesta política serão submetidos a testes documentados de sua eficácia. Neste momento, as equipes envolvidas também colocarão em prática, como exercícios, as actividades aqui previstas.

16.3. O plano de continuidade de negócio deve ainda ser sujeito a uma revisão por parte dos Auditores internos da instituição ou através de mecanismos equivalentes que se adequem à dimensão

17 ENTRADA EM VIGOR E DIVULGAÇÃO

17.1. A presente Política entra em vigor imediatamente após a sua aprovação. Após a sua aprovação a mesma deve divulgada a todos os colaboradores relevantes para efeitos de continuidade do negócio.

****

Documentos revogados

N/A

Documentos complementares

- Lei n.º 22/15 – Código dos Valores Mobiliários
- Política de Segurança de Informação.

Elaborado por: Gabinete de Gestão de Risco e Gabinete de Sistemas de Informação

- O Conselho de Administração -

DISTRIBUIDORA VALOR, S.D.V.M. (SU), S.A.