Plano de Backup e Disaster Recovery

Complemento da Política de Segurança

Chief Information Security Officer

Versão 2.0

Índice

I– Controlo de Versão

Versão	Data	Nome	Ação (Elaboração, Revisão, Alteração, Aprovação)	Conteúdo
1.0	01/2016	Manuel Coquim	Elaboração	Primeira versão do documento.
2.0	09/01/2023	Alexandre Reverendo	Revisão	Revisão anual do documento
	20/05/2023	Gerência	Aprovação	

II– Sumário Executivo

Objetivos do Plano:

- Definir as regras aplicáveis com base na estrutura da **Nextweb** e
- Assegurar que todos conheçam o Plano de Backup e Disaster Recovery (PBDR).

Processos Vitais:

- Execução das ordens;
- Verificação das operações;
- Gestão dos riscos, limites e concentração;
- PLD;
- Comunicação à Administração.

Site de Contingência:

Localização	Rua António Lima Fragoso, 145 –3060-216 Cantanhede NOC da Nextweb – P.S.A.I. LDA
CONTATO	Alexandre Reverendo - Diretor Técnico
Telefones	Tel.: (351) 231 400 966 Tlm.: (351) 91 234 7666
e-mail	areverendo@nextweb.pt

Responsáveis pelo Plano de Backup e Disaster Recovery:

Staff	Nome	Telefones
Diretor de Contingência	Alexandre Reverendo	Tel: (351) 231 400 966 Tlm: (351) 91 234 7666
Administração	Libério Reverendo	Tel: (351) 231 400 965 Tlm: (351) 91 234 7665

III. Premissas e Objetivos do Plano

O Plano de Backup e Disaster Recovery (PBDR) assegurará à **NEXTWEB** a continuidade dos seus negócios em caso de paralisação, decorrente de sinistro, de um ou mais processos considerados críticos. O sinistro torna-se realidade quando ameaças internas ou externas exploram as vulnerabilidades dos processos.

Os processos críticos ao negócio da **NEXTWEB** foram mapeados por meio de levantamento de informações com os Gestores das principais áreas do negócio.

Para tanto, o PBDR é definido como (PBDR = PAC + PCO + PRD), a saber:

- PAC = Programa de Administração da Crise – É acionado após decretada a Crise, e é voltado para todo o processo. Tem o seu término quando se volta à normalidade;

- PCO = Plano de Continuidade Operacional – São acionados os primeiros procedimentos do PAC, e é voltado aos processos do negócio;

- PRD = Plano de Recuperação de desastres – É acionado junto com o PCO, e é focado na recuperação/restauração de componentes que suportam o PBDR.

O desenvolvimento do Plano de Backup e Disaster Recovery é baseado na avaliação dos processos críticos estabelecidos pela Administração compreendendo às suas principais etapas:

- Análise dos riscos de TI;

- Análise do Impacto nos Negócios (BIA);

- Estratégia de recuperação.

Desta forma será necessário simular situações de emergências, definir responsabilidades e escopo de atuação para cada colaborador na execução do PBDR. A manutenção do PBDR atualizado e o treino dos colaboradores são fatores crítico de sucesso.

IV. Site Principal e Site Redundância

A **NEXTWEB** conta com duas unidades: a principal e a de redundância.
A unidade principal (Site Principal) situa-se à Rua António Lima Fragoso, 145 3060-216 Cantanhede, onde a administração e operação do negócio é executada em condições normais.

A unidade de redundância (Site Redundância) contém todos os recursos tecnológicos da Unidade Principal, podendo cada posto de trabalho utilizar tanto a Unidade Principal como o Site de Redundância. Portanto, em situações de contingência, os funcionários designados devem-se dirigir para esse endereço de forma que haja o mínimo impacto possível dentro das atividades da **NEXTWEB**. Para reduzir esse impacto, o site de redundância contém um servidor espelho em tempo real do servidor do Site Principal da **NEXTWEB**.

IV.1. Site de Redundância

LOCALIZAÇÃO	Rua do Comércio, 4 - 3840-126 Covão do Lobo Escritório da Nextweb – P.S.A.I. Lda
CONTATO	Alexandre Reverendo - Diretor Técnico
TELEFONES	Tel: (351) 231 400 966 Tlm: (351) 91 234 7666
e-mail	areverendo@nextweb.pt

Em função do site de redundância atender aos processos críticos em caso de contingência, segue abaixo a designação do local que os colaboradores das áreas devem-se dirigir nessas situações:

Área	Local de Contingência
Gestão	Site Redundância
Risco e Compliance	Site Redundância
Comerciais e Serviços Técnicos	Home Office
Administrativo/Financeiro	Home Office
TI	Depende da situação

V. Plano de Monitoração e Declaração de Desastre

V.1. Definição de Desastre

Será considerado desastre quando o tempo total de recuperação dos processos for superior ao tempo máximo apontado no item VI – Processos e Sistemas Críticos.

V.2. Monitoração de Comunicação de Eventos

Qualquer colaborador da **NEXTWEB**, ao constatar alguma anormalidade que paralise quaisquer processos apontados no item VI deste Plano deverá comunicar o fato ao seu superior imediato, este por sua vez comunicará o fato ao Diretor de Contingência, a saber:

Staff	Nome	Telefones	E-mail
Diretor de Contingência	Alexandre Reverendo	Tel: (351) 231 400 966 Tlm: (351) 91 234 7666	areverendo@nextweb.pt alexdreverendo@gmail.com

Este é o meio de comunicação a ser utilizado pelos colaboradores da **NEXTWEB** como ponto central de contato para solicitar ajuda ou relatar alguma situação que demande o acionamento do PBDR.

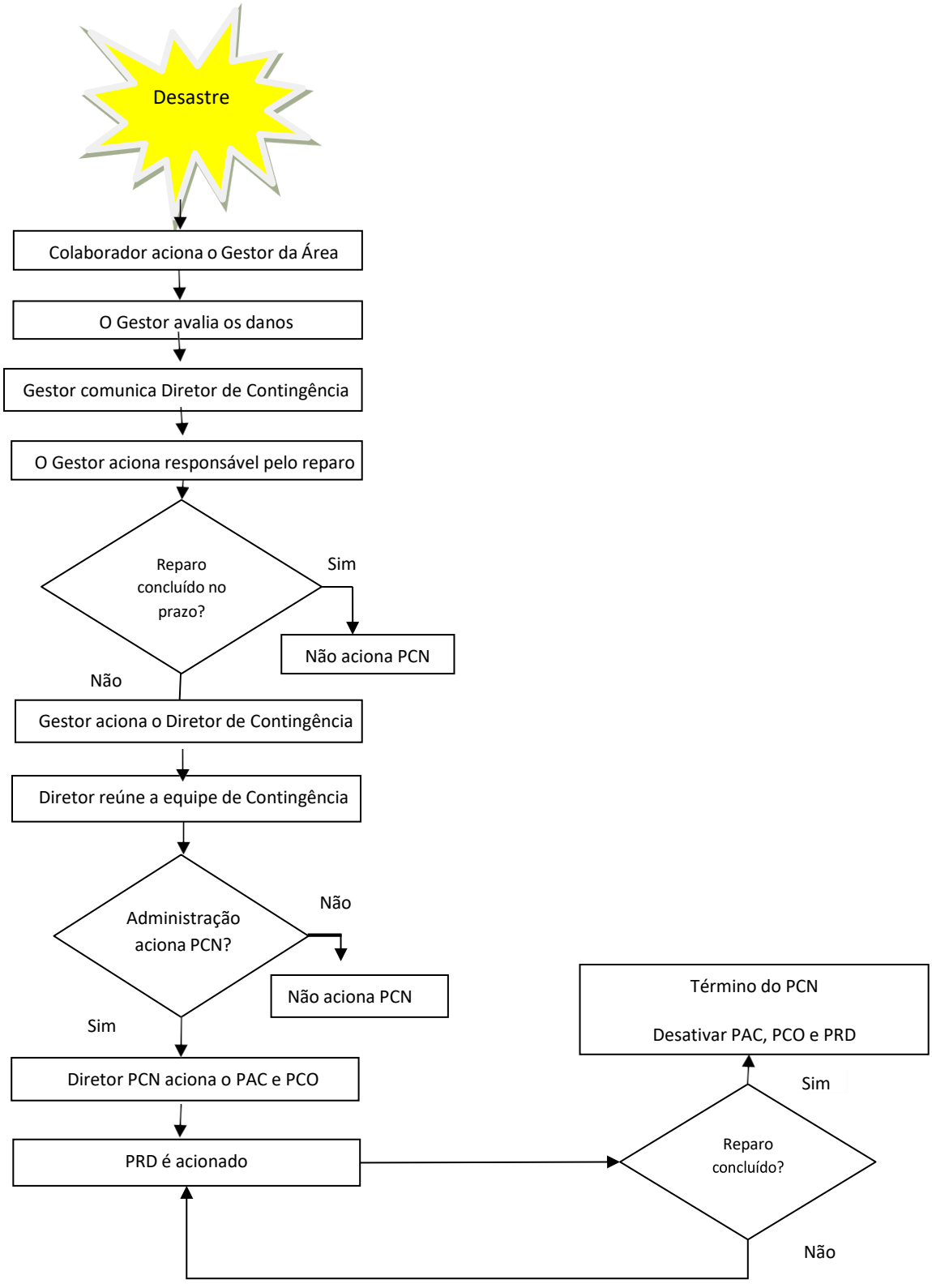
V.3. Declaração de Desastre/Contingência

Ao ocorrer quaisquer eventos que paralise algum processo essencial do negócio, o Diretor de Contingência avaliará a ocorrência e comunicará à Administração.

Com base nas informações recebidas e avaliação do grau de impacto versus horário crítico, compete ao Diretor declarar ou não a contingência.

Em caso da ausência do Diretor responsável pelo PBDR assumirá interinamente a Administração.

Na figura abaixo está descrito o Fluxo de Acionamento do PBDR que resultará ou não na declaração da contingência.


Desastre
Colaborador aciona o Gestor da Área
O Gestor avalia os danos
Gestor comunica Diretor de Contingência
O Gestor aciona responsável pelo reparo
Reparo concluído no prazo?
Sim
Não aciona PCN
Não
Gestor aciona o Diretor de Contingência
Diretor reúne a equipe de Contingência
Administração aciona PCN?
Não
Não aciona PCN
Sim
Diretor PCN aciona o PAC e PCO
PRD é acionado
Reparo concluído?
Sim
Término do PCN
Desativar PAC, PCO e PRD
Não

VI. Processos e Sistemas Críticos

Processo crítico pode ser definido como um processo de trabalho que uma vez paralisado por tempo superior ao definido pela unidade gestora do negócio irá afetar sensivelmente as operações e serviços da organização gerando maior impacto nos clientes internos e externos, definido pela fórmula (MTD = RTO + WRT).

Definição:

- MTD (Maximum Tolerable Downtime) = Trata-se do tempo máximo que um negócio pode tolerar a ausência ou indisponibilidade de uma função de um negócio em particular. Diferentes funções de negócio terão diferentes MTD's.

- RTO (Recovery Time Objective) = Tempo disponível para recuperar os sistemas e recursos de uma ruptura.

- WRT (Work Recovery Time) = Tempo que leva para copiar e rodar uma vez os sistemas (hardware, software e configuração) a serem restaurados para as funções dos negócios críticos.

VII. Abrangências

VII.1. Ameaças Relacionadas

No entendimento dos gestores das áreas avaliadas as ameaças com grau de vulnerabilidade significante estão divididas em:

a. Humanas

Greves, Distúrbio Civil, Falha do Prestador de Serviços/Parceiro, Acesso Indevido às Instalações e Erro Humano não intencional.

b. Tecnológicas

Falha em Aplicativos (SW), Falha em Hardware (HW), Falha em sistemas Operacionais, Vírus de Computador, Falha na Rede Interna (LAN), Falha na Entrada de Dados, Falha na Rede Externa (WAN), Falha de Telecom – Dados e Falha em Sistema de Acesso.

c. Infraestrutura

Falha em Telecom - Voz, Falha em Sistema de Refrigeração, Interrupção de Energia Elétrica, Falha em Instalações Elétricas.

d. Naturais

Alagamento Interno do Ambiente, Queda de Raios, Vendaval e Incêndio.

e. Físicas

Problema Estrutural ou de Instalações e Rompimento de Tubulação Interna (água, esgoto e gás).

Cabe ressaltar que paragens não programadas podem resultar em perdas tangíveis e intangíveis aos negócios da **NEXTWEB**, acarretando perda de confiança dos colaboradores e clientes nos processos do negócio. Desta forma, os potenciais impactos apontados pelos gestores numa eventual interrupção no negócio são:

- Interrupção da prestação de serviços a clientes;
- Multas e sanções;
- Perda da capacidade de gestão e controlo;
- Comprometimento da imagem da organização;
- Exposição negativa na mídia e perda da vantagem competitiva.

VIII. Ações e Procedimentos

Qualquer colaborador deverá estar apto a identificar as ameaças que possam levar a paralisação dos negócios e comunicar imediatamente ao Diretor do Plano de Backup e Disaster Recovery.

VIII.1. Impossibilidade de Acesso às Instalações

Dentre as ameaças que impossibilitam o acesso ao prédio destacamos:

- Princípio de Incêndio;
- Ameaça de Bomba;
- Bloqueios;
- Manifestações.

VIII.1.1. Ações de 05 a 10 minutos após a evidência

Responsável: Diretor do PBDR

Procedimentos:

- Bombeiros: 231 410 000 (Incêndio e Ameaça de Bomba);
- Proteção Civil: 231 410 118 (Ameaça de Bomba, Greves, Bloqueios e Inundações);
- GNR: 231 422 446 (Ameaça de Bomba, Roubo e Furto de Informações e ativos).
- **112**: Número Europeu de Emergência (pode ser ligado através dos telefones das redes fixa e móvel. A chamada é gratuita e é atendida de imediato pelos centros de emergência que acionam os sistemas médico, policial e de incêndio, consoante a situação verificada).

VIII.1.2. Ações em até 20 minutos após a conclusão da etapa anterior

- Entrar em contato com o responsável pelo site backup, conforme indicação no item 2, para avisá-lo sobre a ocupação dos integrantes das áreas contingenciadas e disponibilizar local, notebook e impressora, assim como acesso à Internet, bem como avisar os colaboradores que atuarão em regime Home Office.

- Avisar aos integrantes das áreas contingenciadas para que se dirijam ao endereço do site redundância, ou às suas residências para atuação no regime Home Office, conforme relação indicada abaixo:

ÁREA CONTINGENCIADA	NOME	CONTATO	E-MAIL
Comerciais e Serviços Técnicos	N/D	(351) 231 400 965	comercial@nextweb.pt helpdesk@nextweb.pt
Administrativo/Financeiro	Liberio Reverendo	(351) 91 234 7665	liberio@nextweb.pt
Compliance e Risco	Alexandre Reverendo	(351) 91 234 7666	areverendo@nextweb.pt alexdreverendo@gmail.com
Tecnologia da Informação	Alexandre Reverendo	(351) 91 234 7679 (351) 231 400 966	areverendo@nextweb.pt

- Disponibilizar alertas no site da NEXTWEB indicando o status da contingência, telefones dos colaboradores e telefone fixo do site backup para atendimento.

VIII.2 Falha na Infraestrutura e Tecnologia

Para não haver interrupções nas atividades o ambiente de TI no site principal da sede a Unidade de Redundância será o site de contingência da sede.

A comunicação entre as unidades de negócio é feita por links redundantes. A seguir destacamos a infraestrutura de TI de cada unidade de negócio.

- Servidores
- Telecom
- Energia Elétrica

Na falta de energia elétrica, além das baterias próprias dos computadores, são ativados automaticamente os nobreaks localizados no site principal no CPD com autonomia de 3 horas.

As áreas abastecidas pelos Nobreaks são as mesmas mapeadas com processos críticos pelo BIA.

- Datacenter
- Sistemas de Tecnologia de Informação
- Serviços BackOffice
- Dep. Administrativo/Financeiro
- Gestão de Riscos e Compliance

VIII.3 Acionamento da Contingência externa

As equipas irão para o lugar destinado a cada uma delas.

Manter contato com a empresa Telecomunicações (Manutenção do PABX) e solicitar o encaminhamento de todas as ligações para os ramais do escritório do Site de Contingência, se for o caso.

IX. Procedimentos de retorno à normalidade – Site Principal

Cabe ao Diretor da Contingência encerrar o PBDR e comunicar aos Administradores e aos Gestores envolvidos no processo.

Quando o acesso às instalações estiver liberado e em condições de normalidade, comunicar a todos os colaboradores da NEXTWEB por meio dos gestores para que retornem aos seus postos de trabalho no dia seguinte.

Solicitar à área de TI que retire o comunicado publicado no site da NEXTWEB sobre a situação de contingência.

X. Administração do Plano

A continuidade dos negócios de uma organização, assim como a recuperação de desastres é o resultado da execução e da manutenção de um processo contínuo que envolve planeamento, formalização, monitorização e melhorias.

O processo de Continuidade dos Negócios é de responsabilidade e gestão da área Compliance, que determina o ciclo e as etapas que deverão ser executadas para que tanto os cenários de risco e impacto sobre os negócios como as estruturas e estratégias que embasam o PBDR possam ser atualizadas refletindo o ambiente de negócios da NEXTWEB.

X.1 Divulgação e Treino

Um dos fatores primordiais para o funcionamento deste plano são o conhecimento e a familiaridade das pessoas e dos demais envolvidos na execução das atividades de continuidade de negócios e recuperação de desastres com as estratégias e recursos definidos no planeamento.

Para que seja possível esta familiaridade e conhecimento do plano, conferindo-lhe credibilidade, a equipa da NEXTWEB definiu que serão realizadas anualmente sessões de divulgação a todos os colaboradores e envolvidos no plano.

Para que este conhecimento seja preservado, os colaboradores admitidos e os transferidos para funções de negócios críticos, principalmente aqueles que pertencem à equipa de contingência, deverão ser instruídos das suas respetivas responsabilidades no plano.

O programa de treino deverá contemplar os riscos, ameaças, controlos, responsabilidades, premissas e as estratégias do PBDR, incluindo as alterações recentes.

X.2 Realização de Testes

Os testes têm por objetivo assegurar a eficiência e a efetividade do PBDR e deverão ser planeados e executados com periodicidade mínima anual a partir da data da sua implantação.

A responsabilidade pelo planeamento e organização dos testes, assim como pela definição dos cenários a serem contemplados é da área de Tecnologia da Informação.

Os testes não deverão provocar quaisquer tipos de indisponibilidade ou parada nos ambientes de negócios da NEXTWEB e deverão ser conduzidos pela equipa de contingência em total conformidade com o definido. As simulações deverão ser realizadas sobre cenários e ameaças contemplados no plano, devendo cobrir os riscos e ameaças com maior probabilidade de ocorrência.