

Gestão de Continuidade de Negócios Teórico – A Família ISO 22300

Prof. Luis Claudio, M.Sc., PMP®



ABNT CAPACITAÇÃO

VOCE SABIA QUE A ABNT
TEM TAMBÉM UMA ÁREA
DE CAPACITAÇÃO EM
NORMAS TÉCNICAS?

32 TEMAS

COM MAIS DE 100 CURSOS
PARA VOCÊ SE CAPACITAR!



Para mais informações:
cursos@abnt.org.br ou
(11) 2344-1721 / 2344-1722



Norma Técnica

Código

ABNT NBR 15999-1:2007 Versão Corrigida:2008 **CANCELADA**

Data de Publicação : 22/10/2007

Válida a partir de : 22/11/2007

Título : Gestão de continuidade de negócios
Parte 1: Código de prática

Título Idioma Sec. : Business continuity management Part 1: Code of practice

Nota de Título : Esta versão corrigida da ABNT NBR 15999-1:2007 incorpora a Errata 1 de 01.02.2008. Confirmada em 23.10.2014

Comitê : ABNT/CEE-063 Gestão de Riscos

Páginas : 40

Status : Cancelada em 05/10/2015 **Substituída por :** ABNT NBR ISO 22313:2015

Idioma : Português

**Motivo do
Cancelamento :**

Organismo : ABNT - Associação Brasileira de Normas Técnicas

Objetivo : Esta Norma estabelece o processo, os princípios e a terminologia da gestão da continuidade de negócios (GCN). O propósito desta Norma é fornecer uma base para que se possa entender, desenvolver e implementar a continuidade de negócios em uma organização além de obter confiança nos negócios da organização com clientes e outras organizações. Ela permite também que a organização avalie sua capacidade de GCN de uma maneira consistente e reconhecida.



CONTINUAR
PESQUISANDO

ABNT CAPACITAÇÃO

VOCÊ SABIA QUE A ABNT
TEM TAMBÉM UMA ÁREA
DE CAPACITAÇÃO EM
NORMAS TÉCNICAS?

32 TEMAS

COM MAIS DE 100 CURSOS
PARA VOCÊ SE CAPACITAR!



Para mais informações:
cursos@abnt.org.br ou
(11) 2344-1721 / 2344-1722



Norma Técnica

Código

ABNT NBR 15999-2:2008 **CANCELADA**

Data de Publicação : 10/11/2008

Válida a partir de : 10/12/2008

Título : Gestão de continuidade de negócios
Parte 2: Requisitos

Título Idioma Sec. : Business continuity management Part 2: Specification

Comitê : ABNT/CEE-063 Gestão de Riscos

Páginas : 19

Status : Cancelada em 06/06/2013 **Substituída por :** ABNT NBR ISO 22301:2013

Idioma : Português

**Motivo do
Cancelamento :**

Organismo : ABNT - Associação Brasileira de Normas Técnicas

Objetivo : Esta Norma especifica os requisitos para planejar, estabelecer, implementar, operar, monitorar, analisar criticamente, exercitar, manter e melhorar o SGCN documentado dentro do contexto dos riscos de negócios de toda a organização.



CONTINUAR
PESQUISANDO



Normas Necessárias para a aplicação da **ABNT NBR 15999-2:2008**

ISO 22301:2019(en) Security and resilience — Business continuity management systems — Requirements

Table of contents

- Foreword
- Introduction
- 1 Scope
- 2 Normative references
- 3 Terms and definitions
- ▼ 4 Context of the organization
 - 4.1 Understanding the organization
 - ▶ 4.2 Understanding the needs and expectations
 - ▶ 4.3 Determining the scope of the business continuity management system
 - 4.4 Business continuity management system
- ▼ 5 Leadership
 - 5.1 Leadership and commitment
 - ▶ 5.2 Policy
 - 5.3 Roles, responsibilities and authorities
- ▼ 6 Planning
 - ▶ 6.1 Actions to address risks and opportunities
 - ▶ 6.2 Business continuity objectives and planning
 - 6.3 Planning changes to the business continuity management system
- ▼ 7 Support
 - 7.1 Resources
 - 7.2 Competence
 - 7.3 Awareness
 - 7.4 Communication
 - ▶ 7.5 Documented information
- ▼ 8 Operation
 - 8.1 Operational planning and control
 - ▶ 8.2 Business impact analysis and risk assessment
 - ▶ 8.3 Business continuity strategies and plans
 - ▶ 8.4 Business continuity plans and procedures
 - 8.5 Exercise programme
 - 8.6 Evaluation of business continuity management system
- ▼ 9 Performance evaluation
 - 9.1 Monitoring, measurement, analysis and evaluation
 - ▶ 9.2 Internal audit



Available in:

EN

FR



Redlines ▼

Bibliography

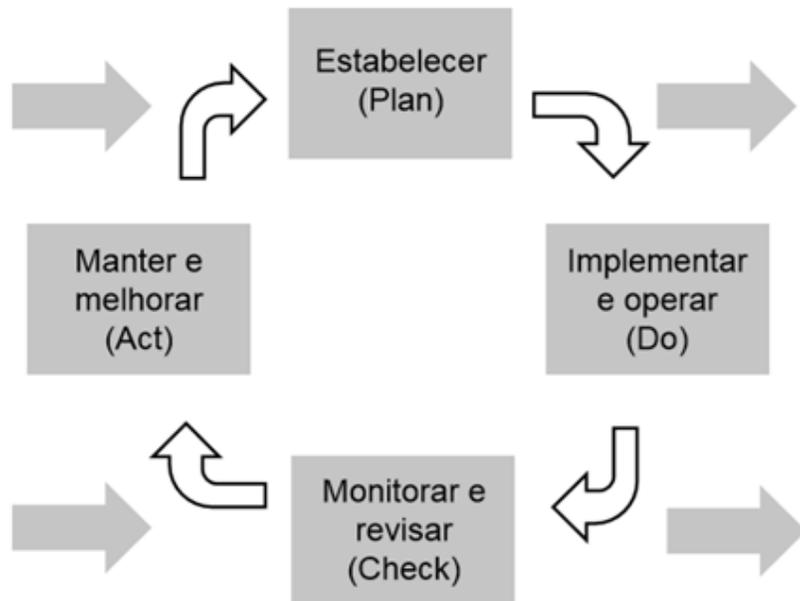
- [1] ISO 9001, *Quality management systems — Requirements*
- [2] ISO 14001, *Environmental management systems — Requirements with guidance for use*
- [3] ISO 19011, *Guidelines for auditing management systems*
- [4] ISO/IEC/TS 17021-6, *Conformity assessment — Requirements for bodies providing audit and certification of management systems — Part 6: Competence requirements for auditing and certification of business continuity management systems*
- [5] ISO/IEC 20000-1, *Information technology — Service management — Part 1: Service management system requirements*
- [6] ISO 22313, *Societal security — Business continuity management systems — Guidance*
- [7] ISO 22316, *Security and resilience — Organizational resilience — Principles and attributes*
- [8] ISO/TS 22317, *Societal security — Business continuity management systems — Guidelines for business impact analysis (BIA)*
- [9] ISO/TS 22318, *Societal security — Business continuity management systems — Guidelines for supply chain continuity*
- [10] ISO/TS 22330, *Security and resilience — Business continuity management systems — Guidelines for people aspects of business continuity*
- [11] ISO/TS 22331, *Security and resilience — Business continuity management systems — Guidelines for business continuity strategy*
- [12] ISO/IEC 27001, *Information technology — Security techniques — Information security management systems — Requirements*
- [13] ISO/IEC 27031, *Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity*
- [14] ISO 28000, *Specification for security management systems for the supply chain*
- [15] ISO 31000, *Risk management — Guidelines*
- [16] IEC 31010, *Risk management — Risk assessment techniques*
- [17] ISO Guide 73, *Risk management — Vocabulary*

O que é Continuidade de Negócios?

Continuidade de Negócios é a “capacidade de uma organização de entregar produtos e serviços em níveis aceitáveis após um incidente.”

A Gestão da Continuidade de Negócios (GCN) envolve utilizar recursos adequadamente a fim de aumentar a capacidade de uma organização de lidar com interrupções.

A GCN deve fazer parte do sistema geral de governança e gestão da organização, ou seja, o Sistema de Gestão de Continuidade de Negócios (SGCN) é parte da organização.



Ciclo PDCA e o SGCN

Plan (Estabelecer)

Uma política de continuidade, objetivos, metas, controles, processos e procedimentos pertinentes de forma a ter resultados alinhados à organização.

Do (Implementar e operar)

A política de continuidade de negócios, controles, processos e procedimentos.

Check (Monitorar e analisar criticamente)

O desempenho em relação aos objetivos e política de continuidade de negócios, reportar os resultados para a direção, definir e autorizar ações de melhorias e correções.

Act (Manter e melhorar)

Tomando ações corretivas e preventivas, baseadas nos resultados da análise crítica da direção e reavaliando o escopo do SGCN, as políticas e objetivos de continuidade.

Escopo e Referências da ISO 22313 e da ISO 22301

Escopo

São normas genéricas e aplicáveis a todos os tipos e tamanhos de organizações que:

- a) estabelecer, implementar, manter e melhorar um SGCN;
- b) assegurar conformidade com a política de continuidade de negócios;
- c) fazer uma autodeterminação e autodeclararão de conformidade.

Referências

A Norma para certificação é a ABNT NBR ISO 22301.

A Norma de orientações é a ABNT NBR ISO 22313.

Termos e Definições

Continuidade de Negócios (*business continuity*)

Capacidade de uma organização de planejar e responder a incidentes e interrupções de negócio a fim de continuar suas operações em um nível aceitável pré-definido.

Gerenciamento de Continuidade de Negócios (*business continuity management*)

Um processo holístico de gerenciamento que identifica ameaças a uma organização e os impactos caso as ameaças explorem vulnerabilidades e fornece um framework para promover resiliência a fim de resguardar os interesses das partes interessadas, a reputação da organização, o valor de marca, além das atividades críticas.

Termos e Definições

Sistemas de Gerenciamento de Continuidade de Negócios (*business continuity management system*)

É parte do sistema geral de gerenciamento e tem como objetivo estabelecer, implementar, operar, monitorar, analisar, manter e melhorar a continuidade de negócios.

Plano de Continuidade de Negócios (*business continuity plan*)

Procedimentos documentados para guiar a organização a fim de responder, recuperar, retomar e restaurar níveis de operação após uma interrupção.

Termos e Definições

Documento (*document*)

Informação e seu meio de armazenamento.

Procedimento (*procedure*)

Modo específico de executar uma atividade ou processo.

Política (*policy*)

Intenções e diretrizes de uma organização formalmente expressas pela alta gestão.

Termos e Definições

Evento (*event*)

Ocorrência de (ou mudança em) um conjunto particular de circunstâncias.

Obs. An event may consist of something not happening.

Incidente (*incident*)

Evento que pode ser, ou levar a, uma interrupção de negócio, perdas, emergências ou crises.

Termos e Definições

Parte Interessada (*interested party, stakeholder*)

Pessoa ou grupo de pessoas que podem afetar ou serem afetadas por uma organização.

Recursos (*resources*)

Todos os ativos, pessoas, habilidades, informações, tecnologias, fornecedores etc. que uma organização dispõe a fim de manter suas operações para atingir seus objetivos.

Competência (*competence*)

Capacidade de aplicar conhecimentos e habilidades a fim de atingir resultados.

Termos e Definições

Minimum Business Continuity Objective – MBCO

Mínimo nível de serviços ou produtos necessários para que a organização atinja seus objetivos de negócio durante uma interrupção.

Recovery Point Objective – RPO

Ponto no qual uma informação precisa ser restaurada a fim de possibilitar o restabelecimento de alguma atividade que dela dependa.

Obs. May also be referred to as 'maximum data loss'

Termos e Definições

Maximum Tolerable Period of Disruption – MTPD

Tempo máximo decorrido para que se torne inaceitável o impacto adverso resultante da interrupção de um serviço ou produto, ou da não realização de uma atividade.

Obs. May also be referred to as ‘maximum acceptable outage’

Recovery Time Objective – RTO

Período de tempo após um incidente no qual um produto ou serviço deve ser restabelecido, uma atividade retomada, ou recursos recuperados.

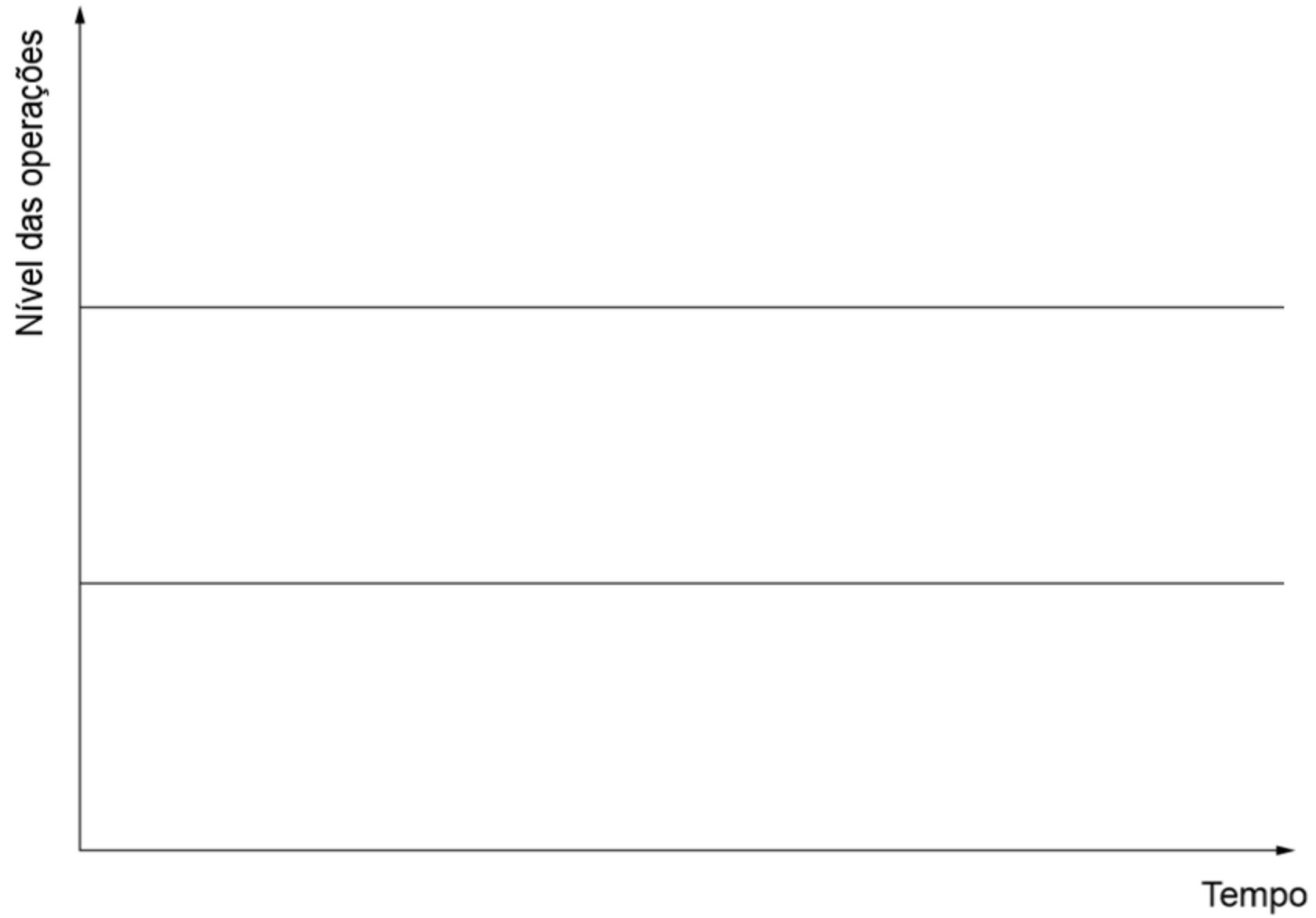
Obs. For products, services and activities, the recovery time objective must be less than the time it would take for the adverse impacts that would arise as a result of not providing a product/service or performing an activity to become unacceptable.

Termos e Definições

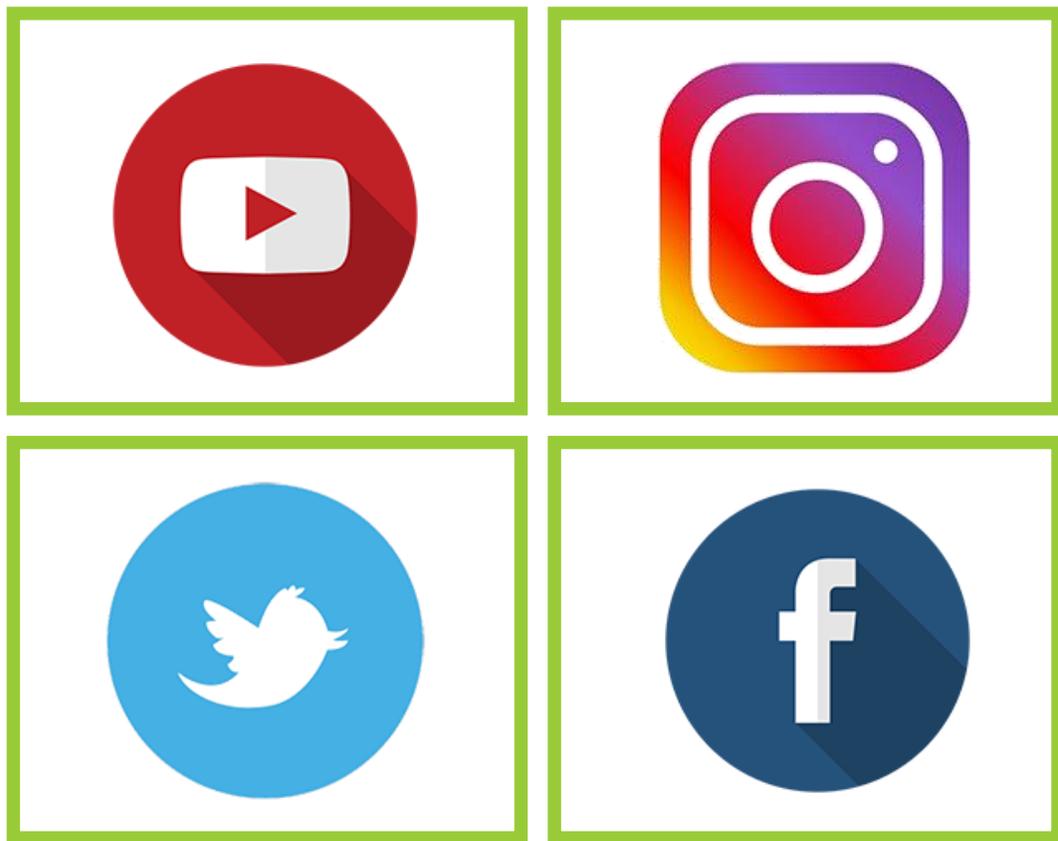
Business Impact Analysis – BIA

Processo de analisar funções operacionais e o efeito de interrupções sobre elas.

•



CanalGovTI.com.br



Nas redes sociais
@CanalGovTI

