coopera+ Fórum Tecnologia da Informação

XXIX SUERJ

CUIDAR DE VOCÊ. ESSE É O PLANO. Unimed somos coop

Desenvolvendo uma Política de Continuidade de Tecnologia da Informação

Sergio Manoel

Sócio-Diretor da Trinity Cyber Security

AGENDA

1. Gestão de Continuidade de Negócios como diferencial competitivo
2. Sistema de Gestão de Continuidade de Negócios
3. Política de Continuidade de Tecnologia da Informação

[Certificação Internacional EXIN - Business Continuity Management Foundation]

sorteio

Sorteio do livro com dedicatória

AGENDA

1. GCN como diferencial competitivo

2018 - ANO DA GCN

Apagão em 13 estados deixa 70 milhões de pessoas sem luz

Distribuidoras de estados do Sudeste e Centro-Oeste receberam a determinação de cortar parte de seus clientes para proteger o resto do país do apagão

Apagão que deixou Norte e Nordeste sem luz foi causado por falha humana, diz ONS

21/03/2018

Disjuntor de subestação de Belo Monte foi programado erroneamente

https://www1.folha.uol.com.br/mercado/2018/04/apagao-que-deixou-norte-e-nordeste-sem-luz-foi-causado-por-falha-humana-diz-ons.shtml

2018 - ANO DA GCN

- A BRDigital teve um dos seus data centers atingido por um incêndio nesta terça-feira, 06/03/18, em Porto Alegre.

2018 - ANO DA GCN

Ministério Público pede para que todos brasileiros reiniciem os roteadores

07/06/2018 às 16:13 • 2 min de leitura

- O vírus infecta roteadores domésticos e altera o Domain Name System (DNS) para redirecionar os usuários para páginas falsas de instituições bancárias e lojas on-line e assim obter os dados pessoais dos correntistas e senhas, além de roubar informações pessoais e bloquear a internet com o objetivo de cometer fraudes.

- Os modelos de roteadores mais utilizados no Brasil que estão vulneráveis e podem ser infectados pelo vírus são: **ASUS, D-LINK, HUAWEI, MIKROTIK, NETGEAR, UBIQUITI, TP-LINK e ZTE**.

2018 - ANO DA GCN

- Novas leis e regulamentações exigindo requisitos de Continuidade de Negócios
  - GDPR – General Data Protection Regulation
  - LGPD – Lei Geral de Proteção de Dados
  - Resolução nº 4.658 – Política de segurança cibernética (Banco Central do Brasil) e Resolução Nº 4.557 – Gerenciamento de riscos

Pesquisa

- **Fonte:** Allianz Global Corporate, entrevistou em 2017/2018, 1.911 empresários em 80 países sobre as principais ameaças de negócios.

AGENDA

2. Sistema de Gestão de Continuidade de Negócios

Sistema de Gestão de Continuidade de Negócios

- **Continuidade de Negócios** - Capacidade da organização de continuar a entrega de produtos ou serviços em um nível aceitável previamente definido após incidentes de interrupção.

- **GCN** - Processo que identifica ameaças potenciais para uma organização e os possíveis impactos nas operações de negócio caso estas ameaças se concretizem.

- Este processo fornece uma estrutura para que se desenvolva uma resiliência organizacional que seja capaz de responder eficazmente e salvaguardar os interesses das partes interessadas, a reputação e a marca da organização e suas atividades de valor agregado.

Sistema de Gestão de Continuidade de Negócios

- **Incidente de Segurança da Informação**

  ✓ É indicado por um simples ou por uma série de eventos de segurança da informação indesejados ou inesperados, que tenham uma grande probabilidade de **comprometer as operações do negócio** e ameaçar a **quebra** da **confidencialidade, disponibilidade** e **integridade das informações.**

- **Incidente de Continuidade de Negócios**

  ✓ Situação que deve representar ou levar a uma **interrupção de negócios**, **perdas, emergências ou crises.**

  ✓ O Incidente é a concretização de uma ameaça que ocasione **perda** ou **dano** ao ativo, causando a **indisponibilidade**, **interrupção** ou **comprometimento** do processo.

- **Ameaça + Incidente + Dano + Recuperação**

Principais Padrões, Frameworks e Regulamentações de GCN

- **ABNT NBR ISO 22301:2013 -** Segurança da sociedade — Sistema de gestão de continuidade de negócios — Requisitos

- **ABNT NBR ISO 22313:2015** - Segurança da sociedade — Sistemas de gestão de continuidade de negócios — Orientações

- **ABNT NBR ISO/IEC 27031:2015 -** Tecnologia da informação - Técnicas de segurança - Diretrizes para a prontidão para a continuidade dos negócios da tecnologia da informação e comunicação

Principais Padrões, Frameworks e Regulamentações de GCN

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS

NORMA BRASILEIRA

ABNT NBR ISO 22301

Primeira edição
06.06.2013

Válida a partir de
06.07.2013

Segurança da sociedade — Sistema de gestão de continuidade de negócios — Requisitos

Societal security — Business continuity management systems — Requirements

ICS 03.100.01

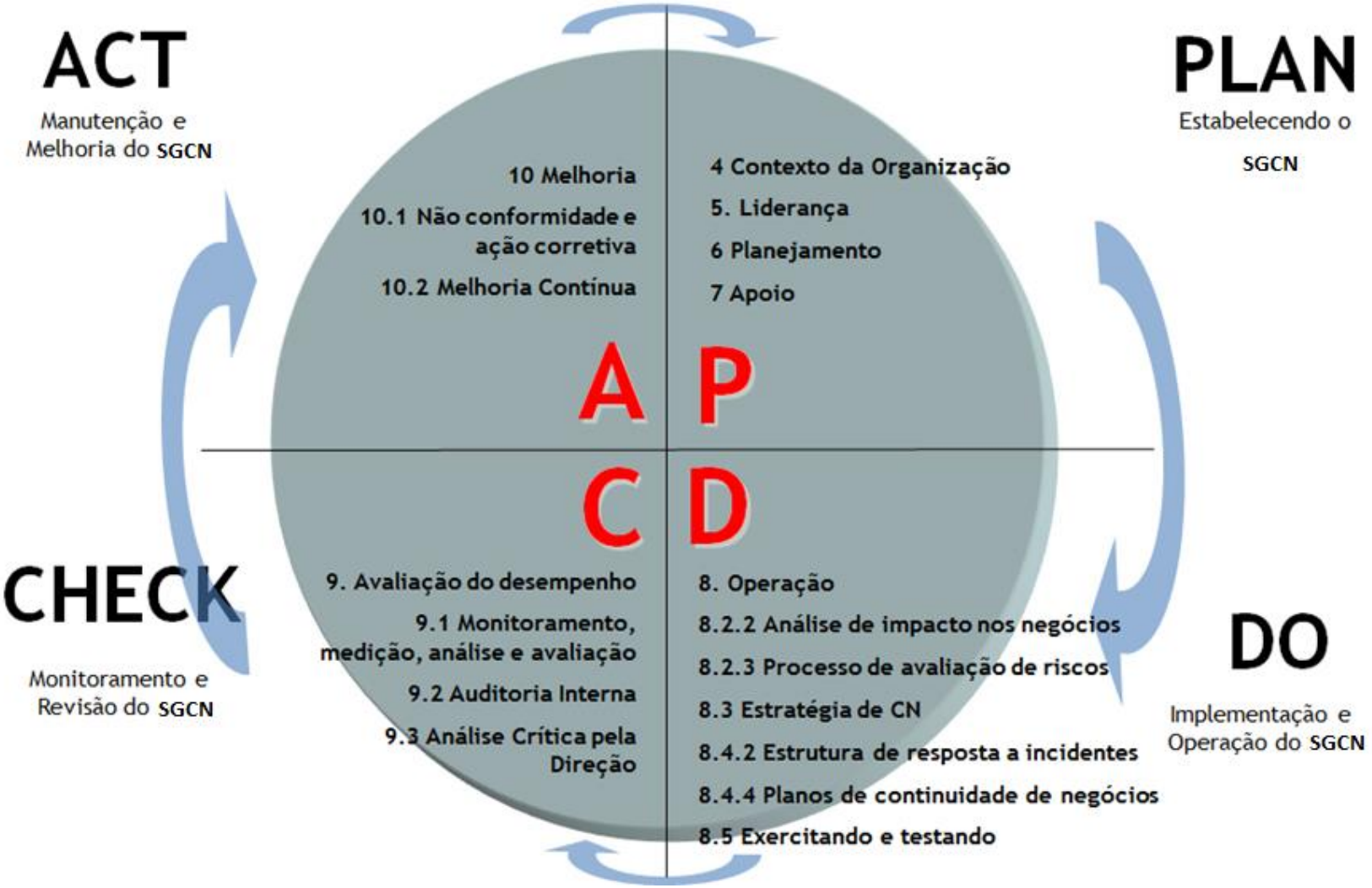
ISBN 978-85-07-04271-6

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS

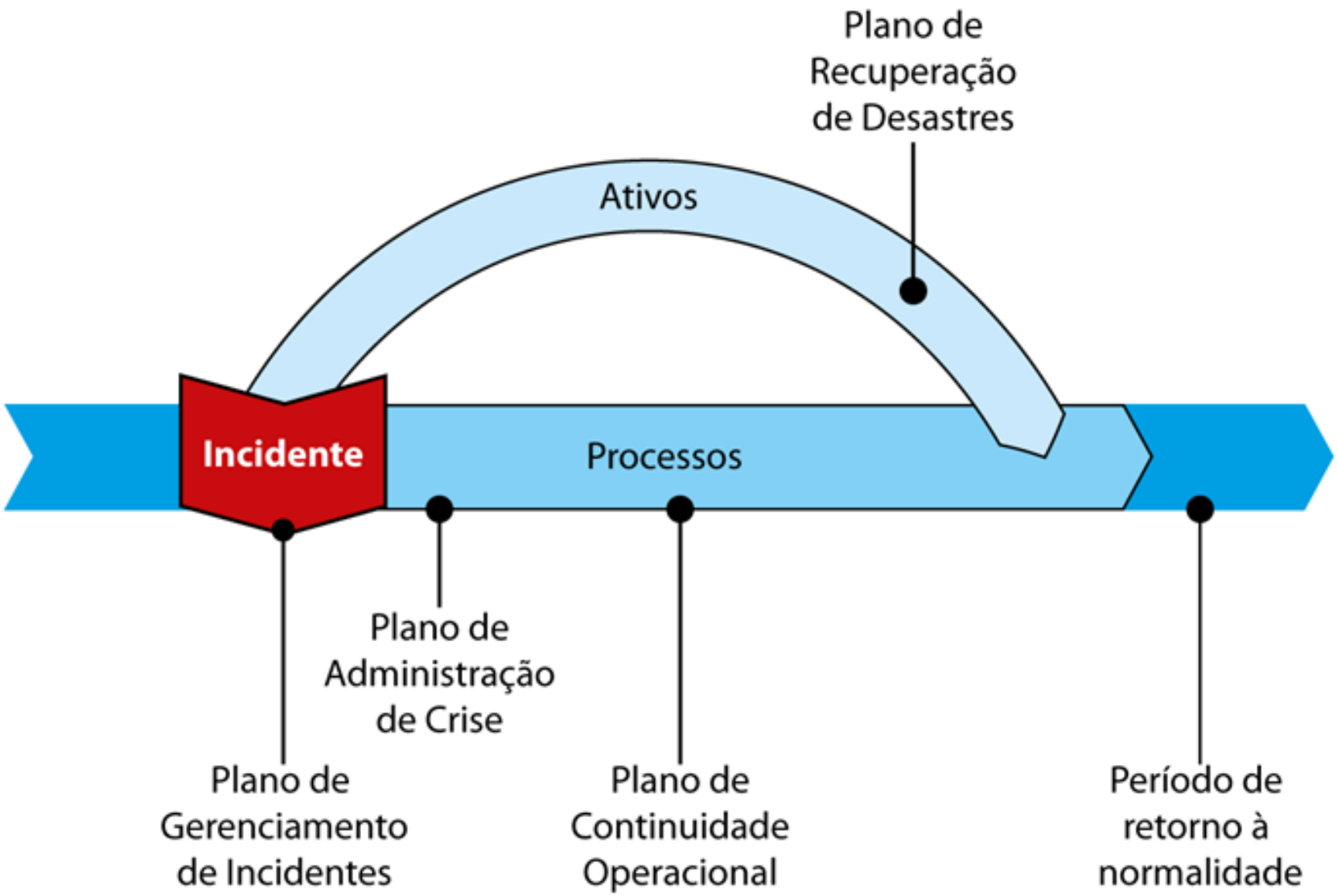
Número de referência
ABNT NBR ISO 22301:2013
28 páginas

Principais Motivações para ter um SGCN

Sistema de Gestão de Continuidade de Negócios



Planos de Continuidade de Negócios



AGENDA

3. Política de Continuidade de TI

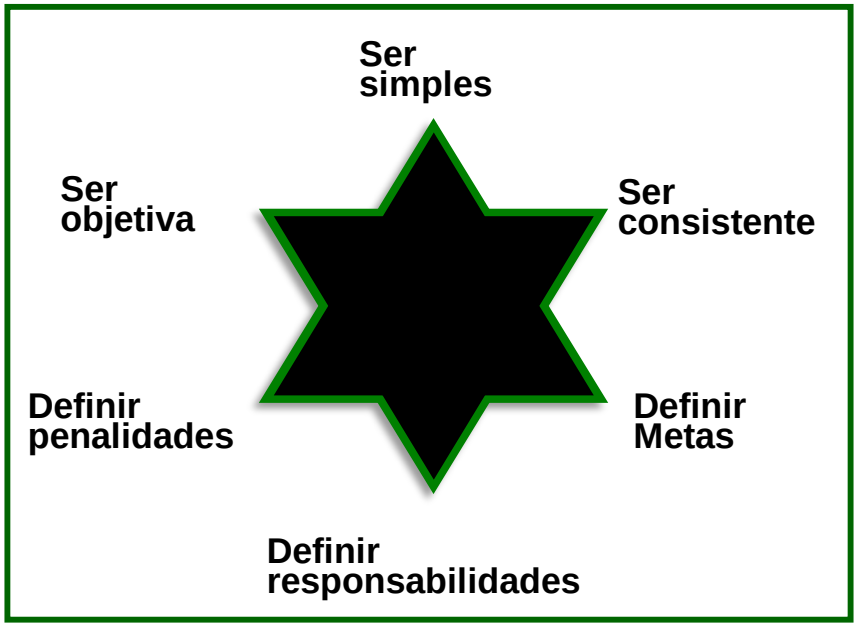
O que a Política precisa ser

- A Alta Direção deve definir uma Política de Continuidade de TI que deve:
  - a) estar alinhada com o propósito da organização;
  - b) estabelecer ou fornecer uma estrutura para estabelecer os Objetivos de Continuidade de Negócios;
  - c) incluir o compromisso de atender aos requisitos aplicáveis;
  - d) incluir o compromisso da melhoria contínua do SGCN.

É uma boa prática que a Política seja comunicada a toda a organização e suas partes interessadas, se apropriado. Uma boa iniciativa é deixar esse documento disponível no site institucional da organização.

Características da Política

FATORES INTERNOS



FATORES EXTERNOS

- ACESSÍVEL
- CONHECIDA
- APROVADA
- DINÂMICA
- EXEQUÍVEL

Como elaborar uma Política

- **Primeira fase:** levantamento de informações de legislação e documentos internos.

- **Segunda fase:** desenvolvimento do conteúdo da Política e elaboração de todos os itens do documento.
  - Grupo de trabalho formado por pessoas de diferentes áreas de atuação, não podendo faltar profissionais de Recursos Humanos, Jurídico, Tecnologia da Informação, Administração e Segurança da Informação.
  - Assim, todos podem contribuir com as experiências da sua área, e o documento final fica de acordo com a cultura da organização. Também é mais fácil posteriormente implementar uma regra que todos conheçam por terem participado da sua elaboração.

Como elaborar uma Política

- **Terceira fase:** revisão e aprovação pelo Diretor de TI ou por alguém da Alta Direção.

- **Quarta fase:** divulgação e implantação da Política.
  - A sua divulgação pode ser realizada por intermédio de palestras, treinamentos, envio de e-mail marketing etc.
  - É recomendado que as partes interessadas deixem claro que leram o documento e que passarão a cumprir as suas responsabilidades indicadas no documento normativo.

Itens da Política

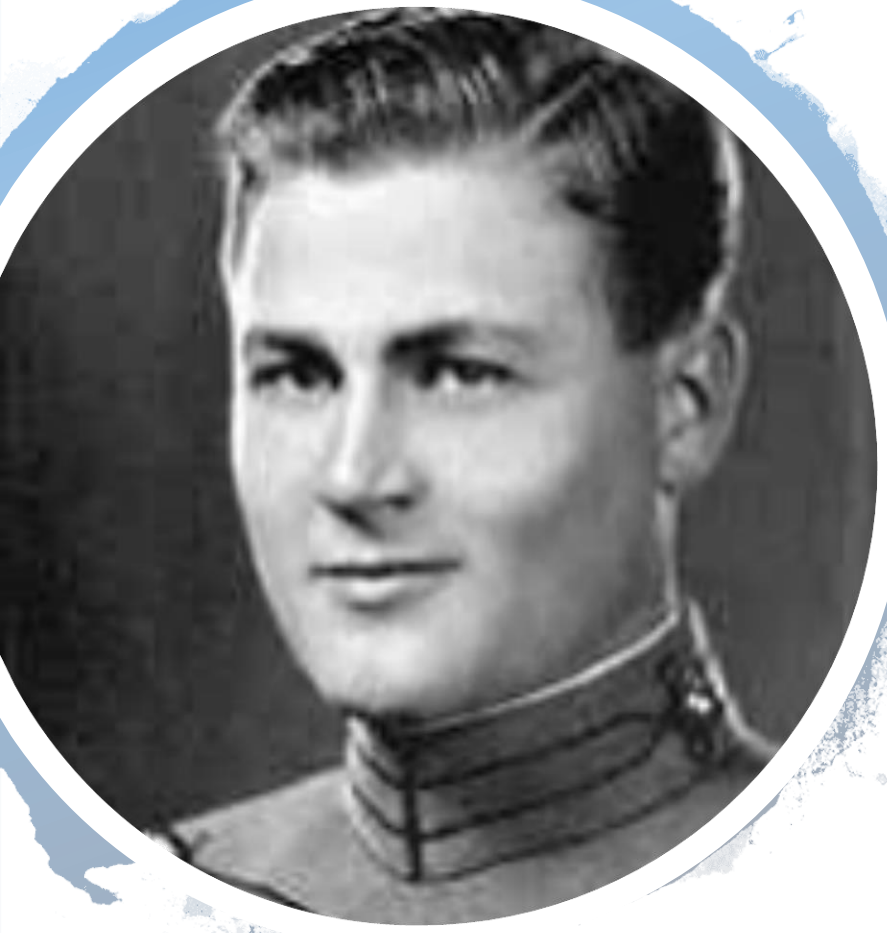
- **Finalidade do documento:** qual a finalidade da Política? Por que ela está sendo publicada na organização?
- **Escopo:** qual é o escopo da Política? Toda a área de TI?
- **Responsabilidades:** quais são as funções e responsabilidades das pessoas?
- **Condições de desastres:** O que é desastre para a área de TI? Falha na internet, falha de algum fornecedor, rompimento do banco de dados etc.
- **Objetivos de Continuidade de Negócios:** conforme explicado no item 6.2 da ISO 22301, é obrigatório definir quais são os objetivos e como eles são aprovados e revisados, bem como quem medirá se os Objetivos de Continuidade do Negócio foram alcançados, a quem os resultados precisam ser relatados, qual a frequência etc.

Itens da Política

- **Prazo de revisão:** deve ser estipulado um prazo de revisão do documento com o tempo de uso de 18 meses, 24 meses ou 36 meses.

- **Penalidades:** caso a Política não seja cumprida pelos funcionários e pelas partes interessadas, o que acontece? Nada?

➢ Fique à vontade caso deseje inserir outros itens, mas lembre-se, não é necessário. Um item opcional que também é muito utilizado é um Glossário com os termos e definições chaves da Política, neste item faz-se a conceituação dos principais termos.



Edward A. Murphy Jr.
Capitão da FAA

Lei de Murphy.

"...se existem duas ou mais formas de fazer uma tarefa, e uma delas puder provocar um desastre, alguém irá adotá-la...”

Agradecimento

Sergio Manoel

(21) 99173-0335

https://www.trinitycs.com.br/