inetum
Positive digital flow

Plano de Continuidade de Negócio

Inetum Portugal

V1

Índice

1. Missão e Objetivos

O Plano de Continuidade de Negócio tem como **Missão** garantir a continuidade do funcionamento das operações da Inetum em Portugal, em situações de crise, de curto ou longo prazo, minimizando a interrupção das atividades, durante a mesma, garantindo a segurança dos colaboradores, a proteção dos ativos e a manutenção das atividades essenciais para o negócio.

O Plano de Continuidade de Negócio estabelece as ações, que a Inetum deve tomar, para que as atividades consideradas críticas para a continuidade da organização – processos de negócio ou de suporte direto ao negócio – possam ser mantidas na sequência de evento disruptivo.

O objetivo do plano é orientar a organização, perante uma disrupção, e restabelecer efetivamente as operações críticas de negócio no menor período possível, com perda mínima de dados.

Este plano tem como **Objetivos**:

- Garantir a segurança e proteção de pessoas e bens;
- Responder de forma eficaz e rápida a eventos disruptivos, reduzindo o tempo de inatividade de processos e operações críticas de negócio;
- Minimizar perdas financeiras para preservação de ativos críticos da organização;
- Mitigar os efeitos negativos que eventos disruptivos possam ter no planeamento estratégico da organização, na sua reputação, operações, capacidade de prestação de serviços e capacidade de permanecer em conformidade com leis, regulamentos e contratos;
- Ajudar na tomada de decisões durante situações de desastre;
- Permitir que a organização retorne às operações normais e controladas;
- Formar e consciencializar os colaboradores para que possam e saibam como agir durante uma crise.

2. Âmbito

Este Plano atua sobre interrupções das operações da Inetum em Portugal, de curta e longa duração, e tem âmbito circunscrito aos processos identificados como críticos, na matriz de análise de impacto de negócio, anexa a este plano, e aos ativos críticos relacionados com os mesmos.

O Plano de Continuidade de Negócio articula com Planos de Recuperação, onde se estabelecem as medidas e procedimentos a serem adotados em caso de falhas ou interrupções, nos sistemas e infraestruturas, que constituem os ativos tecnológicos críticos.

O Plano de Continuidade de Negócio relaciona-se com o Plano de Emergência Interno (no âmbito das MAP's SCIE) e Outros Planos de Contingência, onde se estabelecem instruções e procedimentos a serem executados durante emergências, relativamente a um conjunto de fatores de risco de natureza física, natural e social.

2.1. Eventos Disruptivos

Identificam-se seguidamente os eventos disruptivos considerados no âmbito do Plano de Continuidade de Negócio, tipificados de acordo com a sua origem (externa e interna) e a sua natureza (abaixo identificada), devidamente articulados com as situações de risco organizacionais e operacionais, identificadas nas metodologias e matrizes de gestão de risco.

Natureza	Origem	Eventos Disruptivos
Negócio	Interna	• Corrupção e infrações conexas no âmbito da atividade de negócio e suporte ao negócio • Quebra contratual com clientes relevantes • Quebra contratual de parceiros e/ou fornecedores relevantes • Alterações de legislação
Operacional	Interna	• Alterações dos recursos de IT (manutenção corretiva ou evolutiva; alterações físicas ou lógicas) • Falha dos recursos de IT (físicas ou lógicas) • Falha de comunicações • Falha de energia
Tecnológico e Humano	Externa	• Acesso/Utilização indevido a recursos de IT (negligente ou ilícito / físico ou lógico) • Ataque informático (vírus, phishing, spam, ataques DoS "negação do serviço" e DDoS "negação distribuída do serviço") • Atos de sabotagem (pacote suspeito, ameaças de bomba) • Roubo/Violação de informação
Técnico e Natural	Externa	• Explosão • Incêndio • Inundação • Sismo • Cheia
Biológica	Externa	• Pandemias • Epidemia • Surto

2.2. Impacto dos Eventos Disruptivos

Os eventos disruptivos identificados no ponto anterior, podem ter impacto na continuidade das operações da Inetum, quando atingem processos relevantes, tendo em conta a duração da disrupção, estando devidamente identificados na matriz de análise de impacto de negócio, anexa a este plano.

Os impactos podem ser tipificados do seguinte modo:

Impacto	Imagem	Contratual
Baixo	Sem impacto na imagem da Inetum junto dos clientes e outras partes interessadas.	Sem incumprimento de compromissos contratuais ou legais.
Médio	Imagem da Inetum afetada de forma moderada junto de um conjunto restrito de clientes e outras partes interessadas.	Incumprimento de compromissos contratuais ou legais, sem aplicação de coimas e/ou indeminizações e/ou sem processos judiciais por parte dos clientes ou parceiros. e Sem perda de contratos.
Alto	Imagem da Inetum é afetada de forma moderada junto de um conjunto alargado de clientes e outras partes interessadas. ou Imagem da Inetum afetada de forma severa junto de um conjunto restrito de clientes ou outras partes interessadas relevantes.	Incumprimento de compromissos contratuais, com possibilidade de aplicação de coimas e/ou indeminizações e/ou processos judiciais por parte dos clientes ou parceiros. e Sem perda de contratos.
Muito Alto	Imagem da Inetum afetada de forma severa junto de um conjunto alargado de clientes e outras partes interessadas.	Incumprimento de compromissos contratuais, com possibilidade de aplicação de coimas e/ou indeminizações e/ou processos judiciais por parte dos clientes ou parceiros. e Perda de contratos.

2.3. Ativos de Informação e Componentes de Serviço abrangidos

Ativos de informação e componentes de serviço, identificados como críticos na Framework de Ativos de Informação e Componentes de Serviço, e que estão relacionados com os processos críticos identificados na matriz de análise de impacto de negócio, anexa a este plano.

Estes ativos de informação e componentes de serviço quando expostos a situações que possam provocar violação, degradação ou falha/interrupção não planeada, podem pôr em causa a operação da Inetum.

A criticidade dos ativos de informação e componentes de serviço está classificada na mencionada Framework, confirme regulamentada no processo PTI05 - Gestão de Ativos de Informação e Componentes de Serviço.

3. Estrutura de Continuidade

De forma a operacionalizar e garantir que as ações necessárias à devida execução deste plano, foram constituídas equipas específicas, com identificação de responsabilidade macros, atribuídas a funções chave nas diversas áreas da estrutura organizacional:

	Responsabilidades Macro	Funções na Organização
Comité de Gestão da Continuidade do Negócio	• Definir o Plano de Continuidade de Negócio • Gerir taticamente a crise • Gerir a comunicação em cenário de crise • Avaliação do impacto	• Country Manager • CIO • CISO • Diretores de BL e BU • Direção Delivery Excellence • Direção RH • Direção Legal & Compliance • Direção de Comunicação • Direção Facilities • Direção Financeira • Direção QSP
Comando Operacional Emergência (COE)	• Ativar o Plano de Continuidade de Negócio e planos específicos • Coordenação das equipas atribuídas aos planos específicos	• CIO • CISO • Diretores de BL e BU • Direção Delivery Excellence
Equipa de Recuperação de Negócio	• Operacionalizar o Plano de Continuidade de Negócio, na vertente da gestão dos processos • Recuperar processos e retoma à normalidade	• Equipa de gestão dos processos afetados ou relacionados • Elementos-chave dos processos afetados ou relacionados
Equipa de Recuperação de Tecnológica	• Operacionalizar o Plano de Continuidade de Negócio, nos ativos críticos de natureza tecnológica, de acordo com o Plano de Recuperação Tecnológica • Recuperar ativos e retomar à normalidade	• Equipa DSI de resposta e recuperação
Delegado de Segurança das Instalações	• Ativar o Plano de Emergência Interna no âmbito das MAPs • Retomar à normalidade	• Delegados de Segurança (função que pode estar subcontratada)
Equipa de Emergência	• Operacionalizar o Plano de Emergência Interna no âmbito das MAPs • Retomar à normalidade	• Equipa de 1ª intervenção (função que pode estar subcontratada) • Equipa de Evacuação • Equipa de 1ºs socorros

4. Vertente Preventiva do Plano

A vertente preventiva do Plano de Continuidade de Negócio consubstancia-se no seguinte conjunto de políticas e práticas formalizadas:

- Estrutura de Continuidade, definida no presente plano
- PO01_PIT04_Política de Segurança de Informação
- PO02_PIT04_Política de Privacidade e Proteção de Dados
- PO03_PIT04_Política de Uso Aceitável de Ativos de Informação
- PO04_PIT04_Política de Classificação e Tratamento da Informação
- PO05_PIT04_Políticas de Gestão de Acessos (lógicos e físicos)
- PO06_PIT04_Política de Gestão Backups&Restores
- PO07_PIT04 – Política de Criptografia
- PO08_PIT04 – Política de Desenvolvimento Seguro
- PO09_PIT04_Política de Segurança Física; Procedimentos relacionados
- M03_PIT04_Metodologia de Gestão de Riscos
- PRHXX – Processos de Gestão de Recursos humanos
- PRFXX – Processos de Gestão de Financeira
- PCPXX – Processos de Delivery
- PIT01 – Processo de Gestão do Sistema de Informação Interno
- PIT05 – Processo Gestão de Ativos de Informação e Componentes de Serviço
- M04_PIT04 – Procedimento de Gestão de Ameaças e Vulnerabilidades
- M01_PIT04 – Procedimento de Gestão de Incidentes de Segurança da Informação
- M02_PIT01 – Procedimento de Gestão de Alterações e Configurações
- Plano de Corrupção e Infrações Conexas
- Procedimento de Internal Controls

4.1. Gestão de recursos em situação de normalidade

Em situação normal de operação a gestão de recursos é assumida no âmbito dos processos de Recursos Humanos, Recursos Financeiros e Recursos Tecnológicos.

4.2. Gestão de Redundâncias

Os recursos em emergência – materiais (infraestruturas e equipamentos), TI's e humanos – disponíveis ou a acautelar para operacionalização dos planos de atuação considerados na vertente de interventiva deste Plano de Disponibilidade e Continuidade, sintetizam-se seguidamente.

- **Energia**
  - UPS no Data Center Torre de Monsanto (autonomia 20 min) – destinada a comunicações
  - UPS do Centro de Serviços de Lisboa
  - Estrutura de emergência do edifício (suficiente para evacuação)

- **Comunicações (internas e externas)**

  Formas alternativas de acesso aos sistemas dos clientes:
  - Configuração alternativa do SAP Router (ativação manual)
  - Configuração alternativa do front-end SAP (ativação manual)
  - Ligação por cliente VPN quando fora das instalações
  - Ligação por cliente VPN aos clientes e/ou túneis VPN site-site aos clientes
  - Links backup de comunicações em todas as Localizações da Inetum
  - Telemóveis com acessos de dados (internet)
  - Placas de dados móveis (internet)

- **Deslocalização backup**
  - Deslocalização dos backups, para site secundário, no âmbito do serviço subcontratado de virtual Datacenter

- **Equipamentos portáteis**
  - Computadores portáteis com autonomia suficiente e com políticas de segurança implementadas transversalmente

- **Instalações físicas**
  - Escritórios da Inetum situados em: Algés (Torre de Monsanto); Entrecampos; Porto; Covilhã; Bragança; Lisboa (Entrecampos)
  - Teletrabalho

- **Recursos Humanos**
  - Comité de Gestão da Continuidade do Negócio
  - Comando Operacional Emergência (COE)
  - Equipa de Recuperação de Negócio
  - Equipa de Recuperação de Tecnológica
  - Delegado de Segurança das Instalações
  - Equipa de Emergência

4.3. Níveis de Serviço em Situações de Crise

Numa emergência, durante a ativação da vertente interventiva o nível de serviço mais exigente relativo ao "tempo de resposta" passa a ser 4h, tanto para os serviços SAM, serviços Basis 24x7 e HelpDesk aos sistemas de informação, mantendo-se os restantes níveis: 12h e 36h. A alteração aos níveis de serviço da SAM em emergência é dada a conhecer aos clientes, nos casos aplicáveis, da forma mais adequada.

4.4. Gestão da Disponibilidade e Continuidade

A. Monitorização, Análise e Controlo

A monitorização, análise e controlo da disponibilidade e continuidade dos processos críticos e ativos relacionados, identificados na matriz de análise de impacto de negócios anexa a este plano, são garantidos na condução dos respetivos processos.

B. Estratégia de Ativação do Plano

De acordo com a natureza dos eventos disruptivos, tendo em conta as áreas de impacto Pessoas, Financeiro, Instalações e Sistemas Informação, são adotados diferentes critérios de ativação do plano de continuidade, que determinam a adoção de diferentes soluções de recuperação e equipas a mobilizar.

Natureza dos Eventos	Áreas Impacto	Critérios de Ativação do Plano de Continuidade	Planos Ativados (detalhe em 5.1)	Equipas Mobilizadas
Negócio	Pessoas Financeiro	De acordo com a avaliação de ativação do plano decorrente da análise de impacto de negócio, evidenciada na matriz anexa a este plano	Plano de Continuidade de Negócio Plano de Prevenção de Corrupção e Infrações Conexas (se aplicável)	Comité de Gestão da Continuidade do Negócio Comando Operacional Emergência (COE) Equipa de Recuperação de Negócio
Operacional	Financeiro Instalações Sistemas Informação	É expectável que se ultrapasse os parâmetros de continuidade RTO e RPO estabelecidos, nos ativos críticos1 afetados	Plano de Continuidade de Negócio Planos de Recuperação (Plano Disaster Recovery tecnológico, se aplicável)	Comité de Gestão da Continuidade do Negócio Comando Operacional Emergência (COE) Equipa de Recuperação de Negócio Equipa de Recuperação de Tecnológica
Tecnológico e Humano	Pessoas Financeiro Sistemas Informação	É expectável que se ultrapasse os parâmetros de continuidade RTO e RPO estabelecidos, nos ativos críticos[1] afetados	Plano de Continuidade de Negócio Planos de Recuperação	Comité de Gestão da Continuidade do Negócio Comando Operacional Emergência (COE) Equipa de Recuperação de Negócio Equipa de Recuperação de Tecnológica
Técnico e Natural	Pessoas Financeiro Instalações Sistemas Informação	É expectável que se ultrapasse os parâmetros de continuidade RTO e RPO estabelecidos, nos ativos críticos[1] afetados	Plano de Continuidade de Negócio Plano de Recuperação (Plano de Emergência	Comité de Gestão da Continuidade do Negócio Comando Operacional Emergência (COE)

[1] De acordo com os critérios definidos na matriz de análise de impacto de negócio, anexa a este plano

Natureza dos Eventos	Áreas Impacto	Critérios de Ativação do Plano de Continuidade	Planos Ativados (detalhe em 5.1)	Equipas Mobilizadas
			Interno, se aplicável)	Equipa de Recuperação de Negócio Equipa de Recuperação de Tecnológica Delegado de Segurança das Instalações Equipa de Segurança
Biológica	Pessoas Financeiro Instalações	• Declaração de Pandemia • Declaração de Epidemia, para as áreas afetadas • Declaração de surto, quando determina a evacuação de instalações	Plano de Continuidade de Negócio, com possível criação de plano de contingência	Comité de Gestão da Continuidade do Negócio Comando Operacional Emergência (COE) Equipa de Recuperação de Negócio

C. Parâmetros de Continuidade

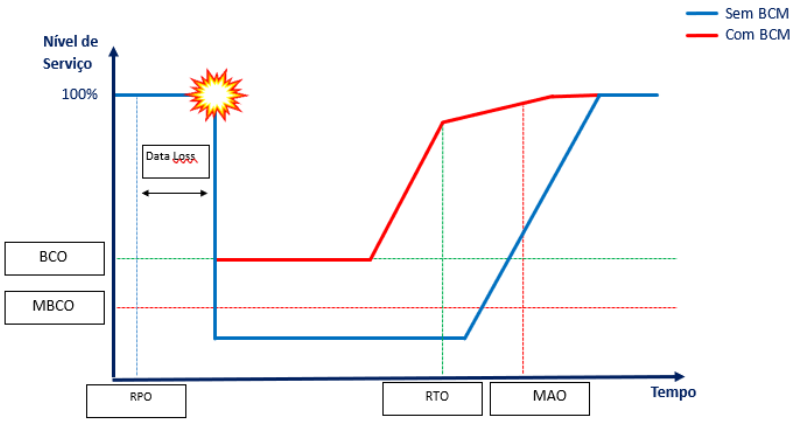
A gestão da continuidade de negócio é caraterizada e quantificada parâmetros de continuidade, tendo por base os seguintes conceitos e definições:

- Objetivo de ponto de recuperação (RPO - Recovery Point Objective) - Ponto até ao qual a informação utilizada por uma atividade/serviço tem de ser restabelecida para permitir que a atividade funcione no seu recomeço. Isto é, qual a quantidade de dados, medida em tempo, que aceitamos perder?

- Objetivo de tempo de recuperação (RTO - Recovery Time Objetive) - Período, após um incidente, dentro do qual um serviço ou uma atividade pode ser retomada ou os recursos sejam recuperados sem impacto inaceitável para o negócio/prestação do serviço. Isto é, qual o tempo necessário para restaurarmos um serviço ou sistema?

- Interrupção máxima aceitável (MAO – Maximum Acceptable Outage) - Tempo que levará para que os impactos adversos, que possam surgir como resultado do não fornecimento de um produto/serviço ou da não realização de uma atividade, se tornem inaceitáveis. Isto é, qual o tempo máximo que toleramos ficar sem um serviço ou sistema?

Os diagramas seguintes ilustram através de representação gráfica estes conceitos tem por base, grandezas como o tempo e níveis de serviço associados à indisponibilidade na entrega e ao informação perdida.



BCO – Business Continuity Objective

MBCO – Minimum Business Continuity Objective

RPO – Recovery Point Objective

RTO – Recovery Time Objective

MAO - Maximum Acceptable Objective

RTO (Recovery Time Objective): Em caso de desastre, quanto tempo podem os processos de negócio estar em baixo?

RPO (Recovery Point Objective): Em caso de desastre, qual a quantidade de dados que o negócio tolera perder?

D. Modelos de Testes ao Plano

Os testes ao presente plano permitem verificar a sua eficácia, validando a exequibilidade dos valores dos parâmetros de continuidade, RPO e RTO, estabelecidos para os recursos críticos de IT, avaliando os níveis de prontidão, da organização, relativamente aos planos de recuperação instituídos e estabelecendo possíveis ações de melhoria.

Foram definidos os seguintes **modelos de teste** ao Plano:

Modelos	Descrição
Simulacro	Exercício planeado que simula, em contexto reais, uma ou mais situações de crise, identificadas neste plano.
Table Top	Exercício simulado com objetivo de testar, de uma forma holística, o plano de continuidade de negócio. Na sua realização pode utilizar informações de histórico de simulacros realizados ao plano ou decorrentes da condução de processos e procedimentos operativos.

Os cenários de teste ao Plano são estabelecidos de entre os eventos disruptivos, identificados no ponto 2.1. e operacionalizados de acordo com o estalecido no capítulo 5.

A Inetum deve garantir a realização de pelo menos um simulacro anualmente.

5. Vertente de Intervenção do Plano

O Plano de Continuidade de Negócio é operacionalizado através do estabelecimento de Planos de Recuperação relacionados aos eventos disruptivos identificados na seção 2.1 Impacto dos Eventos Disruptivos, estabelecendo procedimentos de intervenção a serem adotados e interligados conforme apresentado na seção 4.4 Gestão da Disponibilidade e Continuidade e detalhados na seção seguinte.

5.1. Planos de Recuperação

Na tabela seguinte apresentam-se os **Planos de Recuperação** considerados no **Plano de Continuidade de Negócio da Inetum** relativos às várias naturezas de eventos disruptivos considerados para os quais se pretende dar resposta, relacionados com os processos críticos e ativos críticos identificados na matriz de análise de impacto de negócio, anexa a este plano.

A estrutura e o detalhe de cada Plano de Recuperação constam definida em documento associado a este plano.

Descreve-se seguidamente os itens da estrutura de cada Plano de Recuperação:

- Identificação da natureza da disrupção (conforme tabela do capítulo 2.1 Impacto dos Eventos Disruptivos deste plano);
- Riscos relacionados – organizacionais ou disponibilidades de serviços e segurança da informação - conforme, respetivamente: Matriz "Riscos e Oportunidades" Organizacionais e Matriz "Apreciação e Tratamento do Risco para Disponibilidade & Continuidade dos Serviços & Segurança da informação";
- Processos críticos e Ativos Críticos relacionados, conforme Análise de Impacto no Negócio, anexa a este documento;
- Etapas de atuação - Identificação dos vários momentos que constituem a evolução do incidente/emergência: Início: Decisão de Ativação do Plano; Atuação durante a Disrupção/Emergência; Fim da Emergência; e, Reposição da Normalidade;
- Cadeia de Decisão e Atuação - Decisões/atuações de carater logístico e técnico e respetivos recursos/ferramentas associados;
- Responsáveis/Intervenientes - Identificação dos elementos da cadeia de comando e de outros envolvidos em cada etapa de atuação.

As decisões de ativação do Plano de Continuidade de Negócio e de declaração do fim da disrupção/emergência com reposição da normalidade, fundamentam-se nos três conceitos e parâmetros inerentes à gestão da continuidade de negócio, descritos em 4.4 C Parâmetros de Continuidade (RPO, RTO e MAO).

Os valores dos parâmetros RPO e RTO são estabelecidos para os ativos de informação inventariados (na Framework de Ativos de Informação e Componentes de Serviço) sempre que aplicável, e encontram-se registos na matriz anexa à PO06_PRI04_Política de Gestão Backups & Restores.

Plano Recuperação	Evento Disruptivo	Processos Críticos	Riscos	Ativos Inform Comp.Serviço [2]	Planos Ativados/ Evocados
Plano Recuperação Nº 1	**Negócio** Quebra relação comercial com cliente relevante (€) / estratégico OU Rescisão de contrato com cliente (valor €)	**PCO01**-Gestão de Oportunidade de Negócio **PLC01**-Legal Corporate & Compliance **PRF02**-Gestão Faturação e Cobrança	[3]	Contratos de Clientes	Plano Continui-dade Negócio **(PCN)**
Plano Recuperação Nº 2	**Negócio** Quebra contratual de parceiros e/ou fornecedores relevante (€) / estratégicos	**PCO02** - Gestão de Parcerias **PCF01** - Compras e Gestão Fornecedores **PLC01-**Legal Corporate & Compliance	[3]	Contratos de Clientes Contratos de Fornecedores	**PCN**
Plano Recuperação Nº 3	**Negócio** Corrupção e infrações conexas na atividade de negócio e/ou suporte ao negócio	**PCO01** - Gestão de Oportunidade de Negócio **PLC01**-Legal Corporate & Compliance **PRH01 -** Gestão de Recrutamento e Seleção	[3]	Contratos de Clientes Contratos de Fornecedores	**PCN** Plano Prevenção da Corrupção e Infrações Conexas
Plano Recuperação Nº4	**Operacional** Falha em aplicações críticas e infraestruturas de IT críticas	**PIT01** - Gestão do Sist. Informação Interno **PCP01, PCP03, PCP04, PCP05 -** Processos de Delivery	**R1**[4] **R2**[4]	Ferramentas Aplicações Infraestruturas Configurações Serviços	**PCN** Plano DR tecnológico
Plano Recuperação Nº5	**Operacional** Alterações mal-sucedidas em aplicações críticas e infraestruturas de IT críticas	**PIT01** - Gestão do Sist. Informação Interno **PCP01, PCP03, PCP04, PCP05 -** Processos de Delivery	**R1**[4] **R2**[4]	Ferramentas Aplicações Infraestruturas Configurações Serviços	**PCN** Plano DR tecnológico
Plano Recuperação Nº6	**Operacional** Falha de Energia e/ou Comunicações	**PMC01** - Comunicação **PIT01** - Gestão do Sistema Informação Interno	**R4**[4]	Ferramentas Infraestruturas Aplicações Serviços	**PCN** Plano DR tecnológico
Plano Recuperação Nº7	**Tecnológico e Humano** Acesso Indevido (Físico ou Lógico) OU Roubo/Violação Informação OU Ataque informático ou de Sabotagem	**PIT01** - Gestão do Sist. Informação Interno **PIT04** - Gestão da Segurança de Informação **PRH02 -** Gestão Administrativa de Recursos Humanos	**R3**[4] **R5**[4]	Ferramentas Aplicações Serviços Informação documentada	**PCN** Plano DR tecnológico
Plano Recuperação Nº8	**Técnico e Natural** Explosão / Incêndio Sismo / Cheia	**PMC01 -** Comunicação **PIT01** - Gestão do Sist. Informação Interno **PRH02 -** Gestão Administrativa de Recursos Humanos	**R6**[4] **R8**[4]	Ferramentas Aplicações Infraestruturas Configurações Serviços Instalações	**PCN** Plano DR tecnológico PEI (Plano Emergência Interno) das MAP-SCIE

[2] Conforme Framework de Ativos de Informação e Componentes de Serviço
[3] Matriz "Riscos e Oportunidades" Organizacionais
[4] Matriz "Apreciação Tratamento Risco para Disponibilidade & Continuidade Serviços & Segurança da informação"

Plano Recuperação	Evento Disruptivo	Processos Críticos	Riscos	Ativos Inform Comp.Serviço [2]	Planos Ativados/ Evocados
Plano Recuperação Nº9	**Biológico** Pandemia / Epidemia	**PRH01 -** Gestão de Recrutamento e Seleção **PRH02** - Gestão Administrativa de Recursos Humanos **PMC01** - Comunicação **PIT01** - Gestão do Sist. Informação Interno	**R7**[4]	Estruturas organizativas Instalações	**PCN** Plano Contingência (pandemia ou epidemia)

5.2. Testes ao Plano de Continuidade de Negócio

Os testes ao Plano de Continuidade de Negócio são assegurados conforme estabelecido no ponto 4.4 Gestão da Disponibilidade e Continuidade.

A elaboração do Guião de suporte aos testes fundamenta-se nos **planos de recuperação** apresentados em 5.1 Planos de Recuperação.

O Relatório, a elaborar em cada teste ao plano, constituiu o registo da realização do teste e das suas conclusões, contendo a seguinte estrutura: objetivo, descrição das ações, intervenientes e recursos utilizados, notas dos observadores (para correção ou melhoria) e conclusões relevantes.

A estrutura do Guião e do Relatório de Teste ao Plano de Continuidade é apresentada em Anexo a este documento.

6. Glossário

MAP's – Medidas de Autoproteção

MAO – Maximum Acceptable Outage

PCN – Plano de Continuidade de Negócio

RTO - Recovery Time Objective

RPO - Recovery Point Objective

SCIE – Segurança Contra Incêndios em Edifícios

7. Revisão

A presente política é revista anualmente e produzida nova versão sempre que aplicável, com base nos requisitos de negócio, tecnologia, instalações e pessoas.

8. Documentos associados

PIT02 "Gestão da Disponibilidade e Continuidade"

F01_PIT02_Guião Teste ao Plano Continuidade de Negócio

F02_PIT02_Relatório Teste ao Plano Continuidade de Negócio_ Plano Ações

F03_PIT02_PCN_Planos_Recuperação

Matriz "Apreciação e Tratamento do Risco para Disponibilidade & Continuidade dos Serviços & Segurança da informação" (anexa ao caraterizador do processo PIT04 "Gestão da Segurança da Informação"

Framework de Ativos de Informação e Componentes de Serviço (anexa ao caraterizador do processo PIT05 "Gestão de Ativos Informação e Componentes de Serviço").

Matriz "Gestão de Acessos e Backups" (anexa à PO06_PRI04_Política de Gestão Backups & Restores)

9. Referências

NP ISO 31000:2018 Gestão do Risco - Princípios e linhas de orientação

NP EN ISO 22301:2020 - Sistema de Gestão da Continuidade de Negócio – Requisitos

Norma NP ISO/IEC 20000-1:2018 – " Tecnologias de Informação / Gestão de Serviços; Parte 1: Requisitos do sistema de gestão de serviços"

Norma ISO/IEC 27001:2022 - Information security, cybersecurity and privacy protection — Information security management systems — Requirements