Gestão de Continuidade de Negócios

Agosto de 2024 | Versão 2.0

Índice

Aviso geral

Este documento é de responsabilidade do Sistema de Gestão de Continuidade de Negócios (SGCN). Os seguintes princípios são válidos para este documento:

- Este documento é controlado como parte do controle de governança da Gestão do Sistema de Gestão de Continuidade de Negócios (SGCN).
- Nenhuma modificação deste documento é permitida sem a aprovação formal do titular do documento.
- Este documento é classificado, suas versões são controladas e é periodicamente revisto.
- Todas as dúvidas referentes a este documento devem ser apresentadas ao titular.
- A distribuição, as modificações e o acesso devem levar em conta a classificação de sigilo da informação da TMF Group.
- A versão deste documento está indicada na página de rosto.
- Os dados da revisão são apresentados abaixo.
- Este documento pode estar disponível em vários idiomas. Entretanto, a versão em inglês prevalecerá.

CLASSIFICAÇÃO
Interna

Partes Interessadas	
Titular	Diretor de Segurança e Resiliência
Aprovado por	Comitê de Risco do Grupo TMF
Patrocinador	**Diretor de Operações e Tecnologia**

RELEITURA	
Período	Anual
Última atualização	27 de maio de 2024
Status	Final
Data de aprovação	8 de agosto de 2024
Data de vigência	8 de agosto de 2024

PONTO DE CONTATO	
Contato	ISMS do Grupo TMF
Dados	**Entre em contato com a equipe através do endereço ISMS@tmf-group.com**

1. Introdução, objetivo e escopo

O objetivo da Política de Gestão de Continuidade de Negócios (BCM) (a "Política") é proteger os interesses da TMF Group e de seus intervenientes internos e externos, estabelecendo acordos de contingência para reagir, retomar e recuperar serviços críticos de negócios a um nível operacional pré-definido, na medida do que seja comercialmente razoável.

Esta Política apresenta as intenções e o rumo da TMF Group, formalmente expressos pelo nosso Conselho Administrativo. Como uma organização de serviços profissionais, a TMF Group entende a importância de seus serviços de negócios para as partes interessadas externas e internas e, portanto, a importância de ter um programa holístico de Gerenciamento de Continuidade de Negócios em vigor.

O objetivo desta Política é, portanto, proteger os interesses da TMF Group e de seus intervenientes internos e externos, estabelecendo providências de contingência para reagir, retomar e recuperar, na medida cabível e praticável, as funções essenciais identificadas a um nível operacional pré-estabelecido.

Esta política é aplicável à TMF Group e suas subsidiárias.

2. Declaração da Política

2.1 Primeiros princípios

> Gestão de Continuidade de Negócios (“BCM” sua sigla em inglês para *Business Continuity Management*) é parte integrante da gestão e dos processos essenciais de negócio da TMF Group;

> A segurança da vida é a prioridade da organização. A saúde e a segurança do nosso pessoal devem ser consideradas como parte de todos os processos e atividades de negócios. Durante um incidente, a organização deve priorizar a segurança e o bem-estar da equipe;

> A companhia irá garantir que os processos de continuidade de negócios (“BC” sigla em inglês para *business continuity*) sejam estabelecidos para garantir a continuidade dos principais serviços essenciais da TMF Group, nos casos de ruptura significativa;

> todos os processos essenciais de negócios e recursos, incluindo os de terceiros, quando necessários para a entrega de serviços devem ser identificados e hierarquizados em prioridade;

> O plano de recuperação de desastre para ativos e serviços de tecnologia que são necessários para apoiar processos de negócios críticos deve ser criado com base em avaliações de risco/identificação de falha apropriados, além de mantido e testado periodicamente;

> O Time de Gerenciamento de Crises (“CMT” em inglês) é o responsável pela declaração de crise/invocação do Plano de Continuidade e responsável global pela gestão de qualquer situação de crise;

> As áreas de suporte da TMF Group se esforçarão para prestar apoio à reação, recuperação e restauração a um nível predefinido de operação. Avaliações pós-crise serão conduzidas para verificar as lições aprendidas e para nos permitir melhorar nossos processos e nossas reações.

> A organização deve garantir que todas as comunicações relacionadas à Continuidade de Negócios para as partes interessadas internas e externas sejam coordenadas por meio do time de Comunicações da TMF Group, de maneira oportuna e apropriada

2.2 Requisitos gerais

> Cada escritório/país garantirá que os requisitos estatutários, regulamentares e contratuais relativos à Continuidade de Negócios sejam identificados e cumpridos;

> Cada escritório/país deve implementar e manter um processo formal de avaliação conhecido como Análise de Impacto no Negócio (ou em inglês, *Business Impact Analysis* “BIA”) para determinar as prioridades, objetivos e metas de continuidade e recuperação;

> Cada escritório/país e função global deve conduzir avaliações de risco formais e periódicas para identificar e tratar os riscos de interrupção;

> Cada escritório/país e função global deve manter um plano de tratamento de risco para reduzir a exposição ao nível de apetite de risco da Organização;

- Cada escritório/país deve determinar e selecionar estratégias para cumprir os prazos prioritários definidos para retomar os processos críticos de negócios e atividades prioritárias em um nível mínimo aceitável especificado, após um evento de continuidade de negócios;
- Cada escritório/país é responsável por criar, implementar, monitorar, revisar, manter e melhorar continuamente os planos de Continuidade de Negócios para garantir que os serviços críticos sejam entregues por níveis pré-identificados, no caso de uma interrupção;
- Todos os países, salvo aqueles explicitamente isentados pelo Líder Regional e do Mercado (*Market*), devem ter um Coordenador de Continuidade de Negócios ("BCC" sigla em inglês para *Business Continuity Coordinator*) atuando sob a direção de seu Diretor Local, MD ou cargo equivalente, que será responsável por criar, manter, testar e aplicar o plano de continuidade de negócios local;
- Cada escritório/país deve revisar e manter a documentação do BCM continuamente ou pelo menos uma vez por ano.
- Os recursos de backup devem ser identificados para funções/serviços críticos . Os Procedimentos Operacionais Padrão (SOPs)/manuais/guias para todos os processos críticos devem ser mantidos e disponibilizados para ajudar na transição para um novo recurso na ausência de recursos críticos identificados;
- Cada escritório/país é responsável por identificar ativos e serviços de tecnologia que são críticos para seus processos de negócios e acordar formalmente os objetivos de recuperação com a área de Operações e Tecnologia;
- Enquanto operando em modo de continuidade de negócios, o escritório da TMF Group afetado deve continuar atuando em cumprimento à todas as Políticas da TMF Group e exigências da legislação local de saúde e segurança
- As funções e responsabilidades da equipe designada com funções de continuidade de negócios devem ser claramente definidas no Plano de Continuidade de Negócios ("BCP" sigla em inglês para *Business Continuity Plan*) do escritório

2.3 Gestão e Compromisso

O Conselho Administrativo deverá demonstrar liderança e compromisso com relação ao BCMS, garantindo que a política de BCM seja estabelecida e comunicada dentro da organização.

A Gestão local garantirá:

- Que os deveres e responsabilidades de BCM sejam designados e comunicados dentro da organização;
- O desenvolvimento, a implementação e a manutenção dos planos e medidas efetivos de Continuidade de Negócios.
- A execução do programa de BCM, que seja consistente com a estratégia de negócio geral;
- A provisão de recursos apropriados necessários para a gestão de continuidade de negócios;
- A promoção da integração de BCMS aos processos de negócio;
- Que a organização tenha um programa de conscientização de Continuidade de Negócios;
- Que os riscos e problemas de BCM sejam relatados;
- Melhoria contínua para BCMS.

2.4 Responsabilidades e Atividades

As responsabilidades e atividades necessárias para executar os Planos de BC estão descritas abaixo.

O Coordenador de Continuidade de Negócios (BCC) atuará como ponto de contato principal para assuntos relacionados ao BCP no país. O BCC trabalhará com a administração e os intervenientes locais para estabelecer e manter um Plano de Continuidade de Negócios que tenha um custo-benefício e seja e relevante para as necessidades da unidade de negócios, de acordo com a política, especialmente:

- Ferramentas para registrar, interpretar e relatar à TMF Group:
  - riscos operacionais e estratégias de atenuação;
  - principais atividades de negócios; e
  - possíveis impactos de prejuízo financeiro.
- Requisitos de recuperação
- Assistência localizada
- Gestão de terceiros
- Treinamento e conscientização do pessoal, de acordo com suas responsabilidades de continuidade de negócio

Os membros delegados da administração fornecerão:

- Informações de apoio a:
  - Avaliação de risco;
  - Análise de Impacto sobre os Negócios; e
  - considerações locais específicas, jurídicas ou de outra natureza, sobre desenvolvimento, análises e ensaios do ERP e do BCP locais.
- Participação em reuniões de instrução locais para funcionários, treinamentos e conscientização

2.5 Teste, exercício, treinamento e conscientização

As medidas tomadas nas primeiras horas de uma ruptura significativa e/ou de um evento fisicamente prejudicial são fundamentais para determinar o resultado geral. O pessoal precisará reagir com flexibilidade a diversas situações. Portanto, será previsto o seguinte:

- Testes dirigidos para:
  - homologar os planos de continuidade; e
  - dados de contato com integrantes da equipe (por exemplo, providências em cascata, troca de mensagens de emergência, fornecedores essenciais etc.).
- Os principais integrantes identificados da equipe que façam parte essencial do BCP da TMF Group. Esse exercício permitirá à TMF Group:
  - conscientizar os funcionários sobre suas respectivas funções e responsabilidades;
  - melhorar a capacidade de reação, recuperação e restauração em caso de incidentes;
  - identificar lacunas e possíveis problemas no planejamento e avaliar alternativas; e
  - exercitar a equipe e conseguir a adesão dos funcionários em todos os níveis da organização.

> Identificar as pessoas que devam receber o treinamento pertinente para:
  - entender melhor suas funções e responsabilidades específicas; e
  - garantir a competência na área pela qual são responsáveis.
> Iniciativas de conscientização para obter melhor visibilidade da BCM e das lições aprendidas.

2.6 Documentação e manutenção

> Para garantir que a documentação pertinente seja disponibilizada aos intervenientes, o BCC deve:
> Garantir que cópias atualizadas do ERP e do BCP sejam prontamente acessíveis:
  - a todos os integrantes da Equipe de Administração
  - aos integrantes da equipe de apoio à Administração
  - Contatos Regionais ou de Grupo de apoio ao BCP
> Contatos Regionais ou de Grupo de apoio ao BCP Providenciar a análise e manutenção da documentação, da seguinte maneira:
  - revisão e atualização da Avaliação de Risco e Incidente (RIA) pelos proprietários do plano anualmente ou no evento de grandes mudanças internas ou externas que poderiam introduzir novos riscos ou alterar o nível dos riscos existentes;
  - revisão e atualização do Plano de Tratamento de Risco (ERPs) para riscos que não estão dentro do apetite de risco da organização. Rastreando e garantindo que as ações identificadas no Plano de Tratamento de Risco sejam concluídas pelos proprietários identificados de acordo com o plano;
  - revisão e atualização anual da Análise de Impacto nos Negócios (“BIA” sigla em inglês para Business Impact Analysis) pelos responsáveis pelo plano e TI;
  - análise e atualização dos Planos de Reação a Emergências (ERPs) pelos responsáveis pelo plano pelo menos anualmente, ou quando houver uma mudança significativa;
  - análise e atualização dos BCPs pelos responsáveis pelo plano pelo menos anualmente, ou quando houver uma mudança significativa;
  - teste periódico do sistema/processo de Chamadas em Cascata/Mensagens de Emergência;
  - teste e exercício dos ERPs do escritório (sem prejuízo da legislação local);
  - teste e exercício dos BCPs do escritório pelo menos uma vez ao ano;
  - treinamento e conscientização a nível de escritório local, país, região e Grupo, pelo menos uma vez ao ano; e
  - reuniões departamentais/de equipe/de escritório sobre as providências de continuidade de negócio, de forma contínua.

- Auditoria
  - Os documentos devem estar sujeitos à auditoria por auditores qualificados que avaliarão a efetividade e adequação do programa de BCMS, pelo menos, uma vez a cada três anos. Os resultados da auditoria serão documentados, acompanhados e encaminhados por meio de um plano de ação corretiva.
- Melhoria contínua

- A organização determinará se há necessidades ou oportunidades de negócio ou relacionadas a BCMS que devam ser abordadas como parte da melhoria contínua, considerando os resultados da análise e avaliação, as não conformidades, bem como os resultados da revisão da gestão.

2.7 Segurança e proteção dos funcionários

> No caso de um evento de emergência e/ou no exterior que possa exigir a evacuação de o tratamento médico ou outra forma de assistência aos funcionários, a TMF nomeou Indivíduos Autorizados que estão autorizados a aprovar auxílio financeiro e atuar como primeiro ponto de contato da SOS Internacional caso seja necessário tomar decisões críticas.

> Para mais informações, consulte o Portal de Wellbeing da TMF Group e a Política de Viagens e Despesas.

Definições e Abreviações

TERMO E DEFINIÇÃO
Conselho administrativo: Gestão do grupo
Gestão local: Líderes do país
Auditoria: processo sistemático, independente e documentado para obtenção de evidência de auditoria e avaliação desta objetivamente a fim de determinar a extensão em que os critérios de auditoria foram cumpridos. *(Fonte: ISO 22301:2019; Segurança e Resiliência, Sistema de Gestão de Continuidade de Negócios)*
Continuidade de Negócios (BC): A capacidade da organização de continuar fornecendo produtos ou prestando serviços em níveis predefinidos aceitáveis após incidentes perturbadores. *(Fonte: ISO 22301: 2019; Segurança e Resiliência, Sistema de Gestão de Continuidade de Negócios)*
Coordenador de Continuidade de Negócios (BCC): coordena o planejamento e a implementação de recuperação geral de uma organização ou unidade(s). *(Fonte: Disaster Recovery Journal (DRJ) / Business Continuity Incident (BCI))*
Análise de Impacto no Negócio (BIA): Processo de analisar o impacto no decorrer do tempo de um evento adverso sobre a organização. *(Fonte: ISO 22301:2019; Segurança e Resiliência, Sistema de Gestão de Continuidade de Negócios)*
Competência: Capacidade de aplicar o conhecimento e habilidades para alcançar os resultados pretendidos. *(Fonte: ISO 22301:2019; Segurança e Resiliência, Sistema de Gestão de Continuidade de Negócios)*
Melhoria contínua: Atividade recorrente para melhoria de performance *(Fonte: ISO 22301:2019; Segurança e Resiliência, Sistema de Gestão de Continuidade de Negócios)*
Conformidade: Cumprimento de um requisito *(Fonte: ISO 22301:2019; Segurança e Resiliência, Sistema de Gestão de Continuidade de Negócios)*
Ação corretiva: ação para eliminar a(s) causa(s) de uma não conformidade para prevenir a reincidência *(Fonte: ISO 22301:2019; Segurança e Resiliência, Sistema de Gestão de Continuidade de Negócios)*
Evento adverso: incidente, seja previsto ou não, que cause um desvio não planejado e negativo da entrega esperada de produtos e serviços de acordo com os objetivos de uma organização *(Fonte: ISO 22301:2019; Segurança e Resiliência, Sistema de Gestão de Continuidade de Negócios)*
Efetividade: extensão em que as atividades planejadas são realizadas e os resultados planejados são alcançados *(Fonte: ISO 22301:2019; Segurança e Resiliência, Sistema de Gestão de Continuidade de Negócios)*
Saúde e Segurança (HandS): O processo pelo qual o bem-estar de todos os funcionários, contratados, visitantes e do público está salvaguardado. *(Fonte: Disaster Recovery Journal (DRJ))*
Impacto: resultado de um evento adverso que afete os objetivos *(Fonte: ISO 22301:2019; Segurança e Resiliência, Sistema de Gestão de Continuidade de Negócios)*

TERMO E DEFINIÇÃO
Incidente: evento que possa ser, ou que possa levar a um evento adverso, perda, emergência ou crise *(Fonte: ISO 22301:2019; Segurança e Resiliência, Sistema de Gestão de Continuidade de Negócios)*
Plano de Reação a Emergências (ERP): A reação e resposta imediatas a uma situação de emergência, geralmente concentrada em garantir a proteção da vida e diminuir a gravidade do incidente. *(Fonte: Guia de Práticas Profissionais do Instituto Internacional de Recuperação de Desastres (DRII))*
Plano de Continuidade de Negócios (BCP): Informações documentadas que orientam as organizações a reagir a um evento adverso e recuperar-se, retomar e restaurar a entrega de produtos e serviços consistente com os objetivos da continuidade de negócios. *(Fonte: ISO 22301: 2019; Segurança e Resiliência, Sistema de Gestão de Continuidade de Negócios)*
Plano de Gestão de Incidentes (IMP): Plano de ação claramente definido e documentado para ser usado no momento de um incidente, em geral contemplando o pessoal essencial, os serviços e as ações necessárias para implementar o processo de gestão de incidentes. *(Fonte: Disaster Recovery Journal (DRJ) / Business Continuity Incident (BCI))*
Plano de Recuperação de Desastres de Tecnologia da Informação (ITDRP): O documento aprovado pela Administração que define os recursos, as ações, as tarefas e os dados necessários para gerenciar o esforço de recuperação da tecnologia. *(Fonte: Disaster Recovery Journal (DRJ))*
Crise: Evento ou situação anormal ou extraordinário que ameace uma organização ou comunidade e requeira uma resposta estratégica, adaptativa e pontual a fim de preservar sua viabilidade e integridade *(Fonte: ISO 22361:2022 Segurança e Resiliência – Gestão de crise – Diretrizes)*
Gestão de Crises (CM): Atividades coordenadas para liderar, direcionar e controlar uma organização com relação à crise. *(Fonte: ISO 22361:2022 Segurança e resiliência – Gestão de crise – Diretrizes)*
Plano de Gestão de Crises (CMP): Documento que descreve quais processos e recursos associados serão aplicados por quem e onde em uma crise. *(Fonte: ISO 22361:2022 Segurança e resiliência – Gestão de crise – Diretrizes)*
Equipe de Gestão de Crises (CMT): Grupo de indivíduos funcionalmente responsáveis por liderar a resposta de gestão de crise da organização. *(Fonte: ISO 22361:2022 Segurança e resiliência – Gestão de crise – Diretrizes)*
Alta Administração: Pessoa ou grupo de pessoas que dirige e controla uma organização no nível mais elevado. *(Fonte: ISO 22301: 2019; Segurança e Resiliência, Sistema de Gestão de Continuidade de Negócios)*
Interveniente/ Parte Interessada: Pessoa ou organização que possa afetar, ser afetada por, ou perceber-se afetada por uma decisão ou atividade. *(Fonte: ISO 22301: 2019; Segurança e Resiliência, Sistema de Gestão de Continuidade de Negócios)*
Monitoramento: determinar o status de um sistema, processo ou de uma atividade *(Fonte: ISO 22301: 2019; Segurança e Resiliência, Sistema de Gestão de Continuidade de Negócios)*
Não conformidade: não cumprimento de um requisito *(Fonte: ISO 22301: 2019; Segurança e Resiliência, Sistema de Gestão de Continuidade de Negócios)*
Objetivo: resultado a ser alcançado

TERMO E DEFINIÇÃO
(Fonte: ISO 22301: 2019; Segurança e Resiliência, Sistema de Gestão de Continuidade de Negócios)
Organização: Pessoa ou um grupo de pessoas que tenha(m) sua(s) própria(s) função(ões) com responsabilidades, autoridades e relações com alcançar os objetivos *(Fonte: ISO 22301: 2019; Segurança e Resiliência, Sistema de Gestão de Continuidade de Negócios)*
Política: intenções e direção de uma organização, como formalmente expressadas pela alta administração *(Fonte: ISO 22301: 2019; Segurança e Resiliência, Sistema de Gestão de Continuidade de Negócios)*
Processo: conjunto de atividades interrelacionadas ou que interajam entre si para transformar entradas em saídas *(Fonte: ISO 22301: 2019; Segurança e Resiliência, Sistema de Gestão de Continuidade de Negócios)*
Requisito: necessidade ou expectativa que seja declarada, geralmente por implicação ou obrigatoriedade *(Fonte: ISO 22301: 2019; Segurança e Resiliência, Sistema de Gestão de Continuidade de Negócios)*
Recurso: Todos os ativos (incluindo a fábrica ou o equipamento), pessoas, habilidades, tecnologia, instalações e suprimentos e informações (sejam eletrônicas ou não) que uma organização tenha disponibilizado para uso, quando necessário, a fim de operar e cumprir com os seus objetivos *(Fonte: ISO 22301: 2019; Segurança e Resiliência, Sistema de Gestão de Continuidade de Negócios)*
Risco: efeito de incerteza quanto aos objetivos *(Fonte: ISO 22301: 2019; Segurança e Resiliência, Sistema de Gestão de Continuidade de Negócios)*

Referência a documentos associados

Guia de Despesas e Viagens do Grupo TMF
Biblioteca de políticas da TMF Group
Política de Segurança da Informação
Documentação de ISMS
Diretrizes de Viagem e Despesas da TMF Group

Histórico e registros de revisões

VERSÃO	DATA	AUTOR	DADOS
1.0	09/03/2017	Deepak Iyer	> Primeira versão Alterações feitas após releitura e em conformidade com os comentários recebidos do BCSC
1.1	17/01/2019	Deepak Iyer	Analisado. Nenhuma alteração efetuada. Adequado ao propósito.
1.2	10/03/2020	Devender Kumar	Releitura anual; atualização de seções sobre funções e responsabilidades; alteração do Aprovador para o Comitê de Risco e Conformidade; atualizações para refletir mudanças estruturais; alteração do responsável pela política
1.3	22/03/2021	Anuj Tewari	Revisão anual; Cláusulas específicas sobre os requisitos de BIA, RA, Estratégia e BCP incluídos na Seção 1 (Primeiros Princípios). Seção 2.2 da versão anterior removida e alinhada aos parágrafos 1.2-1.4.
1.4	17/06/2021	A. Tewari	Revisão anual; pequenas alterações nos Primeiros Princípios e Documentação e Manutenção
1.5	19/07/2023	Anuj Tewari, Ze Mei Chiang, Rohit Rajput	Revisão anual; atualizações menores e reformulações
2.0	**27/05/2024**	**Subhodh Subramanian, Darshilla Rive, Alvaro Guerrero, Rohit Rajput**	**Revisão anual; inclusão de uma seção "Gestão e Compromisso", alterações menores na seção "Documentação e manutenção", atualização da seção "Definições e abreviações"**