Curso Preparatório para Certificação EXIN BCM Foundation

Área de Aprendizagem

www.pmgacademy.com

Official Course

Módulo 1

Nível
Advanced

www.pmgacademy.com

Design: By Freepik

Prof. Adriano Martins Antonio

Módulo 1

Introdução

Maior Aproveitamento

Assista no mínimo 2x

Contate o instrutor

Realize os exercícios

Leia o glossário

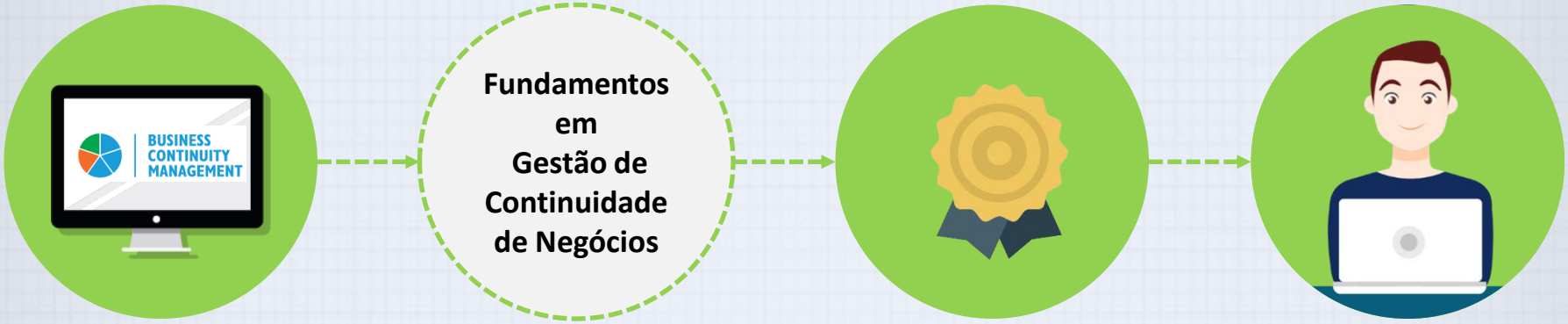
Execute os simulados

Sobre o Autor

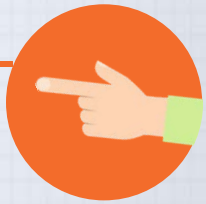
Adriano Martins Antonio

- Instrutor oficial credenciado aos institutos EXIN, People CERT e APMG.
- Consultor de Gestão de Projetos de TI, Governança de TI, Escritório de Projetos....
- Mais de 20 anos de experiência.
- MBA em Gestão Empresarial pela FGV – SP.
- Possui diversas certificações.

Sobre Este Curso



- O conteúdo da norma ISO/IEC 22301:2012...
- As fases da implementação da ISO 22301;
- Os elementos da implementação da ISO 22301;
- Implementação do Sistema de Gestão;
- O ciclo PDCA (Planejar-Desenvolver-Verificar-Agir) dentro deste framework;
- Envolvimento da Direção;
- Análise de Impacto nos Negócios;
- Análise de Riscos;
- Plano de comunicação.



O Que é Continuidade de Negócios?

"processo de negócio responsável pelo gerenciamento de risco que podem impactar seriamente o negócio. O gerenciamento de continuidade de negócio protege as conveniências das principais partes interessadas, reputação, marca e atividades de criação de valor. O processo envolve a redução de riscos a um nível aceitável e planejamento para a recuperação de processos de negócio caso surja alguma interrupção. O gerenciamento de continuidade de negócio define objetivos, escopo e requisitos para o gerenciamento de continuidade de serviço de TI.".

O Que é Continuidade de Negócios?

CONTINUIDADE DO NEGÓCIO

1. Construir e melhorar a resiliência do seu negócio;
2. Identificar os seus principais produtos e serviços e as atividades mais urgentes que os sustentam;
3. Elaborar planos e estratégias que o permitam continuar suas operações de negócios;
4. E permita recuperar-se de forma rápida e efetivamente de qualquer tipo de ruptura, seja qual for o seu tamanho ou causa.

O Que é Continuidade de Negócios?

Fonte: ISO 22301:2012

CONTINUIDADE DE NEGÓCIO OU *BUSINESS CONTINUITY* (BC)

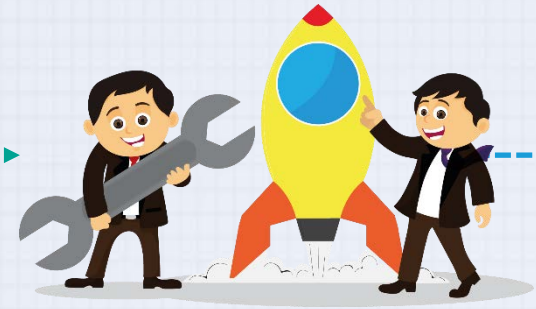
"Capacidade da organização em continuar a entrega de produtos ou serviços em níveis predefinidos aceitáveis após um incidente perturbador".

GERENCIAMENTO DE CONTINUIDADE DE NEGÓCIOS – GCN (*BUSINESS CONTINUITY MANAGEMENT - BCM*)

"Um processo de gestão holística, que identifica potenciais ameaças a uma Organização e os impactos às operações de Negócios que tais ameaças, se ocorrerem, podem causar. Tal gestão fornece um framework para o desenvolvimento da resiliência organizacional, com a capacidade de proporcionar uma resposta eficaz, que protege os interesses das suas principais Partes Interessadas, reputação, marca e atividades de geração de valor.".

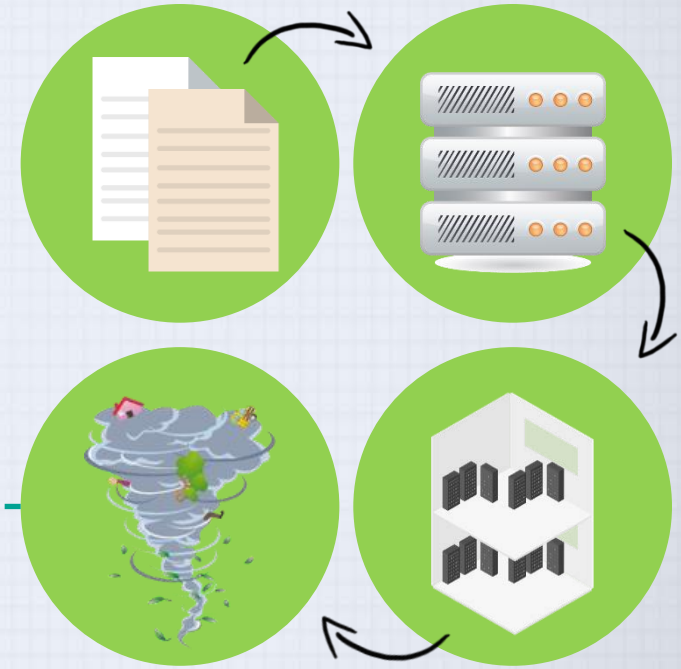
O Que a Continuidade de Negócio Não é

EQUÍVOCO 01



Continuidade do negócio é um trabalho que deve ser realizado apenas por pessoas da TI.

Tudo isso é necessário e deve ser parte de gerenciamento de continuidade de negócio, mas infelizmente não é o suficiente.



O Que a Continuidade de Negócio Não é

Planos de Continuidade do Negócio

=

Continuidade de Negócio

EQUÍVOCO 02

Acreditar que a continuidade de negócio é igual aos planos de continuidade do negócio.

EQUÍVOCO 03

A continuidade de negócio é um trabalho único.

Vamos implementar a ISO 22301, que todos nós estaremos bem.

- Um plano desatualizado é inútil.
- Testar a forma como os planos funcionariam em situações realistas.
- O cuidado e a manutenção da continuidade do negócio devem se tornar parte das operações diárias.

Por que Continuidade de Negócios?

Não há a menor chance de se prosperar como **EMPREENDEDOR OU FUNCIONÁRIO**, sem um **SISTEMA DE CONTINUIDADE DOS NEGÓCIOS**.

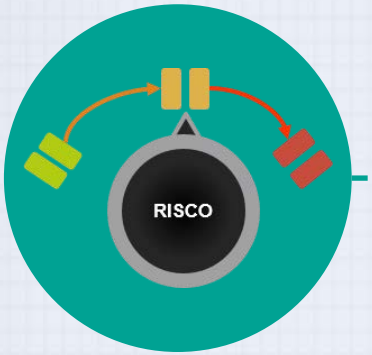
Grande guia

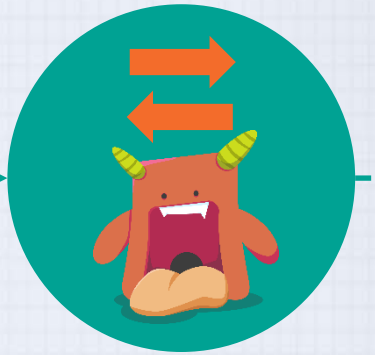
Enxergue não apenas as suas necessidades mais instantâneas...

Mas também todas as variáveis e situações a serem consideradas para que seu objetivo realmente seja alcançado.

- **Recuperação de desastres;**
- **Recuperação dos negócios;**
- **Crises;**
- **Incidentes;**
- **Emergências;**
- **Planejamento da contingência.**

Sistema de Gerenciamento de Continuidade de Negócios





Ameaças internas e externas

British Standards Institution - BSI

Padrão Internacional de Normalização 22301

ISO 22301 de 2012.

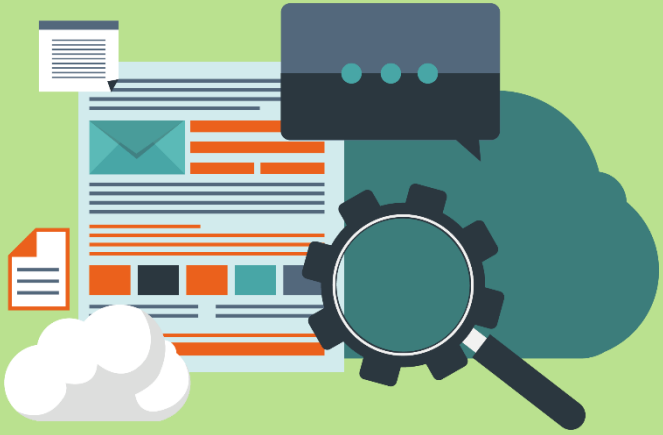
British Standard 25999-2, publicado em 2007.

Proporcionar à empresa a capacidade de responder efetivamente às ameaças como desastres naturais ou violações de dados e proteger os seus interesses comerciais.

Pilares de um Sistema de Continuidade dos Negócios

REGULARIDADE	INTEGRAÇÃO	DETALHAMENTO
Essa qualidade não se refere apenas em dar continuidade aos negócios em si, mas sim para perceber que esse tipo de estratégia não aponta unicamente para um planejamento como algo definitivo, sem nenhuma necessidade de revisão ou atualização.	Quando o assunto é a implementação do SGCN, quanto maior a quantidade de pessoas que saibam administrar os meios de segurança, maior será a possibilidade de elas estarem envolvidas na implementação de medidas em situações de urgência.	Independente das dimensões que possa ter o sua organização, o nível de detalhamento necessário para um bom SGCN deve ser mantido no mais próximo de englobar todas as possibilidades e necessidades de recuperação e manutenção dos negócios.

Pilares de um Sistema de Continuidade dos Negócios

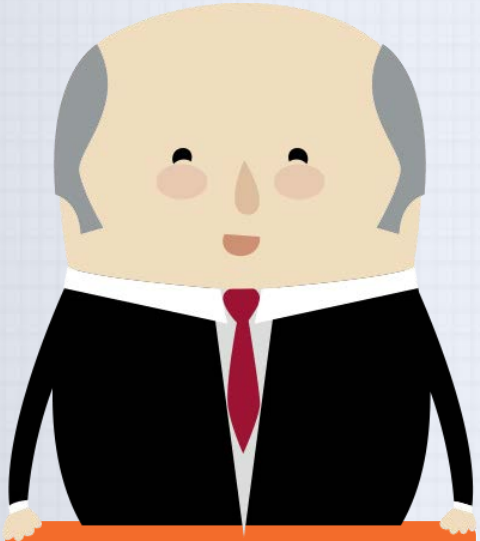


Como eles estarão dispostos:	Como eles serão armazenados:	Quem será responsável por manter esses dados:
• Por data?	• Sistema físico?	• Administração da própria empresa?
• Nível de investimento?		
• Há algum outro fator relevante?	• Na Nuvem?	• Serviço terceirizado?

Características da ISO 22301

ISO 22301:2012

- **Abordagem abrangente.**
- **É equilibrada para a construção de um SGCN.**



- Fornece as ferramentas para rever permanentemente todo o SGCN e melhorá-lo sempre que possível.
- Fornece um sistema de como treinar seus funcionários e conscientizá-los da importância da continuidade do negócio.
- Fornece um caminho de implementação perfeito.
- Fornece framework de gerenciamento, sobre como avaliar se a continuidade do negócio alcançou algum valor financeiro - estabelecendo objetivos e mensurando se os mesmos foram cumpridos.

Estrutura da ISO 22301

Um sistema de gerenciamento de continuidade de negócios – SGCN enfatiza a importância de:

Compreender as necessidades de continuidade e preparação, bem como, a necessidade de estabelecer políticas e objetivos de gerenciamento de continuidade de negócios.

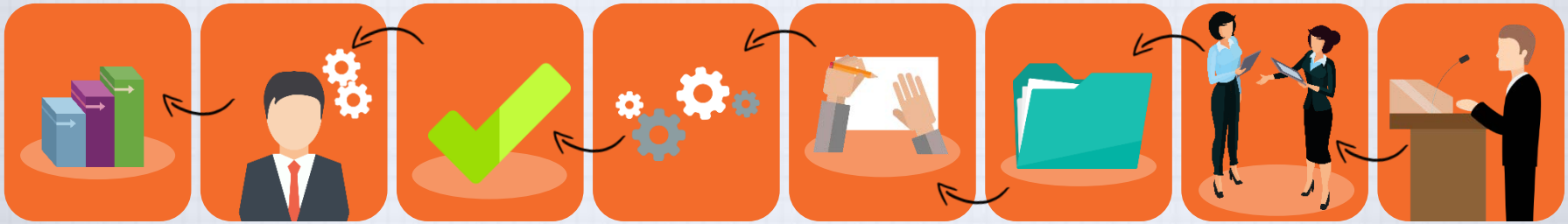
Implementar e operar controles e medidas para gerenciar os riscos globais de continuidade de uma organização.

Monitorar e revisar o desempenho e eficácia do sistema de gerenciamento de continuidade do negócio.

Melhorar continuamente com base em medidas objetivas.

ISO 22301:2012

Ajuda a definir um completo SGCN, pois como qualquer outro sistema de gerenciamento, ele também inclui diversos componentes principais, tais como:



Estrutura da ISO 22301

ISO 22301:2012

GENÉRICOS

A norma foi planejada para ser aplicada em todas as organizações, ou grande parte delas, independentemente do tipo, tamanho e natureza do negócio.

Projetar um SGCN adequado às suas necessidades e satisfazer os requisitos das partes interessadas.

Seções da Norma

Seção 0 – Introdução

Seção 1 – Escopo

Seção 2 - Referências normativas

Seção 3 - Termos e definições referentes à Continuidade de Negócios

Seção 4 - Contexto da organização

Seção 5 – Liderança

Seção 10 – Melhorias

Seção 9 - Avaliação de desempenho

Seção 8 – Operação

Seção 7 – Suporte

Seção 6 – Planejamento

Termos Chave do SGCN – Parte I

CONTINUIDADE DO NEGÓCIO

A capacidade de uma organização reagir às interrupções e continuar suas principais atividades ou operações.

INCIDENTE DISRUPTIVO

Qualquer tipo de incidente que interrompe as operações ou atividades. Pode ser causado por um desastre natural ou também pelo homem, uma falha técnica, etc.

ATIVIDADES

São os processos, ou múltiplos processos, que uma organização produz diretamente, ou apoiam a produção de produtos e / ou serviços.

(SGCN)

Faz parte das atividades gerais de uma empresa, e não se concentra apenas na implementação, mas também em manter e melhorar a continuidade do negócio.

Termos Chave do SGCN – Parte II

PLANO DE CONTINUIDADE DO NEGÓCIO – PCN *(Business Continuity Plan)*

É um documento que descreve como responder a um incidente e como continuar as atividades principais de uma organização.

TEMPO OBJETIVADO DE RECUPERAÇÃO – RTO *(Recovery Time Objective)*

É a quantidade máxima de tempo, em horas ou dias, dentro do qual uma atividade precisa ser retomada, caso contrário, o dano ao negócio seria simplesmente muito alto.

PONTO OBJETIVADO DE RECUPERAÇÃO – RPO (*Recovery Point Objective*) Ou **PERDA MÁXIMA DE DADOS – MDL** (*Maximum Data Loss*)

É a quantidade máxima de dados que uma organização pode perder, sem incorrer em danos inaceitáveis.

Recuperação de Desastres – DR (Disaster Recovery) ou Plano de Recuperação de Desastres – DRP (*Disaster Recovery Plan*)

Se concentra na recuperação de informações dos sistemas de comunicação e dos dados.

Termos Chave do SGCN – Parte II

Objetivo Mínimo de Continuidade de Negócios - OMCN (*Minimum Business Continuity Objective* – MBCO)

Capacidade mínima que uma organização deve fornecer imediatamente após a retomada das atividades.

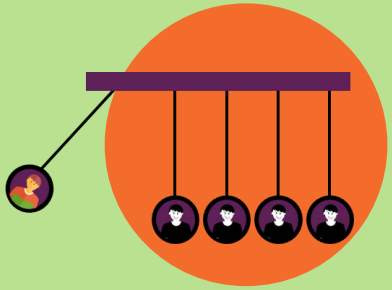
Termos Chave do SGCN – Parte III

Local alternativo

Disponibilidade

Análise de Impacto de Negócios – BIA

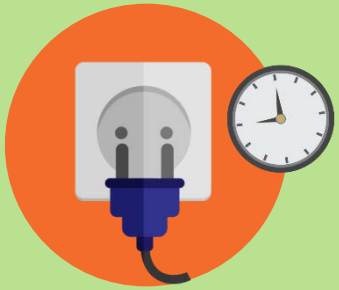
Probabilidade



Impacto

Controle ou Salvaguarda

Termos Chave do SGCN – Parte IV



Período Máximo de Interrupção Tolerável – ou **Interrupção Máxima Aceitável**

Objetivo Mínimo de Continuidade de Negócios – OMCN

Não conformidade

Ameaça

Tratamento de risco ou mitigação de risco

Vulnerabilidade

Pronto para o próximo?

Módulo 2

Contexto da Organização

Introdução

Descrever como determinar o contexto externo da Organização.

Descrever como determinar o contexto interno da Organização.

Explicar a importância das necessidades e expectativas das Partes Interessadas.

Explicar a importância de requisitos legais e regulatórios.

Entenderá os elementos do escopo do SGCN.

Entenderá o que é um SGCN e como este se encaixa em outros sistemas de gestão.

Compreendendo a Organização

Quais são os produtos / serviços que sua organização está produzindo?

Como é fabricado o produto ou o serviço que sua organização oferece?

Você conhece as unidades organizacionais, você tem um organograma?

Conhece todas as localizações físicas da organização?

Quem são seus principais parceiros e fornecedores? Por que eles são importantes para você?

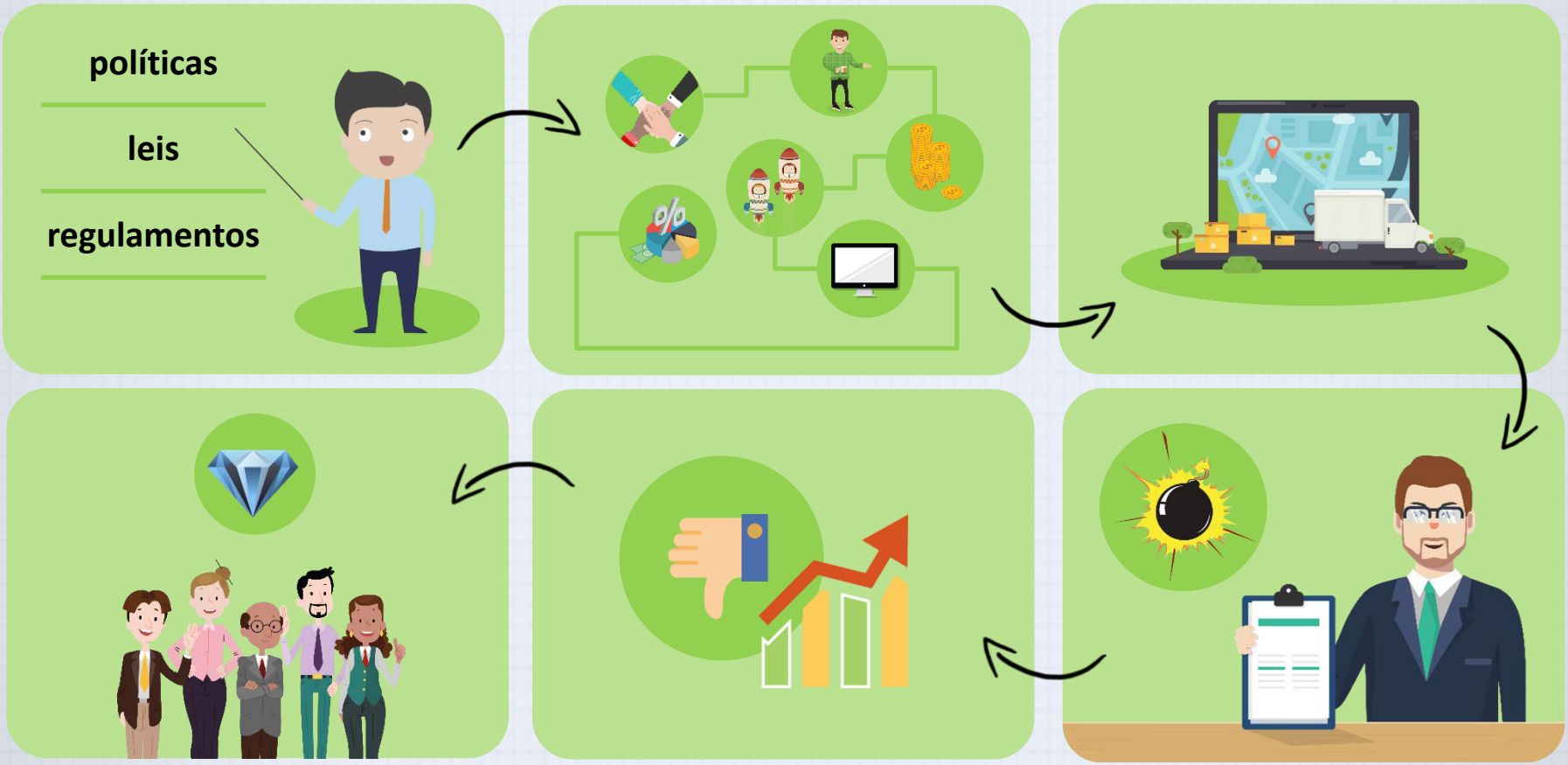
Você sabe qual é o principal ramo de atuação da sua organização?

Você conhece quais são os clientes em potencial da sua organização?

Compreendendo a Organização

Contexto Externo da Organização

A avaliação do contexto externo da organização deve incluir, quando relevante, os seguintes fatores:



Contexto Interno da Organização

Produtos e serviços, atividades, recursos, parcerias, cadeias de suprimentos e relacionamentos com partes interessadas;

As capacidades em termos de recursos e conhecimento, por exemplo, capital financeiro, tempo, pessoas, processos, sistemas e tecnologias;

Sistemas de informação, fluxos de informação e processos de tomada de decisão, tanto formal quanto informal;

Partes interessadas dentro da organização;

Políticas e objetivos, e as estratégias que estão em vigor;

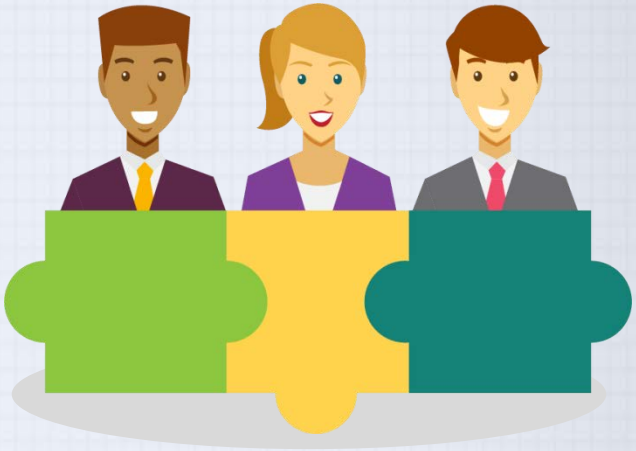
Oportunidades futuras e prioridades de negócios;

Percepções, valores e cultura;

Padrões e modelos de referência adotados pela organização;

Entender as Partes Interessadas

- Garantir que as necessidades e os requisitos das partes interessadas sejam levados em consideração.
- Identificar todas as partes interessadas que sejam relevantes para o seu SGCN;
- Determinar os requisitos com base nas necessidades e expectativas;
- Identificar não só os requisitos obrigatórios e declarados, mas também os que estão implícitos.



Identificando Partes Interessadas

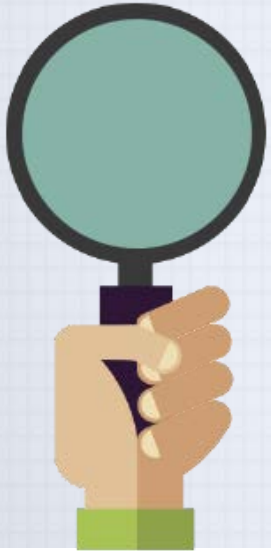
Listar todas as partes interessadas, organizações ou indivíduos, seus requisitos legais, regulamentares e outros interesses.

Funcionários

Acionistas / proprietários do negócio

Órgãos do governo...

Serviços de emergência



Fornecedores e parceiros

Meios de comunicação

Famílias de funcionários

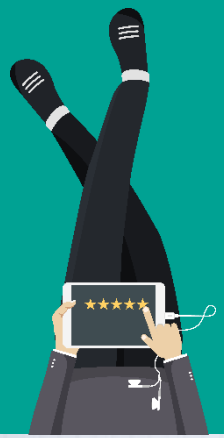
Clientes

Identificar o que cada um deles exige de você.

Identificando Partes Interessadas

Querem a segurança do investimento e um bom retorno.

Querem que você cumpra com leis e regulamentos.



Querem que você cumpra os contratos que você assinou com eles.

Quer notícias rápidas e precisas, etc.

Identificando Partes Interessadas

Os setores envolvidos na implementação e execução do SGCN.

A função de cada um desses para que todo o processo aconteça rapidamente, sem deixar algo importante para trás, e, com o maior nível de detalhes possível.

TRABALHO DA CONTINUIDADE DO NEGÓCIO

Esse tipo de documentação, com o passar do tempo, sofre modificações em função do ganho de conhecimento natural sobre novos aspectos de implementação do SGCN, bem como a mudança de funcionários ou mesmo da hierarquia da empresa.

Requisitos Legais e Regulatórios

Agências governamentais e reguladores são um tipo de parte interessada

ISO 22301:2012

SGCN

A organização deve assegurar que estes requisitos legais, regulatórios e outros requisitos aos quais estejam sujeitos são considerados no estabelecimento, implementação e manutenção de seu SGCN.

- **Deve estabelecer, implementar e manter diversos procedimentos.**
- **Esses requisitos e regulamentação devem estar alinhados com a continuidade das operações da empresa.**
- **Identifique, tenha acesso e avalie os requisitos legais e regulatórios aplicáveis ao seu mercado de atuação em relação:**
  - **Às operações, produtos e serviços;**
  - **Aos interesses das partes interessadas relevantes.**

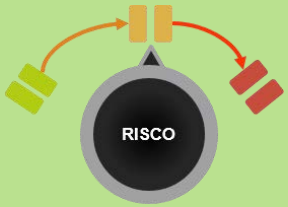
Requisitos Legais e Regulatórios

A ORGANIZAÇÃO DEVE REVISAR OS REQUISITOS LEGAIS E REGULAMENTARES ATUAIS E PENDENTES EM SUAS LOCALIDADES E ISSO PODE INCLUIR:

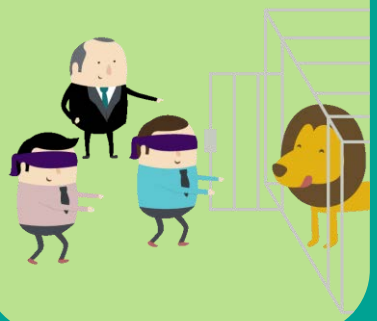
RESPOSTA A INCIDENTES: Inclui o gerenciamento de situações emergenciais, de saúde, segurança, bem-estar e material de legislação;

CONTINUIDADE: Especifica o escopo de um programa ou a extensão ou a velocidade da resposta;

RISCO: Requisitos que definem o escopo ou os métodos de um programa de gerenciamento de riscos;



PERIGOS: Requisitos operacionais relativos a materiais perigosos armazenados no local.



Elementos do Escopo do SGCN

ENTRADAS

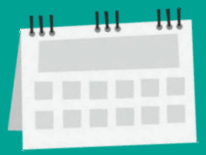
Requisitos das partes interessadas

Tamanho da empresa ou da organização

Orçamento

Tamanho do escopo

Data limite



- Alta direção
- Tomadores de decisão
- Detentores dos orçamentos
- Membros da equipe do projeto

Sessão 4.3 da norma ISO 22301

ESCOPO DO SISTEMA DE GESTÃO DE CONTINUIDADE DE NEGÓCIOS

Elementos do Escopo do SGCN

O escopo dos requisitos do documento deve contemplar:

- **Produtos e serviços;**
- **Locais físicos;**
- **Processos;**
- **Requisitos internos e externos.**

Determinar o Escopo do SGCN

Determinar o escopo do SGCN.

Garantir que o mesmo possa ser adequadamente comunicado às partes interessadas.

Os limites e a aplicabilidade do SGCN devem estar claros.

O escopo deve levar em consideração os contextos externos e internos e as necessidades e expectativas das partes interessadas.

TAMANHO | **NATUREZA** | **COMPLEXIDADE DA ORGANIZAÇÃO**

Ao escrever o escopo, é essencial garantir que os produtos e serviços, atividades, recursos, parcerias, cadeias de suprimentos e relações de partes interessadas estejam claramente distinguíveis no escopo.

Determinar o Escopo do SGCN

ESCOPO

Indicação da escala do incidente

Apetite ao risco da organização

Identificar como o SGCN se encaixa na estratégia geral de gerenciamento de risco da empresa.

Em termos de seus requisitos para a continuidade do negócio, leva em consideração a missão, metas, responsabilidades legais e obrigações internas e externas da empresa, seus objetivos operacionais, produtos e serviços e atividades e recursos.

Definindo o Escopo do SGCN

Não precisa necessariamente ser implantando na empresa toda.

- Melhor definir o escopo para o início de apenas um país, ou uma única unidade de negócios..

- E em seguida, aumentar gradualmente o escopo, à medida que sua curva de aprendizado cresce.

Definindo o Escopo do SGCN

O seu documento de escopo deve incluir:

- não apenas os locais físicos
- processos
- produtos e serviços
- requisitos
- atividades

Definindo o Escopo do SGCN

- A melhor maneira de determinar um escopo é organizar uma reunião com o seu patrocinador e / ou equipe de projeto.

- Essa decisão estratégica não pode ser feita apenas pelo coordenador de continuidade de negócio.

- Se for decidido que o escopo da implementação do SGCN envolve apenas uma parte da sua organização, então "a alta gestão" não será os seus principais executivos da empresa, mas sim, os altos gerentes destes departamentos, ou das unidades de negócios que foram selecionadas.

Qualidade e Quantidade de Documentos

- Guiam os procedimentos, regras, determinações, metas e muitos outros aspectos administrativos.
- Garantem que não apareçam problemas com a legislação.

+

- Quanto mais documentos e mais detalhados forem...

...mais difícil será mantê-los...

−

um número menor de documentos também é insuficiente e não descreve exatamente o que é preciso fazer.

Qualidade e Quantidade de Documentos

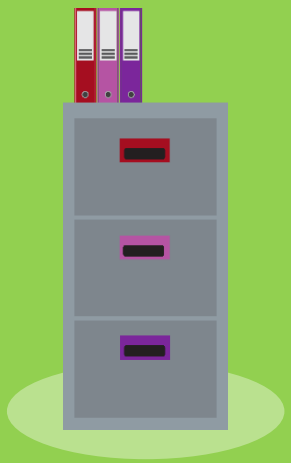
A quantidade e qualidade têm como base três aspectos básicos:

Facilidade de Armazenamento.

Armazene a documentação em um local organizado e de fácil acesso. Informações extensas para uma empresa pequena, não atrairá a menor atenção de quem precisa absorver uma quantidade alta de conteúdo.

Organização do conteúdo.

Organize a documentação para facilitar o acesso e a busca, principalmente em momentos de emergência.



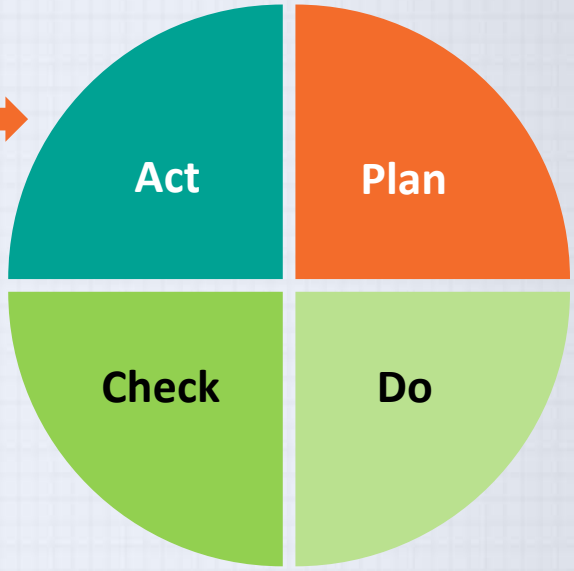
Uma quantidade racional.

Mantenha o equilíbrio na quantidade de documentação, mantenha o necessário, pois ambos, o exceto e a falta são prejudiciais.

Implantação da ISO 22301

ISO 22301:2012

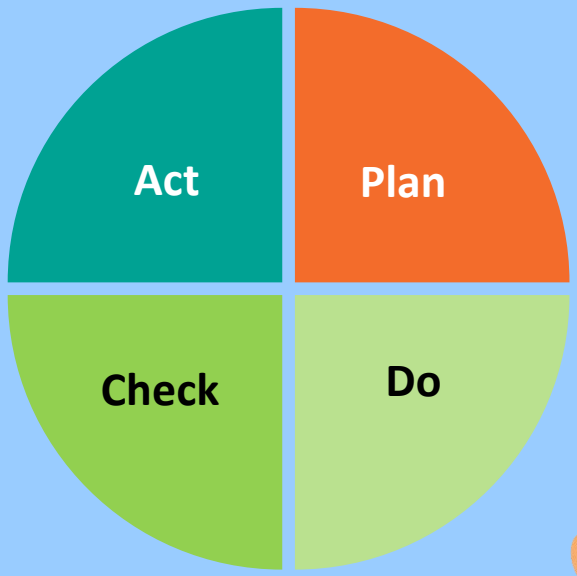
Suas etapas no plano de projeto devem se assemelhar às seções 4 a 10 da norma, exatamente na ordem em que estão descritas.



Ciclo Plan-Do-Check-Act

- Implementar o que planejou;
- Verificar se sua implementação atingiu os resultados pretendidos;
- Preencher a lacuna (Gap Analysis) entre o que conseguiu e o que você planejou.

Implantação da ISO 22301



Note que a palavra implementação NÃO quer dizer apenas a fase de implementação (Do) do ciclo PDCA, mas por implementação, entenda todas as etapas necessárias para aplicar os requisitos da ISO 22301, independentemente da fase do processo.

Processo de Implantação da ISO 22301 – Parte I

Todo o processo de implantação da norma deve ser acompanhado de um eficiente processo de comunicação com as partes interessadas.

Com as decisões e qualquer outro tipo de contato.

Processo de Implantação da ISO 22301 – Parte I

Estabelecer o projeto

1

Identificar Requisitos

2

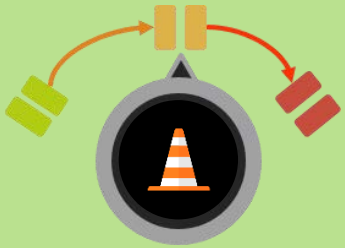
Definição do escopo, das responsabilidades e do gerenciamento

3

Identificar as prioridades e objetivos da continuidade

6

Identificar os riscos dos incidentes disruptivos



5

Implementar procedimento de suporte

4

Processo de Implantação da ISO 22301 – Parte II

Determinar as prioridades de mitigação e os recursos necessários

7

Definir os procedimentos de continuidade de negócios

8

Teste e exercícios

9

Revisão de gerenciamento

13

Auditoria de certificação

14

Conduzir uma auditoria interna

12

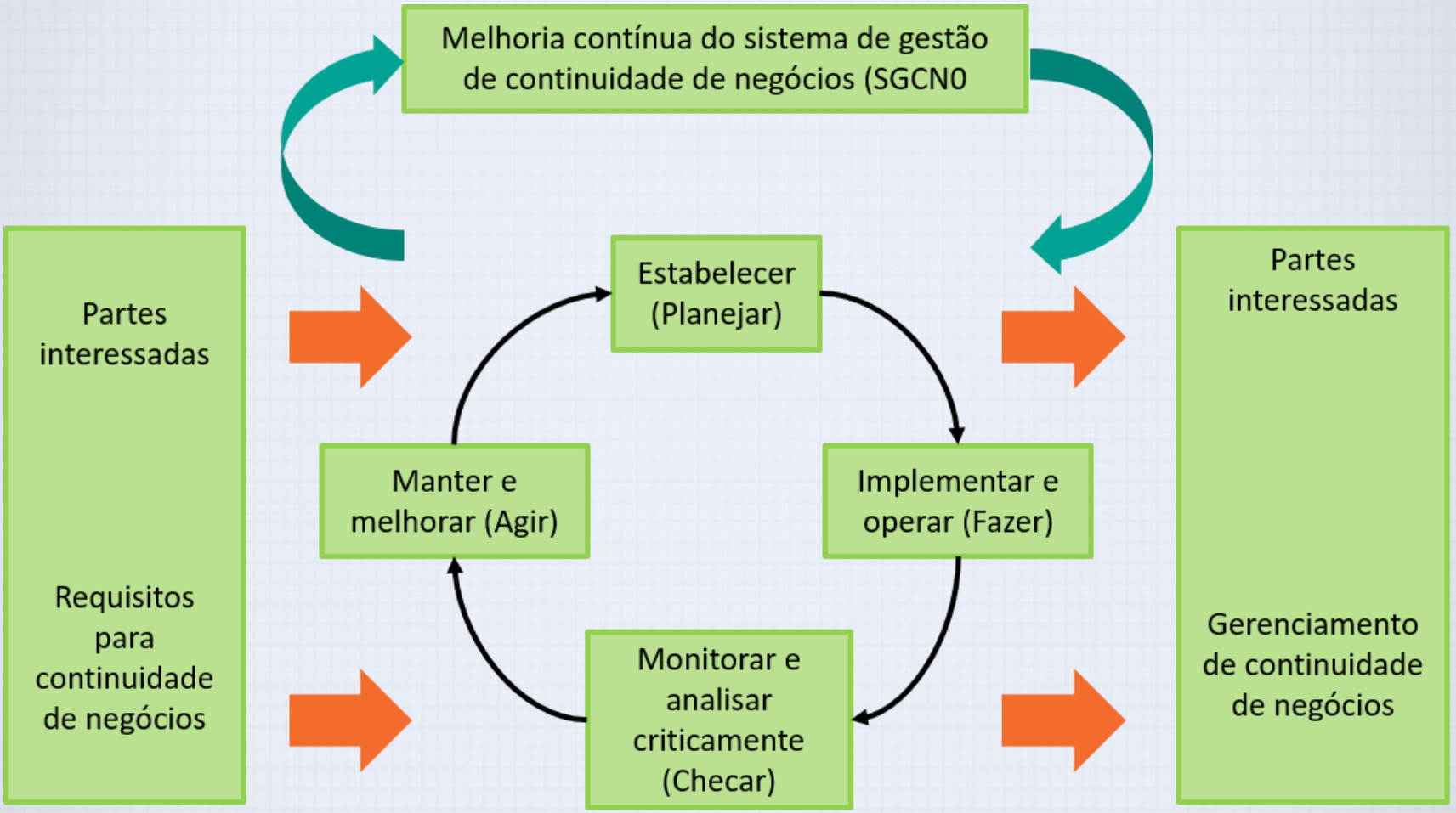
Ciclo de Vida do SGCN

"PLAN-DO-CHECK-ACT"

Garante um grau de consistência com outras normas de sistemas de gestão, tais como:

- ISO/IEC 9001, que trata do Sistema de Gestão da Qualidade.
- ISO/IEC 14001 - Sistemas de Gestão Ambiental.
- ISO/IEC 27001:2013 - Sistemas de Gestão de Segurança da Informação.
- ISO/IEC 20000-2 - Gestão de Serviços de TI.
- NBR ISO 28000 que trata da Especificação para Sistema de Gestão de Segurança para a Cadeia Logística.

Ciclo de Vida do SGCN



Ciclo de Vida do SGCN

- **Plan (Planejar e Estabelecer).** Estabelece uma política de continuidade de negócio, objetivos, metas, controles, processos e procedimentos pertinentes para a melhoria da continuidade de negócios, de forma a ter resultados alinhados com os objetivos e políticas gerais da organização.

- **Do (Implementar e operar).** Implementa e opera a política de continuidade de negócios, controles, processos e procedimentos.

- **Check (Monitorar e analisar criticamente)**. Monitora e analisa criticamente o desempenho, em relação aos objetivos e política de continuidade de negócios, reporta os resultados para a direção, para que estes procedam com uma análise crítica, e definam e autorizarem ações de melhorias e correções.

- **Act (Manter e melhorar).** Mantém e melhora o SGCN, tomando ações corretivas e preventivas, baseadas nos resultados da análise crítica pela Direção e reavaliando o escopo do SGCN e as políticas e objetivos de continuidade de negócios.

PDCA nas Seções da Norma

Seção 4

- Porque introduz os requisitos necessários para estabelecer o contexto de um SGCN.
- Demonstra como se aplica na organização, bem como suas necessidades, requisitos e escopo.

Seção 5

- Porque ele resume os requisitos específicos para o papel da Alta Direção no SGCN...

Seção 6

- Descreve os requisitos para a aplicação de objetivos estratégicos e princípios direcionadores para o SGCN como um todo.

PDCA nas Seções da Norma

Seção 7

- Suporta a operação do SGCN, atribuindo as competências e comunicação de forma recorrente, conforme a necessidade, com as partes interessadas, bem como, documentando, controlando, mantendo e retendo as documentações necessárias.

Seção 8

- Define os requisitos para a continuidade de negócios, determinando como abordá-los e como desenvolver procedimentos para gerenciar um incidente disruptivo.

Seção 9

- Resume os requisitos necessários para medir o desempenho da gestão da continuidade de negócios, a conformidade do SCGN, com esta Norma e com as expectativas da Direção, além de buscar a opinião dos gestores com relação às expectativas.

PDCA nas Seções da Norma

Seção 10

- Porque identifica e atua em aspectos do SGCN que não estão em conformidade, através de ações corretivas.

Documentação e Registros Necessários

- Determinando o contexto da organização;
- Procedimento para identificação dos requisitos legais e regulamentares aplicáveis;
- Lista de requisitos legais, regulamentares e outros;
- Escopo do SGCN e explicação de exclusões;
- Política de continuidade de negócio;
- Objetivos de continuidade de negócio;
- Competências pessoais;
- Comunicação com as partes interessadas;
- Processo para análise de impacto de negócios e avaliação de risco;
- Resultados da análise de impacto de negócios;

Documentação e Registros Necessários

- Resultados da avaliação de riscos;
- Procedimentos de continuidade do negócio;
- Procedimentos de resposta a incidentes;
- Decisão se os riscos e os impactos devem ser comunicados externamente;
- Comunicação com as partes interessadas, incluindo um sistema de assessoria de riscos, seja nacional ou regional;
- Registros de informações importantes sobre o incidente, ações tomadas e decisões tomadas;
- Procedimentos para responder a incidentes disruptivos;
- Procedimentos para restaurar os negócios a partir de medidas temporárias;
- Resultados de ações que abordam tendências ou resultados adversos;
- Dados e resultados de monitoramento e medição;
- Resultados de revisão pós-incidente;
- Resultados da auditoria interna;
- Resultados de análise crítica da direção;
- Natureza das não conformidades e as ações tomadas;
- Resultados de ações corretivas;

Documentação e Registros Não Obrigatórios

- Plano de implementação para alcançar os objetivos de continuidade do negócio
- Plano de treinamento e conscientização
- Procedimento para o controle de informações documentadas
- Contratos e acordos de nível de serviço - ANS (*SLA – Service Level Agreement*) com fornecedores e parceiros de terceirização
- Estratégias de continuidade do negócio
- Tratamento de risco
- Cenários de incidentes
- Exercícios e planos de teste
- Relatórios pós-exercícios
- Plano de manutenção do SGCN
- Métodos de monitoramento, medição, análise e avaliação
- Procedimento para auditoria interna
- Programa de auditoria interna
- Procedimento para ação corretiva

Integração com Outras Normas

DOCUMENTOS QUE PODEM SER USADOS PARA A ISO 22301, ISO 27001 E ISO 9001:

- Procedimento para controle de documentos;
- Procedimento para auditoria interna;
- Programa de auditoria interna;
- Relatório de auditoria interna;
- Procedimento para ação corretiva;
- Formulário de ação corretiva.

DOCUMENTOS QUE PODEM SER USADOS APENAS PARA A ISO 22301 E ISO 27001:

- Lista de requisitos legais, regulamentares e outros;
- Metodologia de avaliação de risco;
- Relatório de avaliação de risco;
- Plano de continuidade do negócio.

Integração de Documentos de Outras Normas

✓ **DOCUMENTOS QUE VOCÊ PODE USAR PARA A ISO 22301, ISO 27001 E ISO 9001:**

- Processo para determinar competências e treinamento do pessoal;
- Definir objetivos e medidas;
- Análise crítica da direção.

✓ **DOCUMENTOS QUE VOCÊ PODE USAR APENAS PARA A ISO 22301 E ISO 27001:**

- Processo que determina a aplicabilidade dos requisitos legais, regulamentares e contratuais;
- Manutenção do plano de continuidade do negócio;
- Teste do plano de continuidade do negócio.

Integração de Documentos de Outras Normas

- Poderá ter um procedimento de auditoria interna e um único programa de auditoria interna para as três normas.
- Permitirá planejar todas as auditorias anuais em conjunto.
- Será possível auditar todos os três sistemas ao mesmo tempo.
- Exigirá apenas um auditor interno para as três normas.

Integração com Outros Sistemas de Gerenciamento

ISO 22301:2012

COMPARTILHA ASPECTOS DIFERENTES COM OUTROS PADRÕES ISSO:

- **9001**
- **14001**
- **20000**
- **27001**

UTILIZA A MESMA FILOSOFIA DO MODELO PDCA:

- **O mesmo formato de documento ISO e os procedimentos de gerenciamento de documentos.**

Vários processos podem ser usados para mais de um padrão, ou a combinação de mais de uma norma, tais como:

- análise de gestão
- Determinação de competências e treinamento
- auditoria interna

Integração com Outros Sistemas de Gerenciamento

A ISO 9001:2015 compartilha:	ISO 27001, norma para segurança da informação compartilha:
• Análise crítica da direção	• Segurança da Informação
• Auditoria Interna	• Segurança Física
• Gerenciamento de documentação	• Segurança de ambiente
• Responsabilidades e papéis	• Controle de acesso
• Ações corretivas e preventivas	• Conformidade ou *Compliance*

ISO 38500:2015	Governança de TI	Compartilha o conceito do uso aceitável, eficiente e eficaz da tecnologia da informação dentro da organização.

Integração com Outros Sistemas de Gerenciamento

A ISO 20000-1:2011, uma norma para a Gerenciamento de Serviços de TI, a mesma na qual a ITIL se baseia, compartilha os processos:

- Gerenciamento de Incidentes
- Gerenciamento de Segurança da Informação
- Gerenciamento de Continuidade de Serviços de TI
- Gerenciamento de Capacidade
- Gerenciamento de Disponibilidade

Pronto para o próximo?

Módulo 3

Liderança

Introdução

O comprometimento e política de gestão em relação à importância do envolvimento da Alta Direção ou Diretoria no planejamento e gestão do sistema de continuidade de negócios.

1. Entender as implicações vitais do comprometimento da Alta Direção;
2. Descrever como a Diretoria pode demonstrar seu comprometimento em gerenciar a continuidade de negócios;
3. Descrever os elementos de uma política de continuidade de negócios.

Papéis e Responsabilidades:

1. Entenderá os diferentes papéis no planejamento e na gestão de continuidade de negócios;
2. Identificará as competências necessárias no planejamento e na gestão de continuidade de negócios.

Falhas no Projeto de Continuidade

- **RAZÕES PARA A FALHA:**

Falta de compreensão e de compromisso da Alta Direção.

Os profissionais de continuidade de negócios podem ser evitados pelos colaboradores.

- redução de custos
- estratégia de negócios
- riscos de negócios

- crescimento
- lucro
- participação de mercado
- satisfação do cliente

PARA SOLUCIONAR

- Diretoria
- Gerentes
- Colaboradores
- Fornecedores
- Outros

Falhas no Projeto de Continuidade

Venda a ideia de continuidade de negócio nos mesmos termos, na mesma linguagem.

- Informe o que a organização pode perder se houver uma catástrofe, uma paralização dos negócios.
- Demonstre em termos financeiros.
- Apresente os riscos.
- Evite mostrar ferramentas, sites ou qualquer outra solução sem antes demonstrar os benefícios de negócios da implementação de continuidade de negócios.

Liderança e Comprometimento

ISO 22301:2012

Liderança em relação ao SGCN

Eles precisam motivar e capacitar as pessoas a contribuírem com a eficácia de um SGCN.

Deverá apresentar evidências de seu comprometimento com o estabelecimento, implementação, operação, monitoramento, análise crítica, manutenção e melhoria do SGCN.

POLÍTICAS → **OBJETIVOS** → **REQUISITOS DO SGCN** → **Estejam estabelecidos e compatíveis com as diretrizes estratégicas e os processos de negócios da própria organização.**

Liderança e Comprometimento

- **Disponibilizar recursos necessários para um SGCN;**
- **Comunicar a importância de uma gestão de continuidade de negócios eficaz e;**
- **Garantir que o SGCN atinja os resultados esperados.**

- Todos os colaboradores da organização devem ser informados desses novos papéis e responsabilidades;
- Das definições de critérios e níveis de aceitação de riscos;
- Do envolvimento ativo em exercícios e testes;
- Das auditorias internas para o SGCN;
- Das análises críticas.

Responsabilidades da Alta Direção

- **Liderança**
- **Comprometimento**

Elaboração de uma política de continuidade de negócios.

Definição dos objetivos e planos do SGCN.

- Responsáveis pelo SGCN, assim como para implantar e oferecer manutenção do ciclo de continuidade de negócios.
- Estas pessoas podem realizar outras atividades dentro da empresa.

papéis

responsabilidades

competências

SGCN

Responsabilidades da Alta Direção

- Definir uma política de continuidade de negócios alinhada com o propósito da organização.
- Disponibilizar uma estrutura para estabelecer os objetivos de continuidade de negócio.
- Atender os requisitos e se comprometer com a melhoria contínua do SGCN.

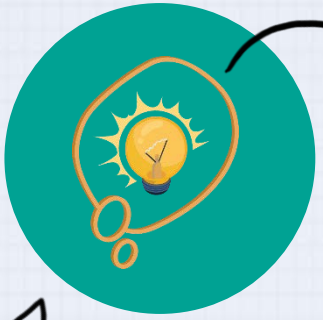
- Estar disponível como informação documentada
- Ser comunicada com toda organização.
- Estar disponível para as partes interessadas.
- Ser analisada criticamente de tempos em tempos, ou sempre que ocorrer mudanças significativas.

Responsabilidades da Alta Direção

Garantir que os papéis, responsabilidades e autoridades relevantes sejam atribuídos e comunicados dentro da organização.

- **Devem assegurar a responsabilidade e autoridade.**
- **Garantia de que o sistema de gestão esteja em conformidade com os requisitos da ISO 22301.**
- **E que sejam gerados relatórios de desempenho do SGCN para a Diretoria.**

Abordagem na Adoção de um SGCN



“vender a ideia”

Fazer com que eles consigam enxergar além da lucratividade, e comecem a pensar no Sistema de Continuidade dos Negócios como uma oportunidade e não apenas como um sistema de prevenção e recuperação de dados.

SGCN não é prioridade da empresa no momento.

Abordagem na Adoção de um SGCN

- **Um diferencial na qualidade da prestação de serviços.**
- **Na mitigação dos riscos.**
- **Quando se demonstra preocupação com as informações particulares dos clientes, etc.**

- Expor as informações de forma clara;
- Evitar o uso de palavras imperativas;
- Termos técnicos;
- Demonstrar incertezas;
- Projeções vaga.

ROI (retorno sobre investimento)

Demonstrando a Liderança no SGCN

Fornecer evidência de seu compromisso com o desenvolvimento e implementação de um SGCN.

Estabelecer as políticas e os objetivos de continuidade de negócios de acordo com o objetivo da organização.

Deve ser evidenciado o seu compromisso, não só no estabelecimento de um SGCN, mas também em outras fases, como na implementação, operação, monitoramento, revisão, manutenção e melhoria.

Nomear uma ou mais pessoas com a autoridade e competências apropriadas para serem responsáveis pelo SGCN e pela sua efetiva operação.

Demonstrando a Liderança no SGCN

Deve se assegurar que as funções, responsabilidades e competências do SGCN sejam estabelecidas.

Garantir a disponibilidade de recursos suficientes para que um sistema desse funcione.

Assegurar que as auditorias internas do SGCN sejam conduzidas, e principalmente, dirigir e apoiar uma melhoria contínua.

Demonstrar a liderança, principalmente em níveis mais intermediários de gestão.

Envolver no nível operacional, participando ativamente nos exercícios e nos testes, além de incluir assuntos sobre Continuidade de Negócio como um item permanente em reuniões de gerenciamento.

Demonstrando a Liderança no SGCN

- **Em resumo, os níveis gerenciais devem demonstrar uma liderança:**
- **Estabelecendo uma política de continuidade dos negócios;**
- **Assegurando que os objetivos e os planos do SGCN sejam estabelecidos, assim como as funções...;**
- **Comunicando o que foi definido, como os critérios de aceitação de riscos;**
- **Envolvendo-se ativamente nos testes;**
- **Assegurando que as auditorias internas do SGCN sejam realizadas;**
- **Realizando avaliações de gerenciamento do SGCN;**
- **Demonstrando seu compromisso com a melhoria contínua.**

Benefícios de um SGCN

Conformidade

Vantagem de marketing

Reduzir a dependência das pessoas

Evitar danos em grande escala

Objetivo da Política de SGCN

LIDERANÇA

- Aderente ao propósito da organização.
- Descrevam quais são os objetivos de continuidade de negócios.
- Uma declaração do seu compromisso em satisfazer os requisitos e do apoio da melhoria contínua do SGCN.

Disponível e documentada

Ser comunicada

Estar à disposição das partes interessadas

- **Em muitos casos, os executivos não têm ideia de como a continuidade do negócio pode ajudar sua organização.**

Objetivo da Política de SGCN

1

- **Fazer com que a alta direção defina o que quer alcançar com a continuidade do negócio.**

- **Criar um documento de fácil entendimento para os executivos, e com o qual eles poderão controlar tudo o que está acontecendo dentro do SGCN.**

2

Conteúdo da Política

PROPÓSITO DA EMPRESA

- **tamanho**

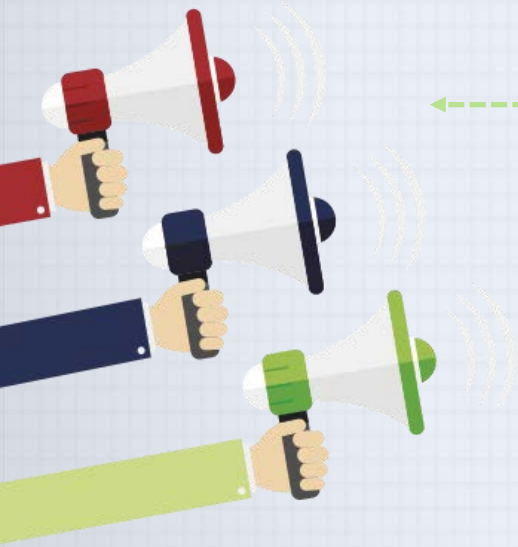
- **natureza**

- **complexidade**

- **ambiente operacional**

- **dependências**

- **cultura**

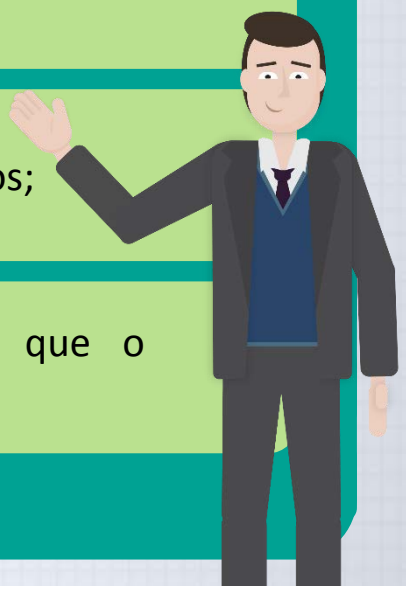


- Garantir que ela seja compreendida dentro da organização.
- Que esteja disponível para todas as partes interessadas.
- Pode ser complementar a outras políticas relevantes.

Conteúdo da Política

A POLÍTICA TAMBÉM DEVE:

- Ter um escopo e limites do programa de continuidade de negócios da organização, incluindo limitações e exclusões;
- Identificar as autoridades e delegações, incluindo a pessoa ou pessoas responsáveis pelo SGCN da organização;
- Estabelecer os critérios para o tipo e níveis de incidentes a serem abordados;
- Incluir referências a padrões, diretrizes, regulamentos ou políticas que o gerenciamento de continuidade deve considerar ou cumprir.



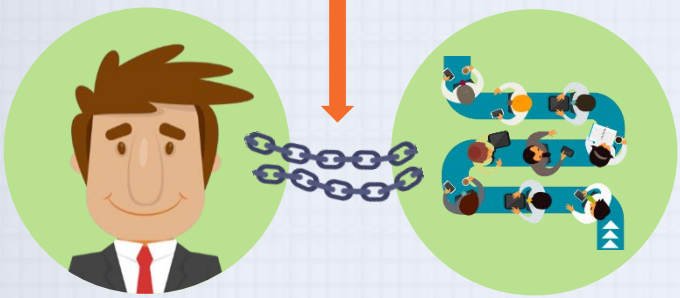
Conteúdo da Política

A política de continuidade do negócio pode conter o seguinte:

- **Termos-chave;**
- **Compromisso de financiamento;**
- **Referências a outras políticas relacionadas;**
- **Intenções da administração em relação aos níveis de serviço durante a interrupção;**
- **Atividades para estabelecer uma capacidade de continuidade de negócios;**
- **Gerenciamento contínuo e manutenção da capacidade de continuidade do negócio.**

Melhores Práticas de uma Política

POLÍTICA DE CONTINUIDADE DO NEGÓCIO



Atividades dos gestores

Continuidade de negócios

ISO 22301:2012

Exige que a gerência assegure que o SGCN seja compatível com a direção estratégica da organização.

Se uma política precisa ser adaptada à organização, então não faz sentido copiar a política.

MELHOR PRÁTICA DE COMUNICAÇÃO DE UMA POLITICA

É definir quem é responsável por essa comunicação.

Melhores Práticas de uma Política

Uma política não precisa ser um documento muito detalhado.

Pequenas Empresas

- Incluir o escopo do SGCN.
- As responsabilidades.
- Quem irá medir se os objetivos de continuidade do negócio foram alcançados.
- A quem os resultados precisam ser relatados.
- Com que frequência.

Política de segurança da informação

Política de gerenciamento de riscos

Melhor controlar essas políticas como documentos separados, pois o foco permanece muito mais claro.

Melhores Práticas de uma Política

OBJETIVOS

REQUISITOS CONTRATUAIS

AS LEGISLAÇÕES

Pense nas principais intenções de gestão com continuidade do negócio

Deve aprovar essa política

- Enviá-la primeiro para uma revisão por alguns outros tomadores de decisão importantes da sua empresa.

- Definir este documento como Política de Continuidade de Negócios ou como Política de Gerenciamento de Continuidade de Negócios.

Funções Organizacionais, Responsabilidades e Autoridades

- Assegurar que o programa de continuidade do negócio seja estabelecido, implementado e mantido de acordo com a política de continuidade de negócio;
- Informar sobre o desempenho do programa de continuidade do negócio para a alta administração a fim de proceder com revisões e fornece uma base para a melhoria;
- Promover a conscientização do programa em toda a organização;
- Garantir a eficácia dos procedimentos de resposta a incidentes, mas não necessariamente, na sua implementação durante um incidente.

COMITÊ DE DIREÇÃO

Todos os papéis, responsabilidades e autoridades no programa de continuidade do negócio devem ser definidos e documentados e estarem sujeitos a auditoria.

A DIREÇÃO da organização deve também, nomear um ou mais representantes com competências e autoridades definidas para:

"GERENTE DE CONTINUIDADE DO NEGÓCIO"

Apresentando os Benefícios

- Demonstrar os benefícios da continuidade de negócios na empresa.
- Nunca espere ser efetivo ao demonstrar os benefícios em apenas uma apresentação de poucos minutos.
- Levará certo tempo para que a Alta Direção ou Gerência absorva todos os benefícios.

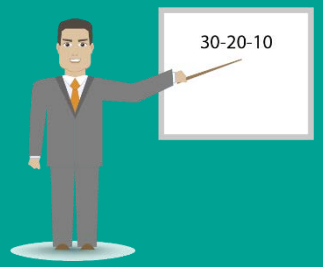
Apresentando os Benefícios

Técnicas

Discurso de elevador (*Elevator Speech*)

Encontre um aliado

Regra 30-20-10



Cuidado com as palavras

Desafios da Apresentação dos Benefícios

Mude esta visão ao explanar os benefícios.

O nível de apoio e suporte

gestão

acionistas

sócios

Deve estar no mesmo nível de importância.

- Lucratividade da empresa;
- Setores de tecnologia, marketing, operações, financeiro etc.
- Obter certa força política em relação as propostas.

- **Demonstrar os benefícios através de números e cálculos.**

Desafios da Apresentação dos Benefícios

- Detalhe qual é o significado do SGCN.
- Estruture a forma de apresentar os benefícios aos interessados.
- Identifique também as forças emergentes.
- Demonstre aos profissionais.
- Especifique o escopo.
- Utilize de dados e números.

Lidando com os Gerentes e Outros Funcionários

Basta apresentar, de forma convincente, os benefícios que sejam relevantes para o seu departamento, ou para eles pessoalmente.

- **Explicar o que pode ser feito para o departamento.**
- **Explicar que é possível garantir que todos os dados sejam copiados e recuperáveis, mesmo em caso de um desastre maior.**

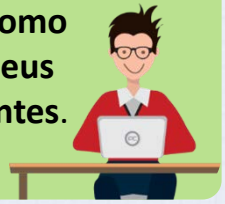
Lidando com os Clientes

CLIENTES → **PARCEIROS DE NEGÓCIOS** → Que fatalmente seriam afetados em casos de perda de dados, problemas na estrutura física ou tecnológica da empresa.

- **Quais dos serviços que você está fornecendo a eles devem ser tratados como prioritários.**
- **Quais são os tempos de recuperação.**
- **Qual é a capacidade mínima.**

Essencial que os clientes reconheçam os benefícios da continuidade dos negócios a eles.

Use os gestores de contas como se fossem seus representantes.



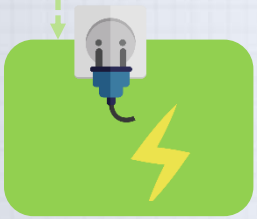
Aproxime-se do cliente.

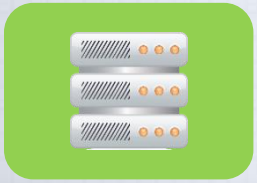
Lidando com os Céticos

"Se uma guerra acontecer, nada disso funcionará".

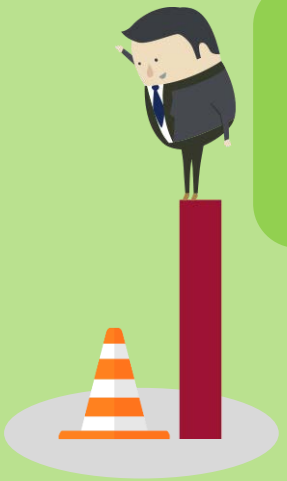
"Se ocorrer um grande desastre aqui na empresa, infelizmente não teremos a capacidade de fazer nada".

"Muito dinheiro para algo que nunca usaremos".





Lidando com os Céticos



"Não podemos prever todos os incidentes".

"Em caso de emergência, as pessoas cuidam primeiro de suas famílias e depois do negócio“.

"As pessoas irão reagir irracionalmente em situações de crise“.

Projeto de SGCN

O gerenciamento de liderança em relação ao SGCN deve ocorrer em todos os níveis.

TÉCNICAS DE MOTIVAÇÃO

ENGAJAMENTO E CAPACITAÇÃO

Um gerente de projeto deve ser alguém que tenha conhecimento e recursos de TI e de negócios também.

Um projeto de continuidade do negócio não deve ser tratado como um projeto de TI.

Tanto os sistemas de TI quanto as operações de negócios - e isso também significa pessoas, escritórios, papelada, etc. - devem ser restaurados - esta é uma das mensagens-chave, que precisa ser comunicada.

Equipe do Projeto e Patrocinador

- Defina o que deseja alcançar com seu projeto e quem será responsável por cada coisa.
- Descreva os papéis do gerente do projeto, dos membros da equipe e do patrocinador.
- Liste as etapas no projeto e seus entregáveis, marcos e prazos.

Plano do Projeto ← **GERENTE DE PROJETOS**

NUNCA PODE SER UMA PESSOA EXTERNA!

Patrocinador do projeto é uma pessoa de alta gerência

SEGURANÇA DA INFORMAÇÃO

GERENTE DE CONTINUIDADE DO NEGÓCIO

Equipe do Projeto e Patrocinador

Ajudar a coordenar o projeto em diferentes unidades organizacionais e, em alguns casos, tomar decisões ao invés dos gestores.

EQUIPE DO PROJETO

- Deve ser composta por cinco a sete pessoas de diferentes unidades organizacionais.
- O ideal é que você tenha um membro do departamento de TI e o resto de outros departamentos significativos ou unidades de negócios.

FERRAMENTAS

- Gráfico *Gantt*
- Softwares de gerenciamento de projetos

Pronto para o próximo?

Módulo 4

Planejamento e Suporte

Introdução

Objetivo da Avaliação de Riscos no planejamento e Gestão de Continuidade de Negócios:

- As etapas envolvidas no tratamento de riscos e oportunidades no SGCN;
- Como os objetivos de Continuidade de Negócios são estabelecidos e gerenciados.

Elementos de apoio do Sistema de Gestão de Continuidade de Negócios (SGCN):

- Os recursos necessários para planejamento e Gestão de Continuidade de Negócios;
- A importância da equipe de Resposta ao Incidente;
- Como é garantido o nível correto de competência de pessoas responsabilizando-se pelo SGCN;
- A importância da comunicação relativa à Continuidade de Negócios da Organização;
- A importância de informação documentada e de um Sistema de Gestão Documental;
- A importância da conscientização relativa à Continuidade de Negócios na Organização.

Planejamento

PLANO DE CONTINUIDADE DO NEGÓCIO

Assegurar que os objetivos sejam estabelecidos por funções e níveis dentro da organização, e indicar claramente como estes serão alcançados.

Significa que devemos nos planejar com ações para enfrentar os riscos e oportunidades.

Resgatar aqueles fatores que são relevantes para o seu propósito e para suas operações.

Entender quais são as necessidades das partes interessadas.

Planejamento

- Ser claramente indicados;
- Ser consistentes com a política;
- Ser mensuráveis;
- Ter prazos para sua realização;
- Levar em conta as necessidades e os requisitos aplicáveis;
- Permitir oportunidades para manter ou melhorar o desempenho;
- Ser monitorado e atualizado, conforme apropriado.

Planejamento

Definindo quem será responsável.

O que será feito.

Quando ele será completado.

Como os resultados serão avaliados.

Objetivos mínimos de continuidade de negócios (***MBCOs - Minimum Business Continuity Objectives***) para produtos e serviços mais importantes, definindo os níveis mínimos aceitáveis exigidos durante uma interrupção, para atingir os objetivos de negócio da organização.

Níveis de Objetivos

OBJETIVOS DO SGCN

ESTRATÉGICOS

Devem ser estabelecidos objetivos para o SGCN como um todo.

TÁTICOS

Estabelecer outros tipos de objetivos, como:

- **Objetivos Mínimos de Continuidade de Negócios (*MBCOs - Minimum Business Continuity Objectives*).**
- **Objetivos de exercícios e testes.**
- **Objetivos de Tempo de Recuperação (*RTOs - Recovery Time Objectives*).**
- **Objetivos do Ponto de Recuperação (*RPOs - Recovery Point Objectives*).**

Níveis de Objetivos

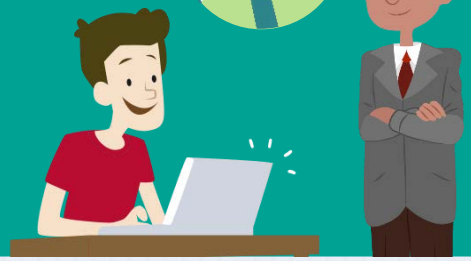
Definir objetivos fáceis de medir.

Os objetivos precisam ser específicos, mensuráveis, alcançáveis, relevantes e baseados no tempo.

S M A R T

- ***Specific***
- ***Measurable***
- ***Achievable***
- ***Relevant***
- ***Time-based***

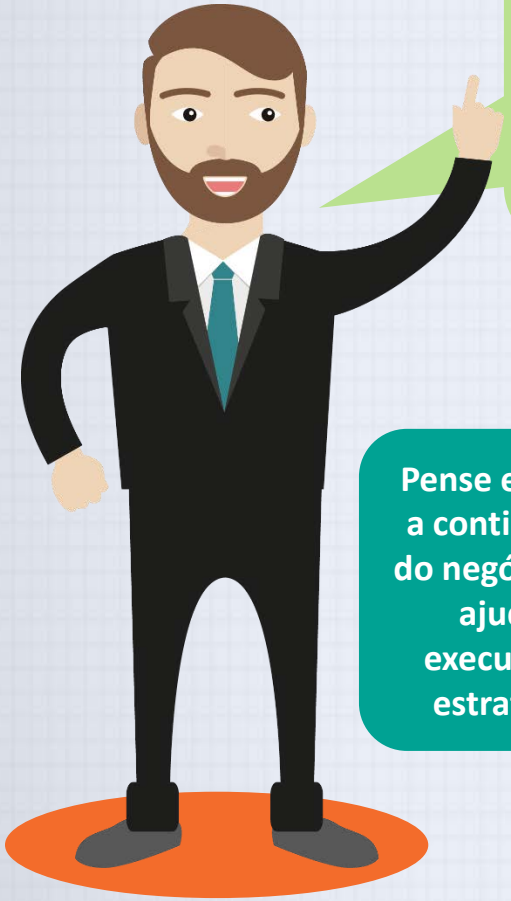
Apenas o que pode ser medido deve ser inserido no plano de ação, ou do contrário não será possível ver os impactos do SGCN.



O documento com a política do SISTEMA DE CONTINUIDADE DOS NEGÓCIOS – SGCN.

- Deve estar adaptado à organização.
- Definir os parâmetros a serem seguidos.
- Ser colocado à disposição para as partes interessadas.

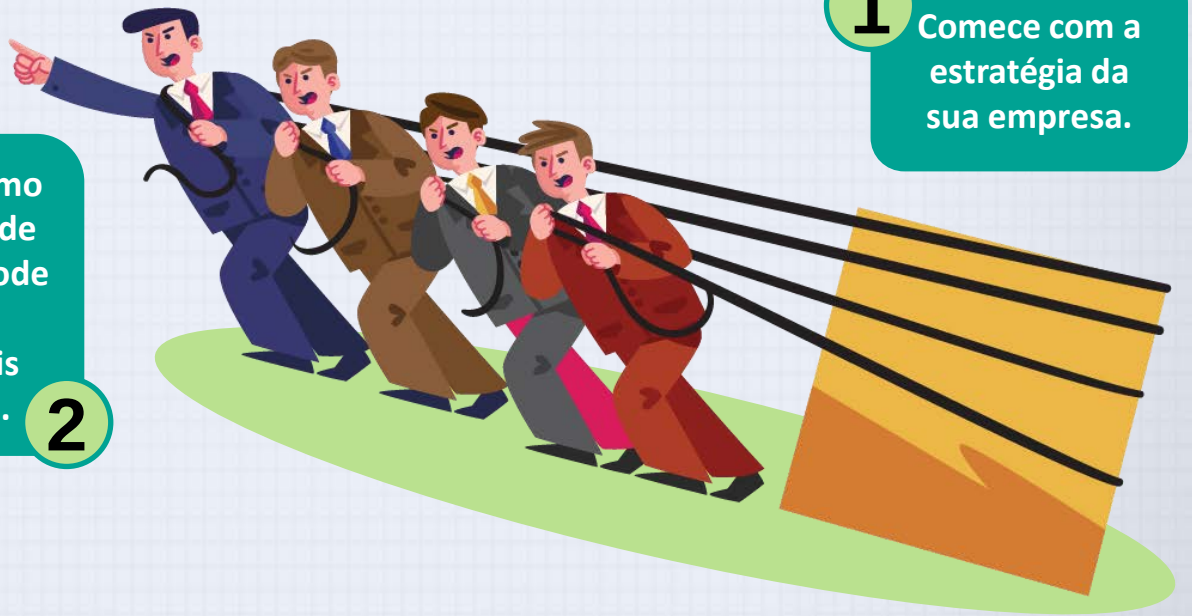
Estabelecendo os Objetivos



Definir os objetivos é sem dúvida extremamente importante, no entanto, nada adianta caso não seja possível mensurar se podemos ou não, atingir tais objetivos.

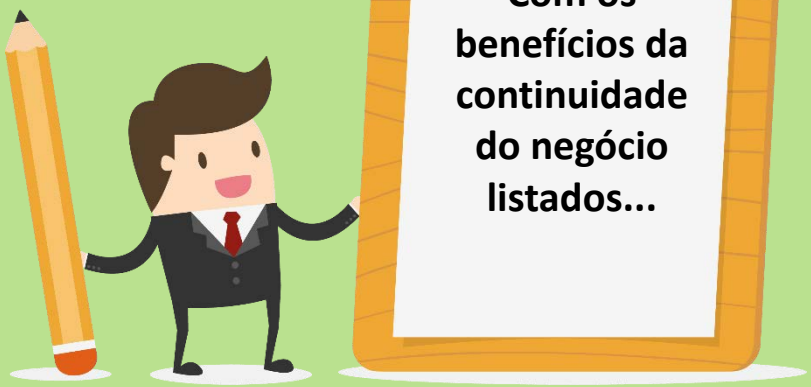
Se forem mensuráveis, você precisa medir para saber se conseguiu o que planejou depois do prazo estabelecido.

1 Comece com a estratégia da sua empresa.



Pense em como a continuidade do negócio pode ajudar a executar tais estratégias. 2

Estabelecendo os Objetivos



- Avalie como eles podem ser traduzidos em objetivos.
- Envolva toda a equipe do projeto nesse brainstorming.
- Se alguém na sua empresa já estiver lidando com a medição do desempenho, eles poderão ser de grande ajuda.

Definindo os Níveis de Objetivos

O que exatamente a sua empresa faz?

Como ter um Sistema de Continuidade de Negócios ajudará cada setor a alcançar seus objetivos, que vão além de entregar um produto ou serviço ao cliente?

Como o impacto do SGCN será medido?

A empresa já adota algum sistema de notas, ou conceitos, para classificar a qualidade das atividades?

Este sistema pode ser usado em todos os setores?

- Criar uma lista de objetivos que esteja de acordo com a realidade e possa trazer benefícios para todos.
- O cuidado em identificar pontos críticos possibilita uma melhor visão global dos índices pretendidos.
- A percepção das dificuldades facilita a criação do levantamento das variáveis envolvidas.

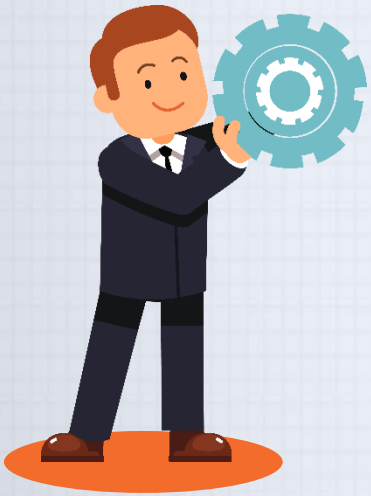
Suporte

Depois de todo o planejamento e definição dos objetivos...

- Deve determinar e fornecer todos aqueles recursos necessários para que um SGCN funcione.

- Garantir a disponibilidade dos recursos necessários para implementar e controlar o SGCN...

- e para atender aos objetivos do gerenciamento de continuidade de negócio da empresa, incluindo a resposta a incidentes.



- **capacidades**
- **recursos**
- **estruturas**
- **mecanismos de suporte**

- **Política**
- **Objetivos**
- **Metas de continuidade de negócios**

Equipe de Resposta a Incidentes

- Detecção e escalação de incidentes;
- Avaliação de incidentes;
- Disparo de uma resposta apropriada;
- Ativação de plano;
- Evacuação;
- Triagem e primeiros socorros;
- Segurança de alguns parâmetros;
- Controle de tráfego;
- Estabelecimento e operações de um centro de operações de emergência;
- Contatar os serviços de emergências e autoridades locais;
- Contatar a equipe de comunicação pública sobre crise da organização;
- Coordenação e comunicação da resposta ao incidente;
- Análise e geração de relatórios pós-incidentes.

A equipe de resposta a incidentes deve formar um grupo, do qual será responsável por gerenciar qualquer incidente disruptivo que afete significativamente, ou tenha o potencial de impactar a organização.

Sensibilização e Treinamento

Sabe qual a principal causa de fracasso na implantação de um Sistema de Continuidade dos Negócios?

Falta de engajamento dos funcionários.

- **Faça um plano anual com as técnicas e explicações que serão usadas mês a mês.**
- **Se optar pelo treinamento formal, esteja ciente de que o melhor a fazer é depois testar seus funcionários.**

e-mail

artigos

apresentação

conversas informais

fóruns

Competências e Tipo de Treinamentos

A empresa precisa definir um sistema que gerencie as competências necessárias do pessoal em todos os papéis e responsabilidades do SGCN.

Gestão de conhecimento

Conscientização

Compreensão e habilidades necessárias para realizar as atividades de continuidade de negócio.

- Esquema de avaliação das competências - para ajudar na identificação de necessidade de treinamento ou desenvolvimento.

PROGRAMA DE DESENVOLVIMENTO DE COMPETÊNCIAS

- Ajudar no compartilhamento de conhecimento:

Detalhes sobre contratação de pessoas com as competências necessárias;

Concepção e desenvolvimento de um programa de desenvolvimento pessoal.

UM PROCESSO para identificar e controlar os requisitos de treinamento em continuidade de negócios para todos os participantes.

Competências e Tipo de Treinamentos

TIPO DE TREINAMENTO QUE PODE SER APROPRIADO:

- Gerenciamento do programa de continuidade de negócio;
- Análise de impacto de negócio;
- Desenvolvimento e implementação da documentação de continuidade do negócio;
- Execução de um programa de exercícios e testes de continuidade;
- Avaliação de risco;
- Habilidades de comunicação.

Gerenciamento de evacuação

Como abrigar o pessoal em outro local

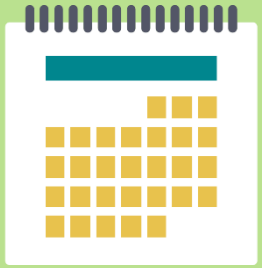
Processos de check-in para contabilizar os funcionários

Acomodações em locais de trabalho alternativos

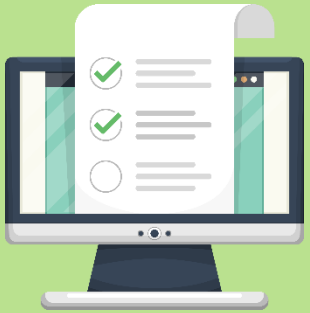
Manipulação de informações da mídia pela empresa

Competências e Tipo de Treinamentos

Treinamentos práticos



Em intervalos regulares



Exercícios e testes

- Devem ser treinadas também em como fazer a interação com os primeiros socorros e outras partes interessadas.
- Devem receber treinamento sobre prevenção de incidentes que possam se transformar em crises.

Programa de Conscientização

funcionários

contratados

parceiros

fornecedores

Todos devem ter ciência da política de continuidade do negócio, e do seu papel e responsabilidade em relação à prevenção, detecção, mitigação, autoproteção, evacuação, resposta, continuidade e recuperação.

- Construir e promover uma cultura de gerenciamento de continuidade de negócio.
- Deve fazer parte dos valores da empresa, devendo ser sua base.
- Uma boa conscientização pode aumentar a resiliência ao longo do tempo...
- ... e minimizar a probabilidade e impacto das interrupções.
- Deve ser apoiado pelo pessoal na organização e liderança dos gerentes.
- Incluir discussões sobre o SGCN como tópico nas reuniões da equipe e de gerenciamento...

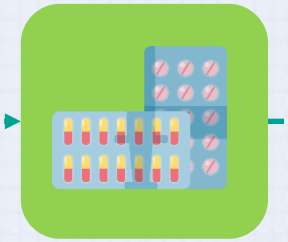
Comunicação

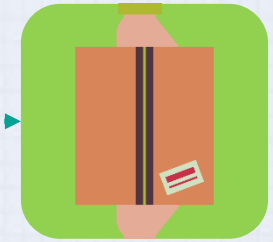
- Deve ser elaborado um processo que defina os meios de comunicação para receber, documentar e responder a todas as partes interessadas, principalmente para alertar os potenciais impactos de um incidente real ou iminente.

COMUNICAÇÃO EXTERNA

- clientes
- entidades parceiras
- comunidade local e etc.

Autoridades competentes





A organização deve ter procedimentos efetivos para a comunicação e troca de informações

Procedimento Para Controle de Documentos

atas de reunião

Deve definir claramente as responsabilidades e regras para o tratamento dos documentos:

procedimentos | **registros** | **relatórios**

documentos | **planos** | **políticas**

- Como eles são mantidos atualizados;
- Qual sistema de versão está em uso;
- Mídia sobre a qual eles são produzidos;
- Como é rastreado as mudanças nos documentos;
- Como você controla os documentos externos que recebe.

ISO 22301:2012

"informações documentadas"

Pode ser uma boa opção elaborar o procedimento de controle de documentos no início do seu projeto.

Controlando os Documentos

Antes de criar o controle de documentos, verifique se já existe algum procedimento que define gerenciamento de documentação ou registros em sua empresa.

1

- **Sistema de gerenciamento de documentos.**
- **Software de gerenciamento de projetos.**
- **Software de gerenciamento de relacionamento com clientes.**

Se já possui regras semelhantes, proponha mudanças, para que fiquem compatíveis com a ISO 22301 e enviem o documento para revisão e aprovação conforme o processo definido.

Controlando os Documentos

Proprietário de cada documento.

- Poderia, ou não, ser a mesma pessoa que o escreveu, e ainda, poderia ser responsável por todos os documentos do SGCN.
- É indicado que o procedimento de controle de documentos possa abranger toda a documentação de uma empresa.
- O uso de um sistema de gerenciamento de documentos depende muito do tamanho da sua empresa, pois para empresas menores, uma ou várias pastas em sua intranet já podem ser suficientes.

Informações Documentadas

- Tome cuidado com a proteção e não divulgação das informações confidenciais.
- Garanta a integridade das informações, tornando-as invioláveis, com backup, acessíveis apenas para o pessoal autorizado e protegido contra danos e perdas.
- Ao criar e atualizar as informações garanta a sua identificação e descrição do documento, independente do formato e da mídia utilizada.
- Todas as informações documentadas exigidas pelo SGCN devem ser controladas para garantir que estejam disponíveis e adequadas para uso.

Pronto para o próximo?

Módulo 5

Operação

Introdução

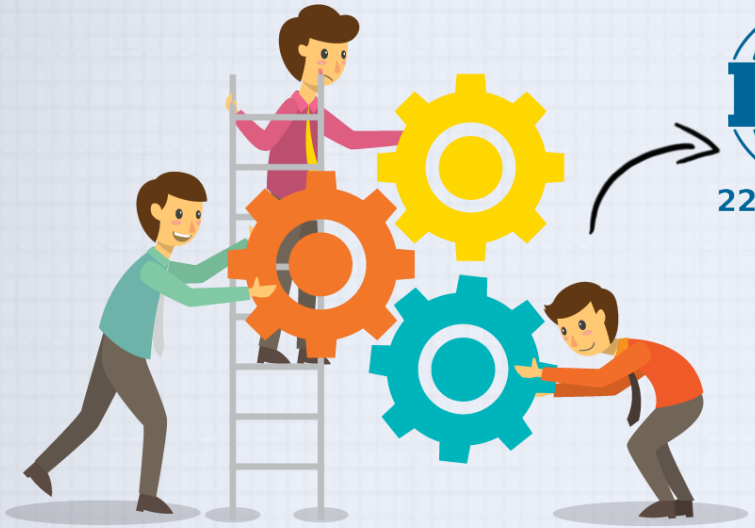
Estratégia organizacional e os procedimentos relacionados, além de:

- Explicar a relação entre a estratégia e os procedimentos de Continuidade de Negócios;
- Descrever o processo de estabelecimento e implementação de procedimentos de Continuidade de Negócios;
- Explicar o conteúdo de um Plano de Continuidade de Negócios;
- Descrever os procedimentos incluídos no Plano de Continuidade de Negócios.

Análise de Impactos nos Negócios (*BIA - Business Impact Analysis*), Avaliação de Riscos (*RA - Risk Assessment*) e a operação da BIA e da RA

- Descrever o objetivo da BIA e seu conteúdo;
- Explicar o conceito de impacto sobre os Negócios e diferentes tipos de impactos;
- Explicar os conceitos básicos da BIA;
- Explicar o conceito de RA e dos diferentes elementos;
- Citar as ameaças, riscos e impactos relacionados ao GCN.

Operação



ISO 22301:2012

A implementação dos ELEMENTOS BÁSICOS da continuidade de negócios.

Principais elementos que serão utilizados para construir sua resiliência, ou seja:

- Avaliação de Riscos (*RA - Risk Assessment*) e Análise de impacto de Negócios (*BIA - Business Impact Analysis*) como elementos principais de análise;
- Estratégia e planejamento de continuidade de negócios, incluindo a resposta a incidentes e recuperação de desastres;
- Plano de Continuidade de Negócios.

Operação

Sem antes de preparar cuidadosamente sua estratégia, pois seriam inúteis em caso de desastre.

Não tente desenvolver sua estratégia sem antes obter os insumos da RA e a BIA.

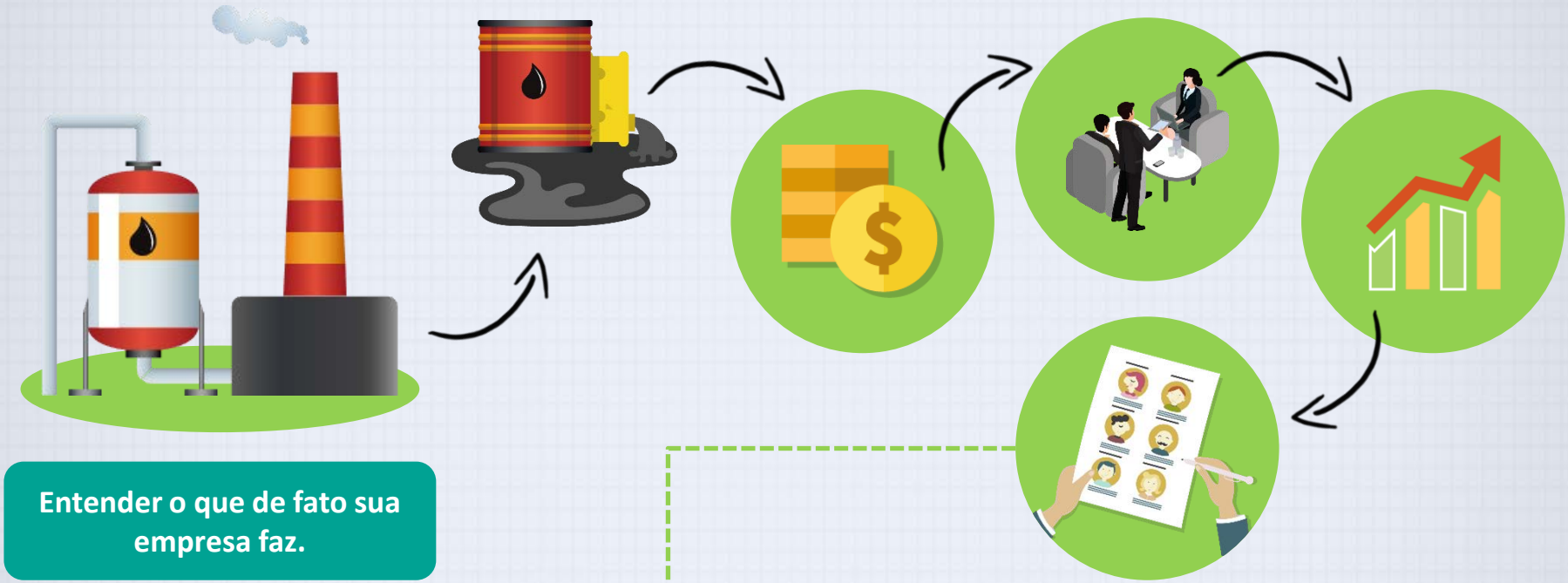
AVALIAÇÃO DE RISCO

Operação

Os principais documentos e registros importantes gerados para esta fase de Operação são:

- Processo para análise de impacto de negócios e avaliação de risco;
- Resultados da análise de impacto de negócio;
- Resultados da avaliação de risco;
- Procedimentos de continuidade do negócio;
- Procedimentos de resposta a incidentes;
- Decisões se os riscos e impactos devem ser comunicados externamente;
- Comunicação com as partes interessadas;
- Registros de informações importantes sobre o incidente, ações tomadas e decisões tomadas;
- Procedimentos para responder a incidentes;
- Procedimentos para restaurar e retornar o negócio a partir de medidas temporárias.

Definindo Atividades



Entender o que de fato sua empresa faz.

E Como é possível separar as atividades em unidades.

Com base em **PROCESSOS**;

Com base em **UNIDADES ORGANIZACIONAIS.**

- Cada um destes se torna uma atividade em termo de SGCN.
- Desenvolver a BIA, a RA, a estratégia e elaborar o plano de recuperação.

Fica mais fácil entender os processos, como uma atividade.

Definindo Atividades

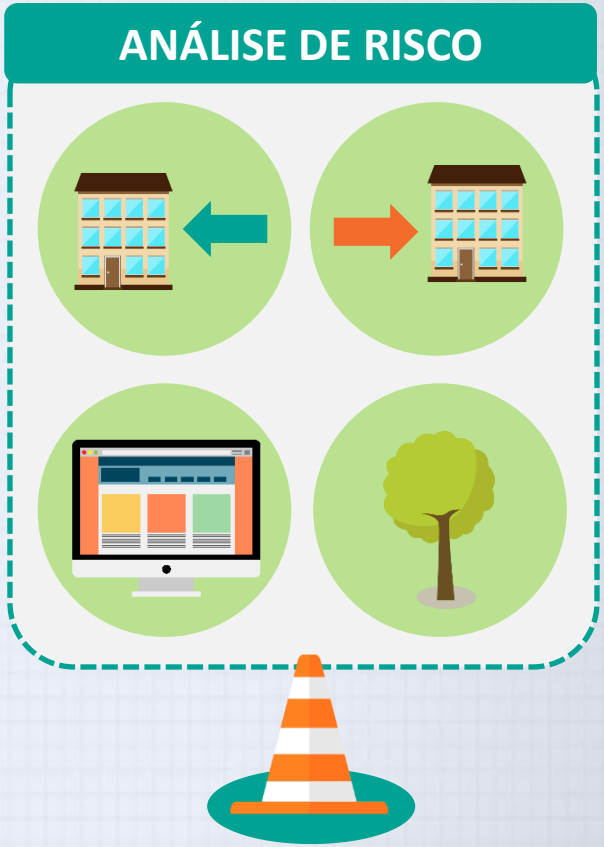
Garante que todos os funcionários lerão somente um único plano quando necessário.

Ficará mais difícil avaliar todos os impactos durante uma BIA se você não souber onde seu processo começa e onde ele termina, por isso, durante a BIA você precisa fazer muita comunicação entre os departamentos e a coordenação.

Planos de recuperação cobrem apenas segmentos de vários processos.

Definindo Riscos

Isso possibilita obter uma melhor visão global de todos os recursos envolvidos na entrega dos produtos e serviços.



Técnica simples de identificação de riscos:

- Fazendo questionamentos.
- Criar cenários e imaginar riscos futuros, provenientes do surgimento de novas tecnologias.
- Perda da matriz da empresa em virtude dos desastres ambientais.
- Problemas econômicos ainda não previstos e das rápidas e imprevistas mudanças no setor onde a empresa está inserida.

Atividades da Operação da Continuidade

Como você pode se preparar para algum incidente, sem conhecer a natureza deles?

E quais as chances de você se preparar para um incidente que tem pouca possibilidade de acontecer, ou imprevistos que podem arrasar a sua empresa?

pesquisa

levantamento

Use as atividades ou departamentos já listados anteriormente.

SISTEMA DE CLASSIFICAÇÃO

- atribuição de conceito
- atribuição de notas para cada risco.
- cálculo de uma média aritmética ou ponderada.

Atividades da Operação da Continuidade

A partir deste cálculo e classificação, é possível escolher quais riscos trataremos e quais riscos nós aceitaremos.

EX.: Trocar a fiação de todo um escritório demandaria mudanças na própria arquitetura do prédio.

- análise de riscos
- com relatório
- cálculo de riscos

- medidas para diminuir a vulnerabilidade e risco residual

Risco residual

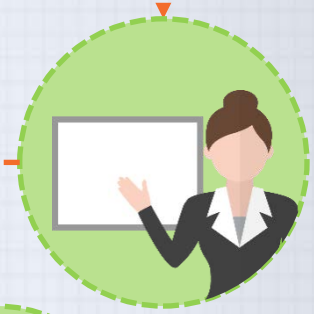
O risco que sobra – que deve ser menor que o risco inicial.

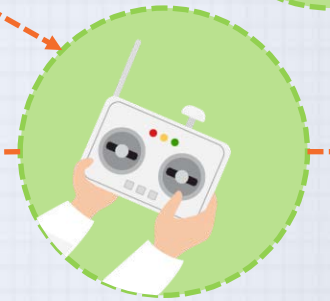
Planejamento e Controle das Operações

Programa de continuidade de negócios

Garanta que os elementos da continuidade de negócios sejam gerenciados adequadamente e com eficácia.

Atividades operacionais





"DOCUMENTAR"

Que estabeleça alguns critérios para essas atividades.

fornecimento de bens e serviços

Atividades dos contratados ou terceirizados.

Indicativo de SGCN Efetivo

Exercícios e Testes;

Monitoramento e Medição;

Revisão Pós-Incidente;

Auditoria interna;

Análise Crítica da Direção;

Processo de Melhoria.

- O escopo e os objetivos do SGCN devem ser consistentes;
- Os resultados do plano de continuidade do serviço documentado devem ser consistentes com os objetivos e expectativas do plano;
- Documentar as áreas de melhoria para planos de continuidade de serviços;
- Documentar as áreas de melhoria para testar planos de continuidade de serviços.

Elementos de um SGCN

Kosutic de 2013

"Sistema de Gerenciamento de Continuidade de Negócios faz parte das atividades globais da empresa que se concentram não apenas na implementação, mas também na manutenção e melhoria da continuidade do negócio. Assim como as empresas têm, por exemplo, gerenciamento financeiro com vários papéis e responsabilidades, da mesma forma, a continuidade do negócio possui certas políticas, procedimentos, processos, etc. que fazem parte do SGCN".

Elementos de um SGCN

- Estrutura organizacional
- Responsabilidades
- Processos
- Recursos
- Atividades

- Com base em unidades organizacionais
- Com base em processos

- Estratégias
- Políticas
- Planos
- Procedimentos
- Registros

- Documentação: Lista de atividades de continuidade de negócios que na verdade são obrigatórios;
- Mecanismos de controle dentro do SGCN para um planejamento e controle operacional efetivo;
- Estabelecimento de um efetivo gerenciamento do ambiente de GCN;
- A manutenção efetiva da continuidade do negócio;
- Resultados indicativos de um GCN efetivo.

Elementos do Programa de Continuidade de Negócio

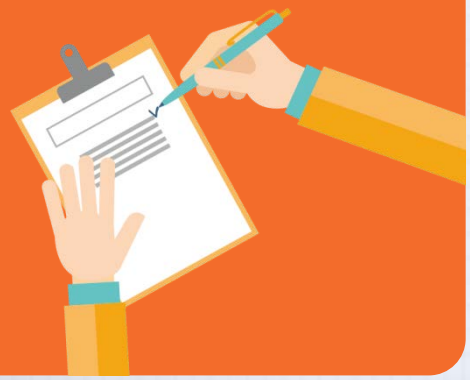
Gerenciamento do Programa de Continuidade do Negócio.

Incorporar as competências e conscientização.

Compreender a organização.

BIA RA

Exercício e teste.



Desenvolver e implementar uma resposta para a continuidade de negócios.

Selecionando opções de continuidade de negócios.

Elementos do Programa de Continuidade de Negócio

- Gestão do ambiente do GCN;
- Gestão das capacidades de continuidade do negócio;
- Medir a eficácia do SGCN.

Gestão do Ambiente de GCN

GESTÃO

Garantir a relevância do escopo da continuidade e das funções e responsabilidades para a continuidade do negócio, através da promoção da continuidade em toda a organização.

- **Abordar a gestão do ambiente do GCN;**
- **As capacidades de continuidade do negócio;**
- **Ser possível medir a eficácia do SGCN.**

Adotar um método reconhecido no mercado de gerenciamento de projetos, pois assim o programa SGCN será efetivamente gerenciado.

Gestão da Capacidade e Medição da Eficácia

Manutenção do PROGRAMA DE CONTINUIDADE DO NEGÓCIO.

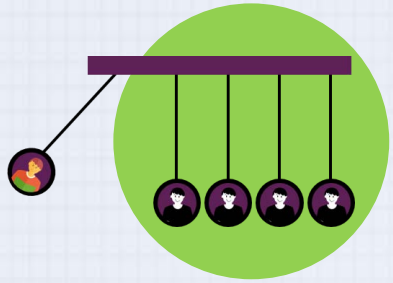
- Além de coordenar uma revisão periódica e a atualização de todas estas capacidades de continuidade do negócio, incluindo uma revisão ou reformulação das BIAs e das RAs.

- Fazer a gestão das capacidades é assegurar a manutenção da documentação de resposta.

Gestão da Capacidade e Medição da Eficácia

- Os principais produtos e serviços identificados e protegidos, garantindo assim a sua continuidade;
- Uma capacidade de gerenciamento de incidentes que forneça uma resposta efetiva;
- A compreensão da própria organização dela mesma e de suas relações com outras organizações, reguladores ou departamentos do governo, autoridades locais e os serviços de emergência.
- Uma equipe treinada para responder efetivamente a um incidente ou ruptura através de exercícios regulares;
- Que os requisitos das partes interessadas sejam entendidos e que possam ser entregues;
- Os funcionários recebem o apoio e comunicações em caso de incidentes;
- A cadeia de fornecimento da organização está segura;
- A reputação da organização está protegida;
- A organização continua em conformidade com suas obrigações legais e regulamentares;
- Os controles financeiros são mantidos ao longo de um incidente.

Análise de Impacto no Negócio e Avaliação de Riscos



ANÁLISE DE IMPACTO

AVALIÇÃO DE RISCO

DOCUMENTAÇÃO

PROCESSO FORMAL

BIA **RA**

Vão permitir a identificação de algumas medidas para limitar o impacto de uma interrupção nos principais serviços, encurtar o período destas interrupções e ainda, reduzir a probabilidade de uma interrupção.

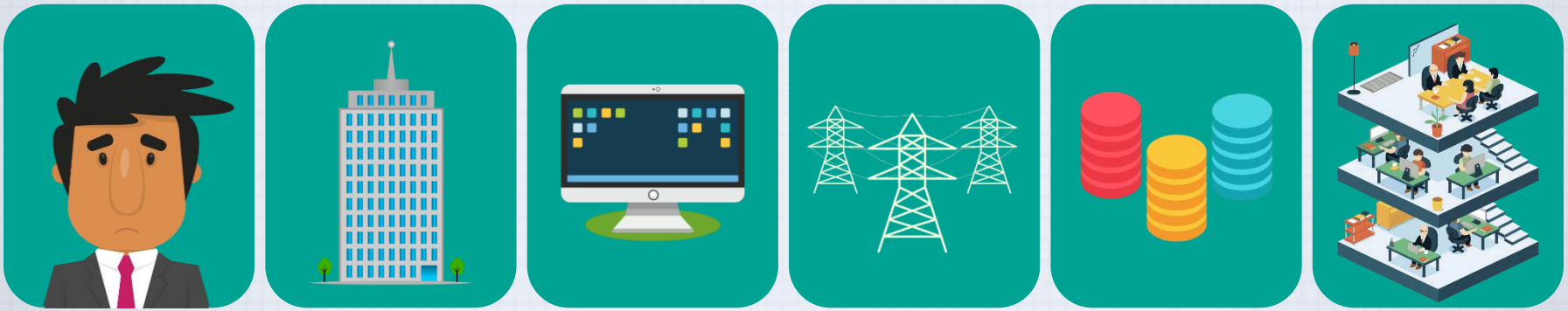
- Porque serão definidos os critérios para avaliar os impactos potenciais de incidentes.
- Considerar os requisitos legais.
- Priorização e custos dos controles.
- Tratamento dos riscos.

Conceito de Análise de Impacto no Negócio – BIA

Elementos cruciais para uma BIA, conforme a ISO 22301, são:

- Avaliação de impacto;
- Avaliação do Objetivo de Ponto de Recuperação (*RPO - Recovery Point Objective*) ou a perda máxima de dados;
- Objetivos Mínimos de Continuidade de Negócios (*MBCO - Minimum Business Continuity Objectives*);
- Recursos necessários;
- Dependência de outros.

O conceito de impacto de negócio é amplo, pois engloba diferentes tipos de impactos:



Conceito de Análise de Impacto no Negócio – BIA

- Desenvolveu uma metodologia de análise de impacto do negócio;
- Realizou a análise de impacto do negócio;
- Determinou o tempo de recuperação;
  - Interrupção Máxima Aceitável (*MAO - Maximum Acceptable Outage*)
  - Objetivo de Tempo de Recuperação (*RTO - Recovery Time Objective*)
- Determinou o tempo de backup;
  - Objetivo do ponto de recuperação (*RPO*) / perda máxima de dados
- As informações foram coletadas de pessoas responsáveis pelas atividades;
- Foi definido o papel-chave para o coordenador da continuidade do negócio ....

NÃO OBRIGATÓRIOS

- Estratégia de continuidade de negócios.
- Questionários da BIA ou os resultados de ferramentas de estratégia de continuidade do negócio.

Objetivos da BIA

- Obter uma compreensão dos principais produtos e serviços da organização e das atividades que os fornecem;
- Determinar prioridades e prazos para a retomada após uma interrupção;
- Determinar os prazos adequados que a retomada deve ser alcançada para manter a capacidade da organização de atingir seus objetivos operacionais;
- Identificar os principais recursos que provavelmente serão necessários para a recuperação;
- Identificar dependências, tanto internas quanto externas, para atingir os objetivos operacionais da organização.

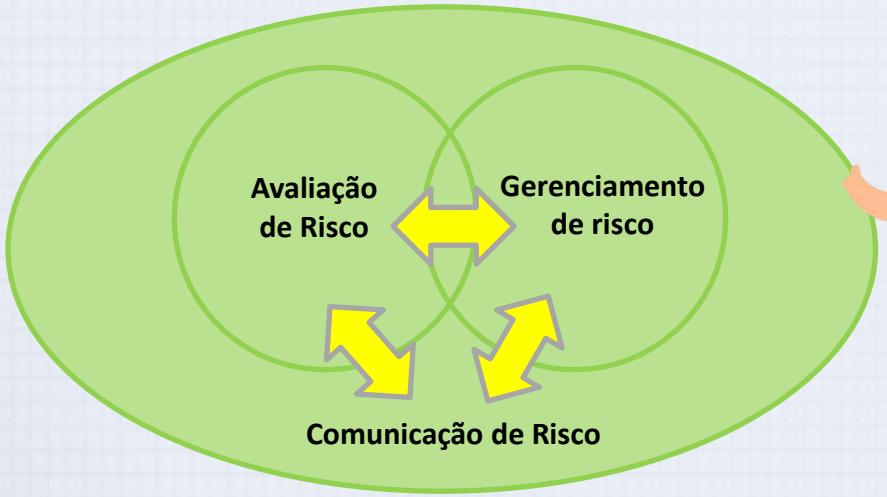
Objetivos da BIA

- "período máximo tolerável de interrupção"
- "período máximo tolerável"
- "interrupção máxima aceitável"

Conceitos de Avaliação de Riscos – RA

É um processo sistemático que tem o objetivo de ajudar a encontrar todos os tipos possíveis de interrupção que possam afetar as operações da organização.

1. **Desenvolveu uma metodologia de Gerenciamento de Riscos.**
2. **Executou de fato a avaliação de risco.**
3. **Realizou o tratamento ou a mitigação de risco.**



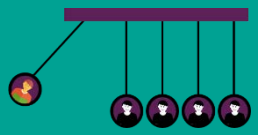
Conceitos de Avaliação de Riscos – RA

Ativos

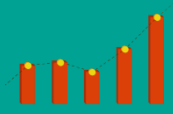
Ameaças

Vulnerabilidades

Impacto / consequência



Probabilidade em termos estatístico



Risco

ISO 22301:2012

- metodologia de avaliação de risco
- planilha de avaliação de risco
- relatório de tratamento de risco

Objetivos da RA

ISO 31010

"A avaliação de risco é aquela parte da gestão de risco que fornece um processo estruturado, que identifica como os objetivos podem ser afetados e analisa o risco em termos de consequências e suas probabilidades antes de decidir se é necessário um tratamento adicional".

Qual é a probabilidade de sua ocorrência futura e se existem fatores que atenuem a consequência do risco ou que reduzam a sua probabilidade.

Por que eles acontecem

o que pode acontecer com tais riscos

Quais seriam as consequências

Objetivos da RA

PROCESSO DE RA

ISO 31000

Princípios e diretrizes do gerenciamento de riscos.

- **Os critérios de aceitação de risco e em quais circunstâncias a empresa está disposta a aceitá-los;**
- **Níveis aceitáveis de risco.**
- **Análise dos riscos.**

✓ As ameaças específicas podem ser descritas como eventos ou ações que poderiam em algum momento, causar um impacto nos recursos.

- Vulnerabilidades podem ocorrer como pontos fracos dentro dos recursos e, em algum momento, podem ser explorados pelas ameaças.

Metodologia de Gerenciamento de Riscos

ISO 31000

GESTÃO DE RISCO

Consiste na avaliação e no tratamento do risco.

Implementar as proteções e controles e realizar revisões...

Opções de mitigação;

Avaliação de riscos;

Desenvolvimento de uma metodologia;

Descobrir quais problemas você pode enfrentar, ou seja, quais incidentes perturbadores podem acontecer com sua organização e em seguida, preveni-los e/ou se preparar para minimizar o dano de tais incidentes.

Metodologia de Gerenciamento de Riscos

Conteúdo da metodologia

Documento da metodologia

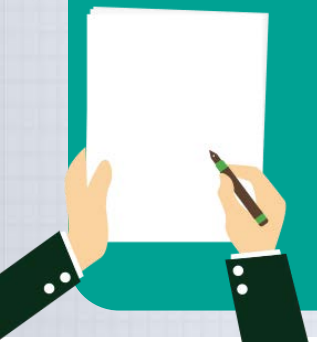
- O processo de avaliação de risco;
- Identificação de risco baseada em atividades ou baseadas em ativos;
- Avaliando apenas ameaças ou também vulnerabilidades;
- Como o nível de risco é determinado;
- Escalas de avaliação;
- Método de cálculo de risco;
- Como a decisão sobre tratamento de risco é feita;
- Quais ferramentas usar.

Metodologia de Gerenciamento de Riscos

METODOLOGIA DOCUMENTADA

- O tratamento de risco;
- Responsabilidades e documentação;
- As leis e regulamentos;
- Requisitos contratuais relacionados ao seu gerenciamento de risco e o período de revisão.

Descrever claramente as funções em todo o processo	Quais documentos precisam ser produzidos	Quem precisa comunicar quais informações	Para quem	Quais relatórios são necessários	Como proteger a confidencialidade das informações
					



Estratégias e Procedimentos

"Durante o desenvolvimento da estratégia você tem que decidir os tempos de recuperação (RTOs) para cada atividade, mas também precisa descobrir como garantir que todos os recursos necessários, como pessoas, dados, hardware, instalações, etc. estarão disponíveis em caso de desastre.".

Vai exigir a criação de procedimentos.

- **Procedimentos de continuidade do negócio.**
- **Procedimentos de resposta e recuperação de incidentes**
- **Procedimentos de compra de emergência.**
- **Plano de continuidade de negócios.**
- **Plano de gerenciamento e comunicação de crises.**
- **Plano de resposta ao incidente.**
- **Plano de recuperação .**
- **Plano de restauração.**

Estratégias e Procedimentos

“Um documento ou um conjunto de documentos que descreve o que você fará, do ponto em que suas operações são interrompidas e os recursos danificados e/ou desativados, até o ponto em que você pode reiniciar suas operações e voltar ao negócio como de costume".

Seleção das Estratégias

RA

BIA

Baseada nos resultados da..

Reduzir o impacto das interrupções, reduzir o período de interrupção e reduzir sua intensidade para níveis aceitáveis.

Analise a possibilidade de proteger as atividades que são mais prioritárias na empresa.

- **Avaliar as vulnerabilidades;**
- **Custo das medidas em relação aos benefícios estimados;**
- **A urgência da atividade e a viabilidade geral.**

Seleção das Estratégias

Se a decisão estiver na estabilização, continuação, retomada e recuperação das atividades...

- Uma mudança de atividade, ou seja, transferir algumas, ou todas as atividades para outra parte da organização, ou externamente, para um terceiro.
- Reencaminhar os recursos, incluindo o pessoal.
- Estabelecer um processo alternativo.
- Recuperar os recursos e habilidades.
- Aplicar uma solução temporária.

- **Se a opção não é retomar e nem proteger as atividades, pense na possibilidade então de mitigar, responder e gerir os impactos.**
- Seguro, que pode fornecer algumas recompensas financeiras por algumas perdas;
- Restauração de ativos através da contratação de serviços de empresas que se especializam na reparação de ativos após o seu dano.

Requisitos de Recursos

Equipes apropriadas...

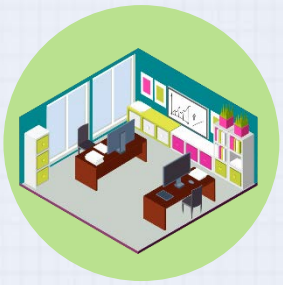
... ou indivíduos com autoridade suficiente...

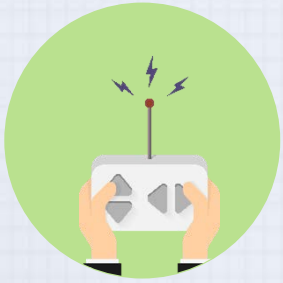
... para supervisionar a preparação...

...resposta e recuperação de incidentes...

Recursos e procedimentos que assegurem que as decisões possam ser rápidas e que estejam de acordo com os níveis estabelecidos de autoridade e governança.




Recursos para Implementar as Estratégias

Pessoas

Informação e dados

Edifícios, ambiente de trabalho e utilitários associados

Instalações, equipamentos e consumíveis

Parceiros e fornecedores

Finanças

Transporte

Sistemas de TI e comunicações

Identificação de Riscos, Ameaças, Vulnerabilidades e Níveis

1 **Decidir sobre a identificação de riscos de incidentes:**

Baseada nas atividades

É mais rápida, porque cada atividade pode ter centenas de ativos.

Baseada nos ativos

2 **Decidir se será avaliado apenas as ameaças ou vulnerabilidades também.**

Ameaças é o que poderia potencialmente acontecer ou prejudicar a sua atividade ou ativo

A vulnerabilidade é uma característica de sua atividade ou ativo que poderia ser explorada por uma ameaça.

Identificação de Riscos, Ameaças, Vulnerabilidades e Níveis

3 Deve ser decidido o nível de risco.

Escala de 1 a 5

1. muito baixo
2. baixo
3. médio
4. alto
5. muito alto

Sobre qual escala de avaliação usar.

Avaliar consequências e probabilidades

- A probabilidade de incêndio é baixa (2)
- As consequências seriam muito altas (5)
- Como resultado, o nível de risco seria calculado através das consequências e probabilidades.

- Baixa-média-alta.
- O risco é aceitável: Sim / Não?

Calculando o Risco e Medições

Metodologia de gerenciamento de riscos.

Consequências ✖ **Probabilidade**

2 + 5 = 7

2 x 5 = 10

Baixa-média-alta → **escala 1-2-3**

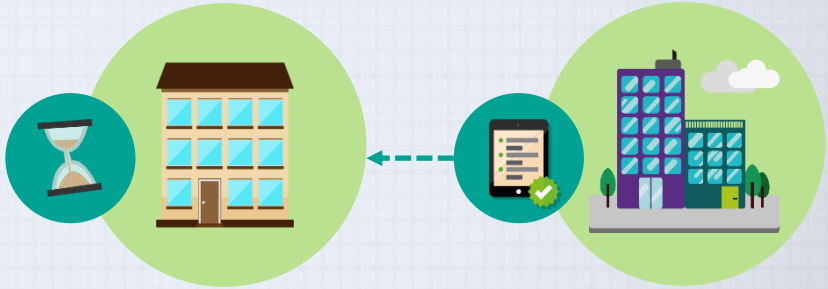
Isso significaria que apenas os riscos dos valores 8, 9 e 10 precisam de tratamento.

Examinar cada risco individualmente e decidir quais devem ser tratados ou não, com base em sua visão e experiência, sem usar valores pré-definidos.

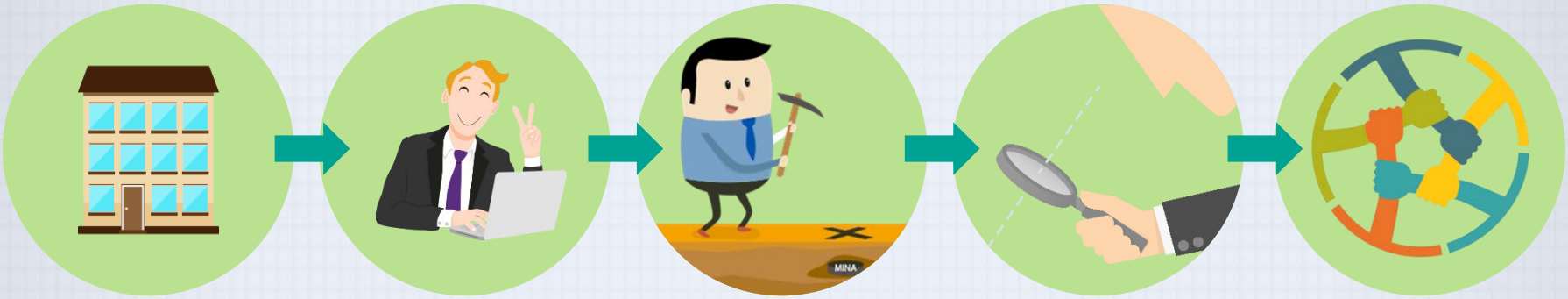
Medição.

Medir se seu processo de gerenciamento de risco é efetivo, avaliando se as salvaguardas e se outras opções de tratamento produziram resultados desejáveis;

Uso de ferramentas de avaliação de risco.

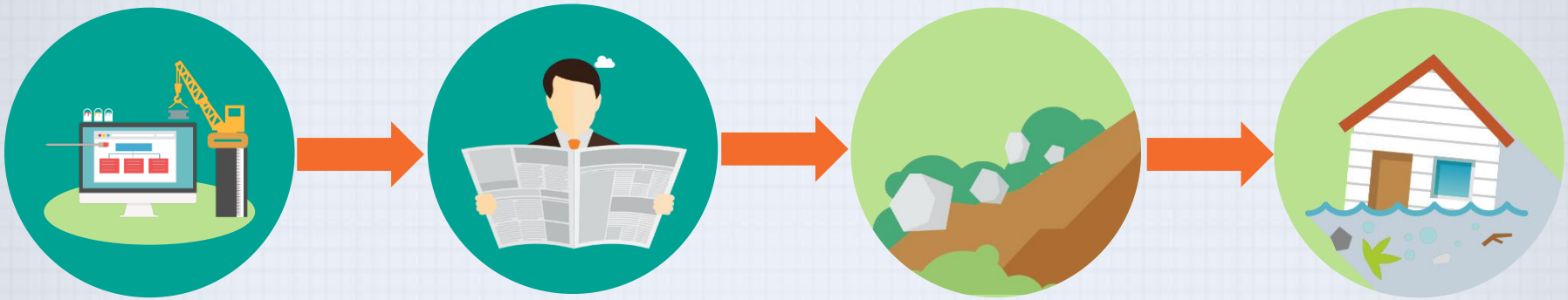


Executando a Avaliação de Riscos



Descubra que ferramentas e atividades são fundamentais para cada departamento para que continuem seu trabalho.

Caso de uma Avaliação de Riscos



Risco alto

- Fiação elétrica antiga e propensa a falhas e curto-circuito;
- Dependência de um único fornecedor para equipamentos importantes de hardware.

Risco médio

- Arquivo em papel em caixas de material inflamável e sem alarme de incêndio;
- A sede da empresa se localiza em uma área propensa a alagamentos.

Risco baixo

- Surgimento rápido de novas tecnologias na área, mudando a dinâmica da empresa e as demandas dos clientes.

Caso de uma Avaliação de Riscos

RISCO BAIXO, porque é exatamente com estas tecnologias que esta empresa trabalha.

RISCO MÉDIO, porque os dados arquivados naquela caixa são antigos, e a perda deles não acarretaria grandes prejuízos.

RISCO MÉDIO, porque pode estragar os equipamentos da empresa, mas não é de todo complexo impedir que um alagamento cause grandes danos na empresa.

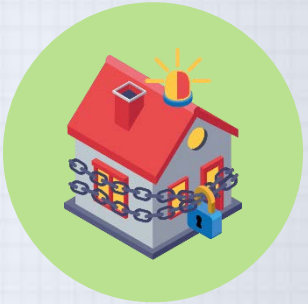
RISCO ALTO, porque qualquer curto-circuito pode ser o estopim para um grande incêndio, que poderia destruir diversas máquinas, arquivos e até mesmo matar funcionários asfixiados

RISCO ALTO, ela precisa ter em mãos o equipamento certo para continuar funcionando, e se seu fornecedor não puder atendê-lo de imediato após um incidente, a sua empresa será imensamente prejudicada.

Realizando o Tratamento e Mitigação de Risco

- Riscos que podem ser diminuídos através do tratamento das vulnerabilidades.
- Foque naqueles que não são de maneira alguma aceitáveis.

- **Dividir a responsabilidade do risco, através da contratação de uma empresa de seguros**



- **Plano de ação bem detalhado**

Brainstorm

Realizando o Tratamento e Mitigação de Risco

“PENSAR FORA DA CAIXA”

FASE DE TOMADA DE DECISÕES

É fundamental que seja dada vez e voz a todos os departamentos e, com a escolha de representantes e porta-vozes, todos os funcionários. Além do mais, ao contar com mais pontos de vista distintos durante um *brainstorm,* é possível chegar a soluções mais criativas, úteis e até mesmo mais econômicas.

Caso de um Tratamento de Riscos

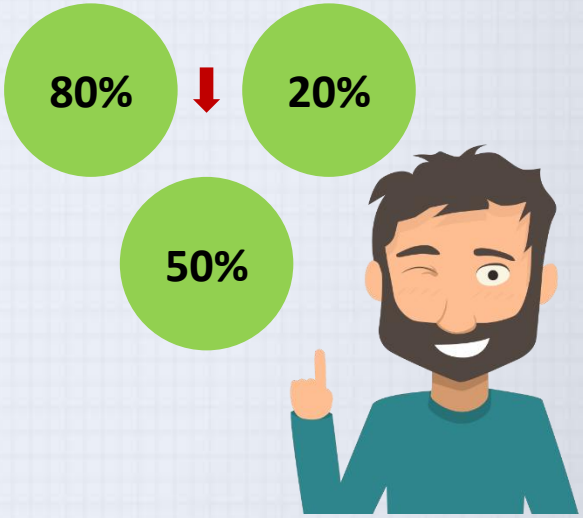
A fiação elétrica será trocada. É um gasto grande, mas a obra precisa ser feita.

Alguns orçamentos serão pedidos para que a empresa contrate mais fornecedores.

A empresa decidiu dividir o risco com a nova seguradora, que vai instalar modernos alarmes de incêndio monitorados durante 24 horas.

A empresa dividirá o risco de alagamento na temporada de chuvas com a nova seguradora, através de um plano especial contra alagamentos.

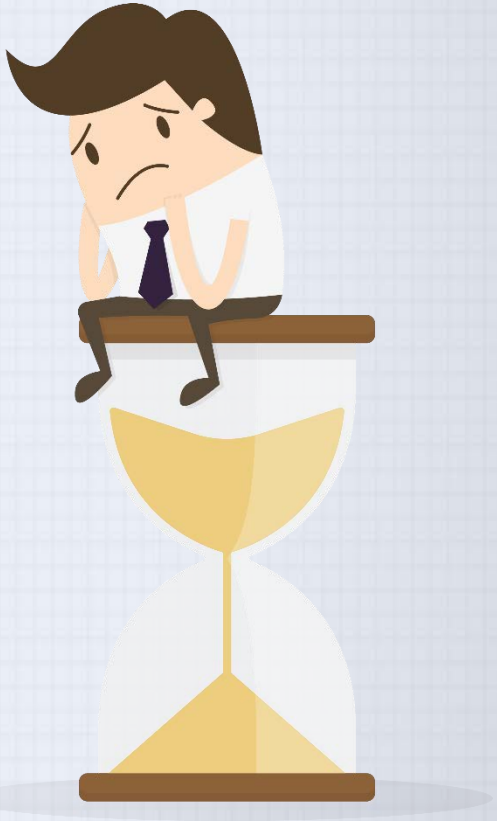
Parte do orçamento será investida em cursos de capacitação mais frequentes para os funcionários.



Desenvolvendo a Metodologia da BIA

Cada área tem um tempo de recuperação diferente. → **Cada departamento pode perder uma quantidade de dados ou informações sem que isso interfira no serviço de tal maneira que ele se torne impossível de executar.**

Mesclar métodos QUANTITATIVOS e QUALITATIVOS.



Como que um incidente impacta a percepção da nossa empresa junto aos clientes?

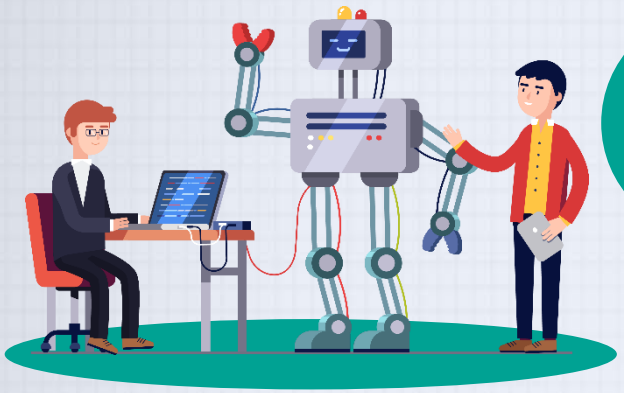
Como a paralisação de determinado setor impacta a percepção da nossa empresa junto aos clientes?

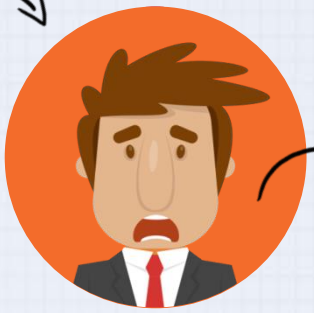
Em quanto tempo determinado setor poderá voltar a funcionar no seu ritmo normal?

Qual será o custo do incidente – considerando possíveis reformas e indenizações – para cada departamento?

Qual será o impacto do incidente nos lucros de cada área da empresa?

Caso de um Desenvolvendo da Metodologia da BIA





O tempo de recuperação dos equipamentos deve ser de alguns minutos ou horas apenas, e quanto mais rápido, melhor.

EX.: dos maiores clientes ou os trabalhos com data de entrega mais próxima – para que a própria reputação da empresa não seja prejudicada.

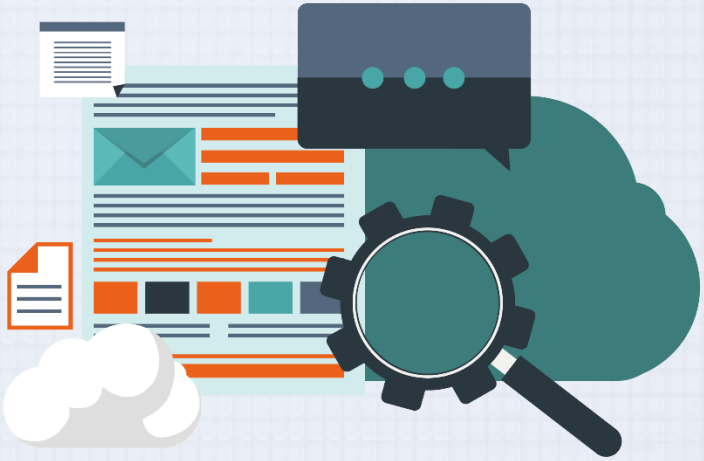
São eles que devem aprovar o plano, e conferir se os gastos e períodos previstos são realistas.

Submeta-se ao CEO ou à gerência:

Executando a BIA

- Ao estar preparado para o pior cenário possível, se acontecer um cenário mediano de danos, você também estará preparado.

Todo o planejamento deve ser feito tendo em mente que a perda de dados é mais prejudicial ao seu negócio do que a perda de equipamentos.



Executando a BIA

- Estabeleça um intervalo de tempo padrão entre os backups, sem margem para atrasos.
- É fundamental ter documentado quando o último backup foi feito para saber, em caso de um incidente, que arquivos e documentos foram perdidos.
- É o momento de analisar os serviços dos quais a empresa depende, e como eles podem ajudar após um incidente.
- É hora de perceber quais setores são interdependentes e quais fornecedores ou provedores são essenciais para que seu trabalho continue.
- Um bom momento para descobrir se seus parceiros têm também uma política de continuidade dos negócios, ou se certificaram nas normas ISOs 9001 ou 27001.

Caso de uma Execução da BIA

A estratégia foi sair para o mercado em busca de novos fornecedores e fazer diversas simulações e orçamentos, a curto e longo prazo, para escolher pelo menos dois novos fornecedores.

Outras empresas entraram na competição pela parceria, mas ao final ficou decidido que a multinacional e a startup seriam os novos fornecedores – provando que, mudanças no cenário administrativo podem ser muitas vezes bem-vindas.

Planos e Procedimentos de Continuidade de Negócios

- Plano de resposta ao incidente.
- Plano de recuperação de desastres (DRP).
- Plano de recuperação das atividades.
- Plano de restauração.

ISO 22301:2012

Documentação obrigatória.

Estratégia de continuidade do negócio

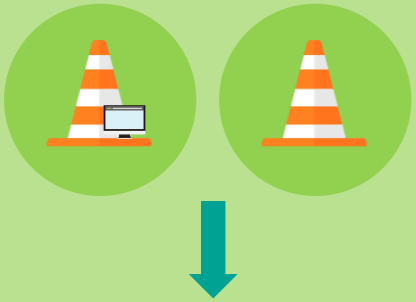
Resultados da avaliação de risco

- Plano de Continuidade de Negócios;
- Procedimentos de resposta ao incidente;
- Procedimento de incidente de segurança;
- Procedimento de ação corretiva;
- Procedimento para resposta à mídia durante um incidente;
- Procedimento de revisão de incidente;
- Procedimentos de emergência e evacuação de incêndio;
- Procedimentos do fornecedor;
- Procedimentos de compra de emergência e muitos outros.

Planos e Procedimentos de Continuidade de Negócios

Processos de Resposta ao Incidente

- **Estes procedimentos devem estar em vigor...;**
- **Indicando quem é responsável;**
- **E quais ações precisam ser acionadas.**



Minimize o impacto de um incidente e lembre-se, o plano de resposta a incidentes é obrigatório.

Ative a resposta correta de continuidade do negócio, durante o incidente;

Comunique-se com as partes interessadas;

Desenvolvendo a Estratégia de Continuidade de Negócio

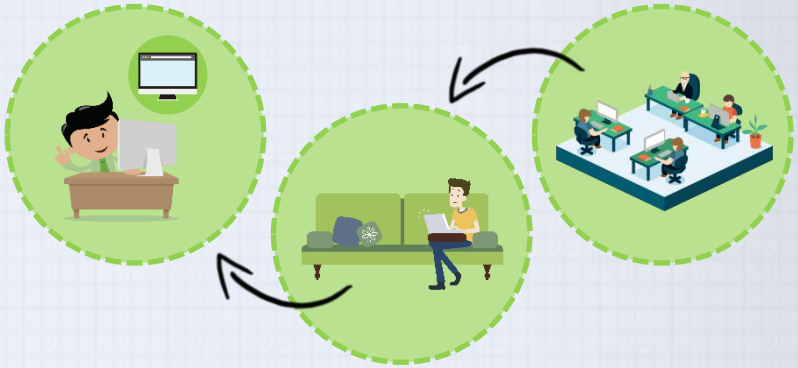
Algum funcionário que é de extrema importância em um departamento tem um substituto caso precise se ausentar?

Eles serão substituídos temporariamente por um pessoal que tem costume de trabalhar sob pressão?

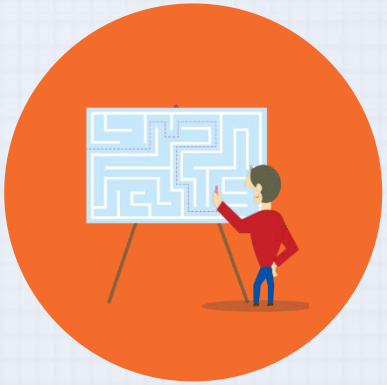
Quanto aos seus colaboradores, eles serão treinados para outras funções em caso de um incidente?

Seu plano é realista o suficiente?

Ou será que ele acaba criado uma espécie de estado de pânico dentro da sua organização?



Considere antecipadamente que a recuperação talvez tenha que ser feita longe do local afetado da empresa.



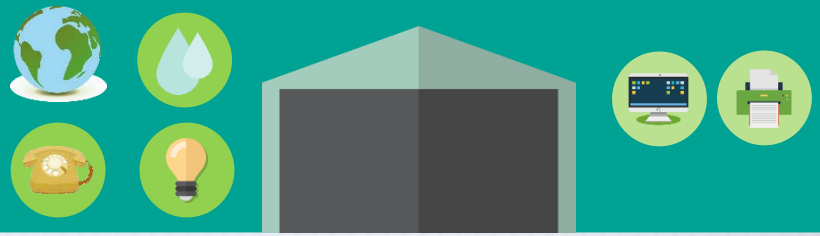
Caso de um Desenvolvimento da Estratégia de Continuidade de Negócio

Os colaboradores continuariam trabalhando em regime *home office* enquanto durar a recuperação total de seu departamento.

Os colaboradores serão treinados apenas para reagir ao incidente, com lições de primeiros socorros e segurança no trabalho.

As atividades voltarão a ser executadas na matriz onde ocorreu o incidente após uma perícia dos bombeiros, que determinará se todo o incidente foi controlado e se mais riscos não foram criados.

O galpão foi alugado para ser usado pela gerência em caso de incidente. O local foi equipado com conexão à internet, água, luz, telefone, sete computadores e duas impressoras / copiadoras.



Cenários de Interrupção

CENÁRIOS

- Pequenas narrativas hipotéticas;
- Que podem ser bem curtas;
- Mas mostrem com exatidão os riscos que a empresa.

Neste momento vários membros da equipe podem dar *feedback* sobre situações semelhantes de incidentes que eles já conheceram, ou já presenciaram, e em uma pesquisa pode também verificar o que acontece de fato em uma empresa que passa pelo incidente que está sendo narrado.

"A imaginação é mais importante que o conhecimento"

Cenários de Interrupção

Comece pela lista dos maiores riscos à sua empresa...

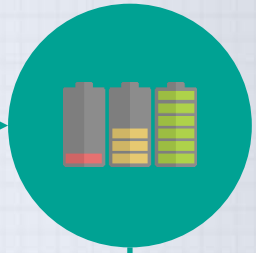
Para uma empresa pequena, criar cenários para os cinco maiores riscos já será o suficiente.

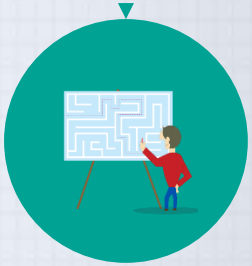
- **Impacto financeiro e psicológico nos funcionários;**
- **Impacto na matriz e nos sistemas da organização;**
- **Impacto nos arredores da empresa.**

A equipe responsável pelo SGCN pode criar estes cenários sem precisar de ajuda de um consultor externo. Alguns poucos parágrafos, que vão direto ao ponto, são suficientes.

Plano de Continuidade de Negócio

Contempla os procedimentos de resposta a um incidente.





Com a finalidade de responder a um incidente e lidar de forma adequada com a retomada e recuperação das atividades da empresa.

- finalidade
- o escopo
- os objetivos e medidas de sucesso
- os critérios e procedimentos de ativação do plano
- os procedimentos de implementação
- as funções, responsabilidades e autoridades
- requisitos e procedimentos de comunicação
- as interdependências e interações internas e externas
- requisitos de recursos
- os fluxos de processos de informações e documentação.

Plano de Continuidade de Negócio

AÇÕES

- Respostas e avaliação do incidente;
- Ser avaliado o que e como aconteceu;
- Quais partes interessadas foram ou poderiam ter sido afetadas;
- Qual a duração prevista do incidente;
- Seus impactos e se o incidente pode ser gerenciado através dos processos de gerenciamento tradicionais e rotineiros.

AÇÕES

- Avaliação do incidente;
- Procedimento de ativação;
- Ações para mobilizar o pessoal;
- Ações para priorizar as atividades;
- Ativar sites alternativos para restauração da TI;
- A forma como será monitorado o incidente;
- Um processo de escalação;
- Como identificar oportunidades de aprendizagem;
- Como assegurar uma boa governança.

Conteúdo de um Plano de Continuidade de Negócios

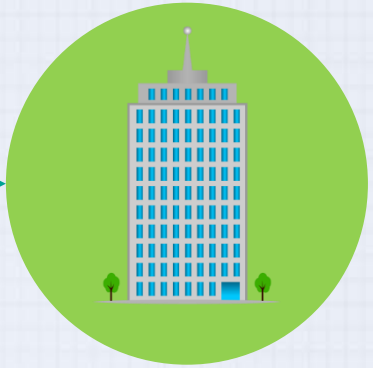
- **CONTROLES DO DOCUMENTO;**

- **PAPÉIS E RESPONSABILIDADES CONTENDO:**
  - Funções e responsabilidades definidas para as pessoas que usarão os procedimentos de resposta durante e após um incidente;
  - Diretrizes e critérios de quais pessoas têm autoridade para ativar os procedimentos e em quais circunstâncias.

- **ATIVAÇÃO (INVOCAÇÃO) E SUSPENSÃO DO PLANO. OU SEJA, CADA PROCEDIMENTO DE RESPOSTA DEVE CONTER:**
  - Um método para ativá-lo dentro ou fora do horário comercial;
  - Um meio formal de alertar a equipe de intervenção;
  - Conforme apropriado, identificar os locais de reunião alternativos.

Conteúdo de um Plano de Continuidade de Negócios

Pode ter um único procedimento documentado, com todos os requisitos e que cubra suas operações inteiras.



Pode ter muitos procedimentos documentados, cada um com um propósito definido.

OBJETIVO

ESCOPO

Devem ser objetivos

Acordados pela alta administração

Entendidos por aqueles que o implementarão.

Qualquer relação com outros procedimentos ou documentos de continuidade de negócios relevantes dentro da organização deve ser claramente referenciada e o método de obtenção e acesso a estes documentos devem ser descritos.

Conteúdo de um Plano de Continuidade de Negócios

- **GERENCIAMENTO DE INCIDENTES COM PROCEDIMENTOS DE RESPOSTA INCLUINDO:**
  - Detalhes das ações e tarefas que precisam ser realizadas;
  - Quando apropriado, incluir questões do bem-estar do pessoal afetado e o bem-estar dos membros da equipe;
  - Uma abordagem dos problemas em um nível apropriado, ou seja, nos níveis estratégicos, táticos ou operacionais. As questões que estão em outros níveis devem ser escaladas ou delegadas a outras equipes conforme necessário;
  - Métodos para registrar informações importantes sobre o incidente, além das ações e decisões tomadas.

- **INFORMAÇÕES DE CONTATO CONTENDO:**
  - Procedimento de resposta com detalhes de contato das partes interessadas pertinentes. Estes detalhes de contato devem ser mantidos em relação às leis locais de proteção de dados;
  - Procedimentos de continuidade de negócio com detalhes de contato e mobilização de organizações e recursos, assim como a polícia, bombeiros, segurança, serviços de saúde, etc...
  - Comunicação e todos os procedimentos de continuidade do negócio abordando a comunicação com outras equipes.

Procedimentos de Continuidade de Negócios

ESPECÍFICO - no que se refere às medidas imediatas que devem ser tomadas durante uma interrupção;

1

FLEXÍVEL - para que eles possam ser usados para responder em cenários com ameaças imprevistas e mudanças nas condições internas e externas;

2

FOCADO - devem se relacionar claramente com o impacto de eventos que poderiam potencialmente interromper operações e desenvolver com base em premissas declaradas e uma análise de interdependências;

3

EFETIVO - em termos de minimizar as consequências de incidentes, através da implementação de estratégia de mitigação adequada.

4

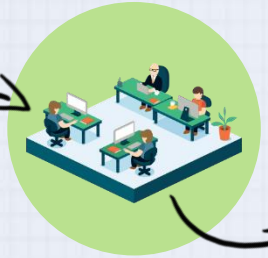
Local para o Gerenciamento de Incidentes

Procedimento de Gerenciamento de Incidentes

ISO 22301:2012

Permitir que a alta administração da organização tenha um controle durante a fase inicial de um incidente, enquanto sua reputação está mais suscetível de ser ameaçada.

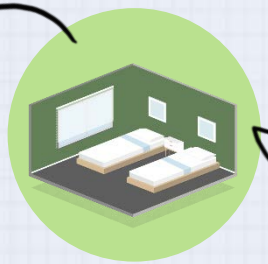
Base



Deve ser o **PONTO FOCAL** para a resposta da organização.

Um **ponto de encontro alternativo** em um local diferente também deve ser indicado, no caso do acesso à localização principal ser negado.

Deve ter **acesso aos recursos apropriados**, pelos quais a equipe de gerenciamento de incidentes pode iniciar suas atividades efetivas.



"centro de comando" dedicado.

Deve ser adequado e incluir um espaço adequado para o número necessário de pessoas, meios de comunicação eficaz e instalações para acessar e compartilhar informações.

Estrutura de Resposta a Incidentes

A estrutura de resposta deve providenciar:

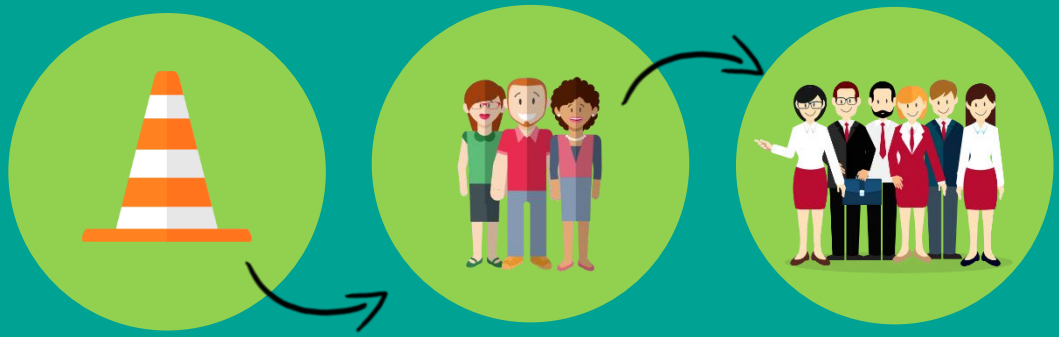
- A identificação de limites de impacto que justifiquem o início de uma resposta formal.
- Avaliação da natureza e a extensão de um incidente ou o impacto potencial;
- Implementação de medidas para assegurar o bem-estar dos afetados;
- Iniciação de uma resposta adequada à continuidade do negócio;
- Processos e procedimentos para a ativação, operação, coordenação e comunicação da resposta;
- Recursos para apoiar os processos e procedimentos necessários para gerenciar um incidente ou trabalhar para minimizar o impacto;
- Comunicação com as partes interessadas, nomeando as autoridades e os meios de comunicação.

1. Ter um ou mais colaboradores competentes disponíveis para avaliar o impacto potencial do incidente e o tempo disponível para isso;
2. Ser capaz de mobilizar as equipes para assumir o controle, conter o incidente e iniciar a resposta adequada da continuidade do negócio;
3. Incluir recursos adequados que podem incluir pessoal, empreiteiros, equipamentos e os recursos financeiros.

Estrutura de Resposta a Incidentes

Organizações maiores ou mais complexas

Abordagem em camadas

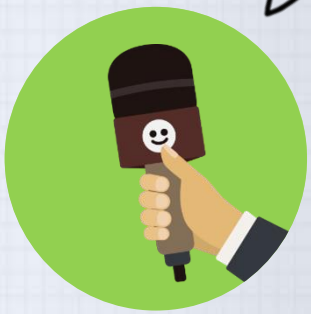


Organizações menores.

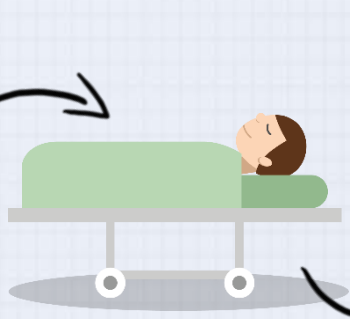
- Nunca devem ser responsabilizados por uma única pessoa.
- Cada equipe deve ter procedimentos para gerenciar um episódio de acordo com suas responsabilidades.

Comunicando o Incidente

Rádios de curto e médio alcance.



Pode ser útil ter diversos modelos de discursos pré-concebidos, com apenas alguns dados para serem preenchidos na hora de fazer o comunicado.



já deve ter sido escolhido seu substituto para se comunicar com a mídia.

Gerenciamento de Crises e Comunicação

- comunicação
- marketing

1. Escolher quais informações serão compartilhadas.

Não são compartilhadas as mesmas informações com pessoas de dentro, com as de fora da empresa.

COLABORADORES E PARCEIROS

ACIONISTAS E O PÚBLICO EM GERAL

Para nenhum deles devem ser divulgadas mentiras, mas fazer uma seleção e triagem das informações é fundamental.

Gerenciamento de Crises e Comunicação

Não é necessário que o gerente de crise seja também, o porta-voz da empresa.

Ele precisa ter visão ampla e holística do funcionamento da organização

Profissionais das ciências atuariais ou que já tenham experiência comprovada na redução de efeitos de incidentes diversos.

E ser capaz de tomar boas decisões rapidamente e principalmente, sob pressão.

- Quanto **maior** a empresa, maior deverá ser o time de gerenciamento de crise.
- Mesmo numa empresa **pequena**, o ideal é que não haja uma sobrecarga de responsabilidades em um único gerente.

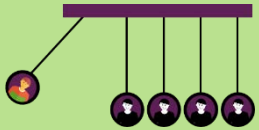
Plano de Resposta ao Incidente

A resposta rápida após o incidente pode significar a diferença entre o reerguimento da empresa ou seu fechamento definitivo.

Reestruturação ✗

Controle do incidente

Da diminuição do impacto



E da eliminação do risco

SEGURANÇA NO TRABALHO

- Crie uma lista para cada possível risco que você e sua equipe já identificaram;
- Escreva as medidas que serão tomadas após eles acontecerem;
- Qual membro da equipe irá ficar responsável por qual ação;
- Frise a importância de deixar tudo documentado.

“como” **“quando”** **“onde”** **“quem”**

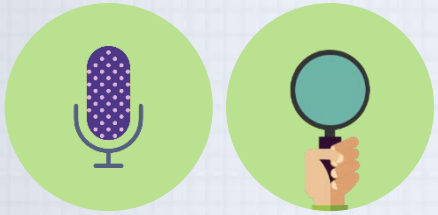
Plano de Resposta ao Incidente

- Verifique também se todos os passos da reação estão sendo seguidos.

- Descreva nos documentos os meios de comunicação que serão usados em cada etapa da reação e tire vantagem da existência deles.

Procedimento de Resposta a Incidentes

ISO 27035 → **Técnicas de Segurança Informação**



Ativação de procedimentos de continuidade de negócios e comunicação com as partes interessadas.

- **Planejamento**
- **Detecção / Reporte de Eventos**
- **Declaração do Incidente**
- **Resposta e Recuperação do Incidente**
- **Pós-Incidente**

Continuamente

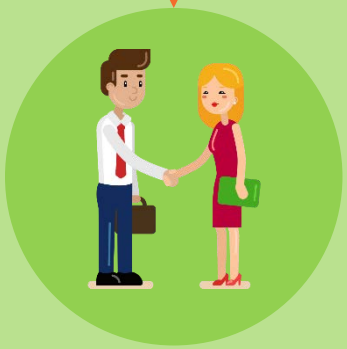
Essa comunicação deve ser regular e feita com a equipe interna e outras partes interessadas, sempre tomando o cuidado de selecionar as informações que serão comunicadas com visitantes e contratados.

Os procedimentos de resposta a incidentes devem ser estabelecidos antes que o evento ocorra, jamais deixe para definir uma resposta no momento que o mesmo está ocorrendo.

Procedimento de Resposta a Incidentes

Comunicação bidirecional

Procedimentos que facilitem a...



parceiros

partes interessadas

A organização deve manter as comunicações com essas partes até o retorno à normalidade das operações de negócio, ou seja, até que o incidente seja extinto.

Caso de um Plano de Resposta ao Incidente

Para os riscos de incêndio e problemas com fiação elétrica:

- Avisar os bombeiros logo após ser detectado o fogo;
- Evacuar o pessoal do local afetado da empresa;
- Extinguir o incêndio caso ele seja de pequenas proporções;
- Cuidar dos possíveis feridos ou encaminhá-los a um hospital;
- Fazer um levantamento das perdas;
- Comunicar a mídia e o departamento de Recursos Humanos deve ser acionado imediatamente.

Caso de um Plano de Resposta ao Incidente

Para os incidentes envolvendo um fornecedor:

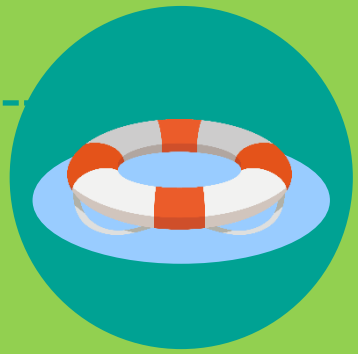
- Verificar a possibilidade de fazer compras rapidamente;
- Se algum trabalho for retardado por causa do incidente:
- Comunique o atraso ao cliente;
- Controle uma possível crise por reclamação online;
- E acelere o trabalho quando possível para que o atraso não se prolongue.

Caso de um Plano de Resposta ao Incidente

Incidente envolvendo arquivos em papel:

- Verificar o que foi perdido e se há um backup eletrônico deles.
- Estimar qual o impacto da perda dos arquivos para o trabalho atual da empresa.
- Avisar a seguradora.

Caso de um Plano de Resposta ao Incidente



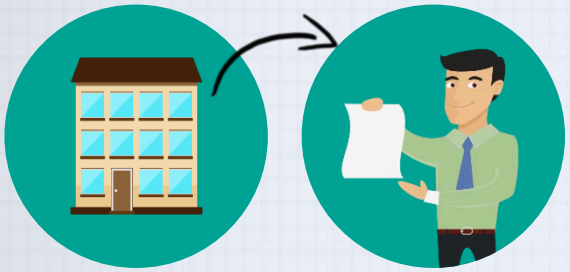
Alagamento:

- Avisar os bombeiros;
- Evacuar a empresa;
- Cuidar dos possíveis feridos ou encaminhá-los a um hospital;
- Fazer levantamento das perdas;
- Comunicar a mídia;
- Departamento de Recursos Humanos deve ser acionado.

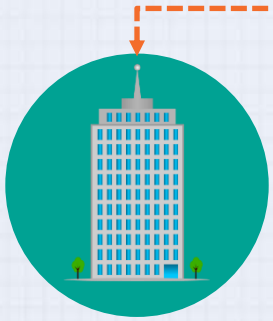
Criando o Plano de Recuperação de Negócios

Estes são os passos para a recuperação completa:

1. **Controlar o incidente quando for possível.**
2. **Verificar os impactos do incidente na empresa de modo objetivo.**
3. **Comunicar à mídia e/ou as partes interessadas.**
4. **Preparar-se para recomeçar.**



- Precisará ter cópias em diversos servidores, na nuvem e em papel, caso a internet não possa ser acessada após o incidente.
- Nem sempre precisam de um consultor externo para redigir tal documento.



Este plano deve ser bem detalhado?

- Se beneficiam de planos detalhados, com divisão clara de trabalho e funções.

Criando o Plano de Recuperação de Negócios

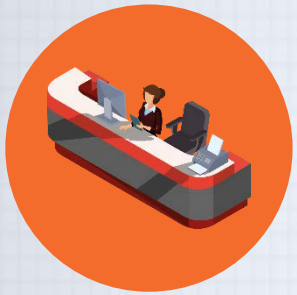
Deve ser detalhado caso haja o risco de o redator do plano não estar próximo quando for hora de executá-lo.

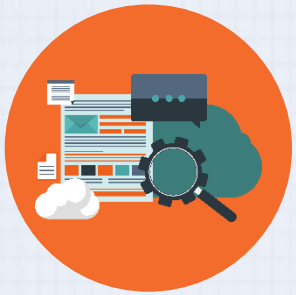
PLANO REALISTA

- Devem ser estabelecidas condições para o funcionamento do plano.
- Pode ser criado mais de um plano por tipo de incidente, dependendo das condições disponíveis.

Plano de Recuperação

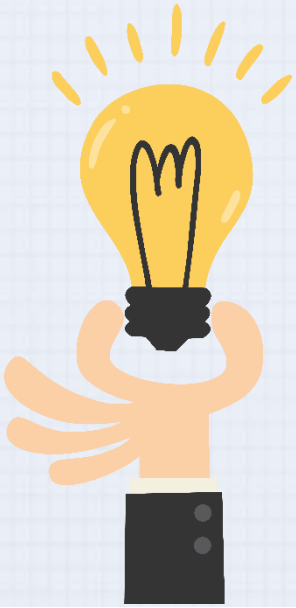
Recuperação dos recursos sem os quais a empresa não funciona.





Plano de recuperação como um anexo do SGCN.

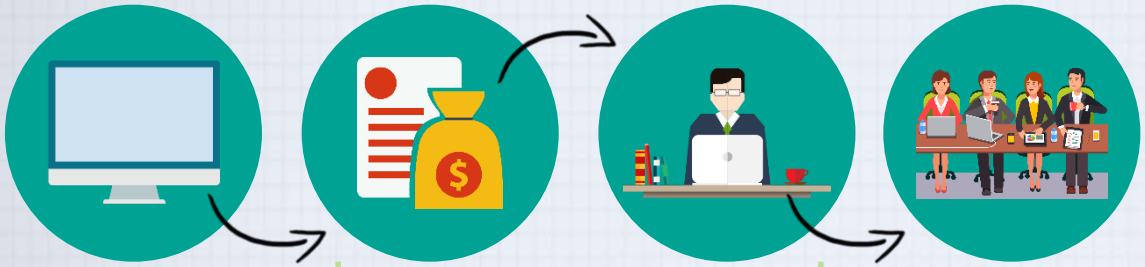
É preciso seguir uma hierarquia, que em geral começa com o setor de TI se restabelecendo.



Plano de Recuperação

- Escreva as tarefas da recuperação em ordem;
- Os números dos telefones úteis;
- Os responsáveis por cada tarefa e, se for possível;
- Fazer a estimativa de quanto cada tarefa deve demorar.
- O endereço da filial ou da sede provisória;
- O meio de transporte que será usado após o incidente;
- A possibilidade ou não de parte da recuperação ser feita via *home office;*
- A checagem de hardware e software;
- A recuperação de dados e produtos;
- E a provável compra de novos equipamentos.

Caso de um Plano de Recuperação



Setor de TI

home office

Se necessário, fará sua recuperação no local provisório.

- Evite uma linguagem técnica.
- Prepare-se para gastar bastante tempo neste documento.

1 **Ficou decidido que o esforço de recuperação começaria assim que o incêndio fosse controlado e todos os funcionários estivessem seguros.**

2 **A verificação da infraestrutura da empresa ocorreria assim que os bombeiros dissipassem toda a fumaça.**

3 **Comunicar as partes interessadas, como os clientes, parceiros e fornecedores. Será feita por e-mail e nas redes sociais. Para a imprensa local, um relações públicas já tem um discurso preparado em caso de incidente.**

4 **A recuperação dos computadores, a ida da gerência para outro local, se necessário, e o início do trabalho dos colaboradores em regime *home office*.**

Plano Específico de Recuperação de Desastres

Criar um PLANO DE RECUPERAÇÃO exclusivo para o setor de TI.

- **Na TI, haver uma descrição minuciosa de todos os passos para se acessar um documento ou prestar suporte é importante.**
- **Não pense que seu maior e mais antigo especialista estará disponível para ajudar na recuperação logo após o incidente.**
- **Descreva tudo de modo que qualquer pessoa possa seguir o passo a passo, mesmo um estagiário, desenvolvedor, analista da central de serviços, etc.**

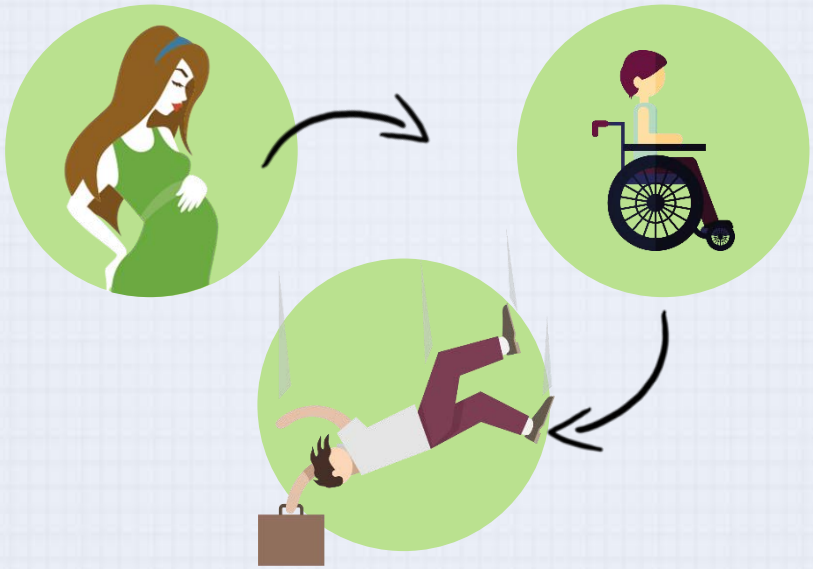
- Faça download de todos os documentos mais importantes.
- Realize *backups* frequentes.

Plano de Bem-Estar

Este plano deve conter tarefas e informações para gerenciar as consequências imediatas de uma interrupção.

Inclui o bem-estar das pessoas, opções estratégicas e operacionais para responder à interrupção.

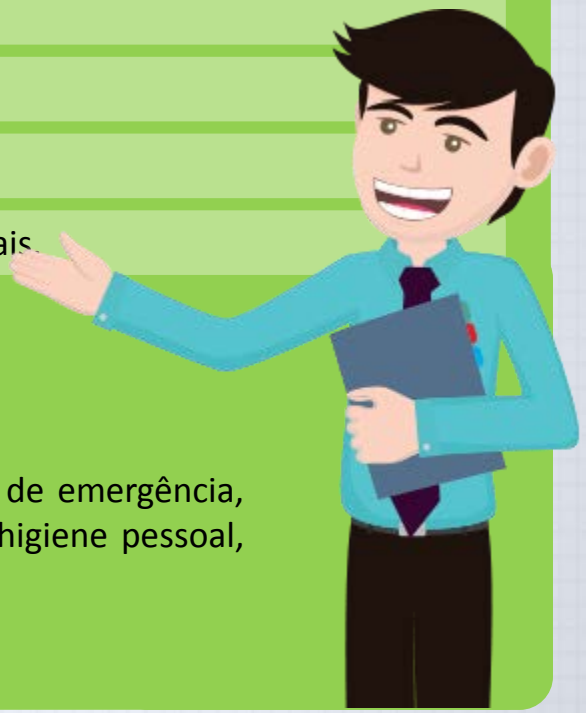
Além de informações sobre prevenção de novas perdas ou indisponibilidade de atividades.



Planejar com antecedência para atender a esses requisitos pode reduzir o risco e tranquilizar os afetados, já que os impactos em longo prazo não podem ser subestimados.

Plano de Bem-Estar

- Procedimento de evacuação do site, incluindo pontos de reunião;
- A mobilização de equipes de segurança, primeiros socorros ou de evacuação;
- Localização e contabilização daqueles que estavam no local ou nas imediações.
- Serviços de tradução;
- Assistência de transporte, incluindo instruções conforme necessário;
- Lista de contato para serviços de emergência;
- Serviços de reabilitação e aconselhamento sejam físicos como os emocionais.



Recursos serão necessários para a resposta ao bem-estar:

- Locais físicos, equipamentos, fontes de energia, produtores de energia de emergência, como os geradores, sistemas de comunicação, comida, suprimento de higiene pessoal, gelo, água, informação técnica, vestuário e abrigo, equipe especializada

Recuperação

Deve ser documentada.

Ajudar a restaurar as operações de negócios

A recuperação começa uma vez que as atividades priorizadas foram retomadas.

Seu principal objetivo é fazer com as operações voltem ao estado que estavam antes do incidente.

- **Reparando os danos resultantes do incidente.**
- **Migrando as operações de instalações temporárias para o local de negócios primários restaurado.**
- **Mudando para um novo local.**

Recuperação

O **PROCEDIMENTO DE RESTAURAÇÃO** deve especificar as atividades priorizadas a serem retomadas, os prazos, os níveis de recuperação necessários para cada atividade.

Recursos necessários:

- Habilidades e qualificações
- Os equipamentos técnicos
- E as instalações de telecomunicações

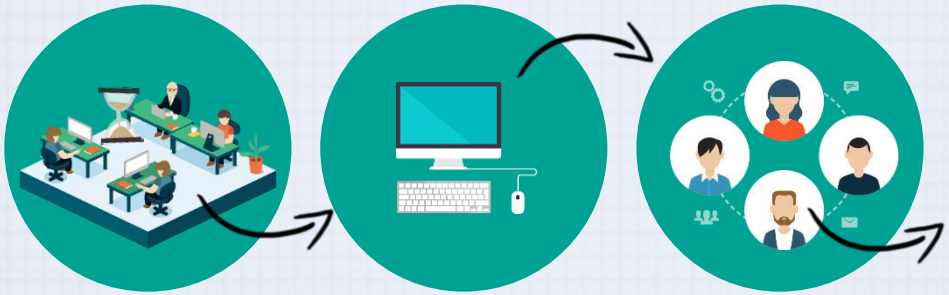
Todos estes requisitos de recursos devem ser documentados e podem incluir:

- Registros impressos e eletrônicos
- Manuais de operação e procedimentos
- Locais das instalações de armazenamento externo
- Planos e procedimentos de recuperação técnica de TI
- Locais alternativos
- Escritórios
- Delegações para pagamento de despesas de emergências
- Lista de funcionários com experiência exigida
- Documentação da infraestrutura de TI e dos aplicativos
- Fonte de suporte de telecomunicações
- E contatos de serviços públicos

Plano de Restauração

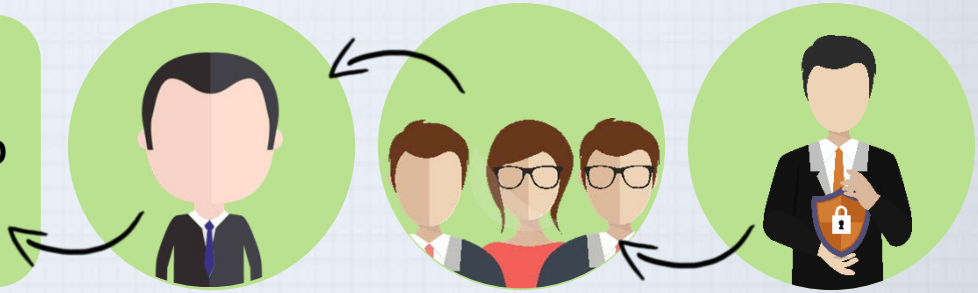
Neste momento, espera-se que o processo de recuperação tenha sido finalizado de forma positiva, pois agora é a hora da restauração.

Agora é hora de planejar os próximos passos até que o negócio volte ao ponto anterior ao incidente, onde tudo funcionava bem.



Aqui, não é preciso descrever detalhadamente o passo a passo, apenas as funções gerais de cada setor e/ou gerente.

Deve preparar este documento e enviá-lo ao CEO para aprovação.



Plano de Restauração

- Migrar operações para instalações de recuperação;
- Recuperar informações documentadas que foram perdidas;
- Comunicar com as partes interessadas relevantes e suas respectivas frequências;
- Normalizar as operações nas instalações restauradas;
- Realizar uma revisão de recuperação;
- Conduzir a devida auditoria e governança corporativa.
- Obter mão de obra adicional para suportar o esforço de recuperação;
- Selecionar opções para restaurar e retornar às empresas;

Caso de um Plano de Restauração

O máximo de permanência de 15 dias no local provisório, pois mais do que isso indicaria que a recuperação da matriz e de seus equipamentos está demorando muito, acarretando na perda de clientes.

Alta administração trabalhará no local provisório até voltar à normalidade.

O setor de Recursos Humanos cuidará de possíveis colaboradores feridos ou que precisem de indenização ou apoio financeiro após o incidente.

Os setores financeiro e administrativo trabalharão em regime *home office,* para que as atividades voltem ao normal.

Suportes necessários no local afetado e a troca de possíveis equipamentos danificados pelo incidente devem ocorrer. Logo após checar que todos os equipamentos funcionam bem, as atividades no local original devem voltar ao normal.

Pronto para o próximo?

Módulo 6

Avaliação de Desempenho e Melhoria

Introdução

Explorar sobre os exercícios, testes, monitoramento, medição, análise e avaliação:

- O processo de exercitar e testar o Plano de Continuidade de Negócios, e como garantir sua eficácia;
- O processo de monitoramento, medição, análise e avaliação do SGCN e seu objetivo;
- O processo de auditoria interna e como garantir a conformidade;
- O objetivo da análise crítica pela Direção.

Etapa Agir, da metodologia PDCA na Continuidade de Negócios

- A importância de se agir em relação às não conformidades e de se tomar ações corretivas;
- A importância da melhoria contínua do SGCN e seu conteúdo.

Exercícios e Testes

Uma série de **EXERCÍCIOS REALISTAS** identificará áreas que necessitam de alteração, por isso da importância de um programa de exercícios consistente com o **ESCOPO DOS PROCEDIMENTOS DE CONTINUIDADE DO NEGÓCIO**, que deve ser **DOCUMENTADO**.

Esse programa deve conter procedimentos de simulações nos sistemas

técnicos | **logísticos** | **administrativos** | **processuais** | **outros**

Deve englobar toda a infraestrutura de continuidade do negócio

Funções | **Responsabilidades** | **Locais de gerenciamento de incidentes e áreas de trabalho.**

Deve ser flexível | **Considerar as mudanças dentro da organização**

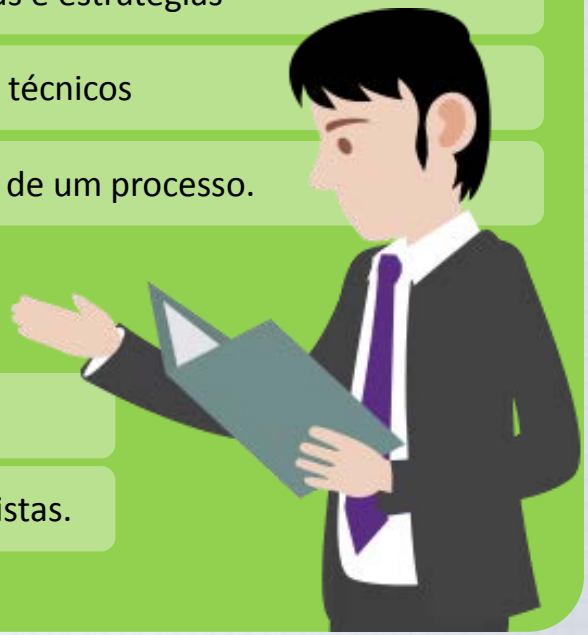
E o resultado de exercícios anteriores.

Através deles é possível antecipar um resultado e permitir que a organização desenvolva soluções inovadoras.

- Ser realistas
- Cuidadosamente planejados
- Acordados com as partes interessadas

Exercícios e Testes

- Sensibilização
- Melhor compreensão do conteúdo
- Uso dos procedimentos de continuidade do negócio
- Melhora na confiança na resposta aos incidentes, oportunidade de melhoria
- Validação do escopo de planejamento, premissas e estratégias
- Garantia do funcionamento correto de recursos técnicos
- Redução do tempo necessário para a realização de um processo.



Métodos:

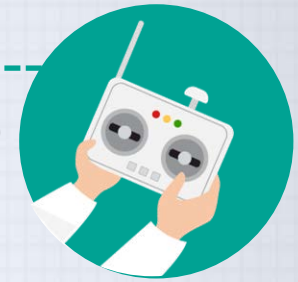
- Seminários
- Simular passo a passo os plano
- Teste de mesa
- Teste funcional e até testes completos bem realistas.

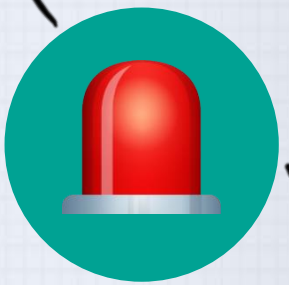
Exercitando e Testando

A maioria das empresas costuma fazer simulações uma vez por ano, mas, se o CEO ver a necessidade de que elas sejam mais frequentes, porque se trata de uma área ou uma empresa com muitas mudanças em pouco tempo, ele vai determinar simulações a cada três ou seis meses.

Depende

Qual a frequência necessária?





Risco menos perigoso

Simulações não devem ser jamais encaradas como exercícios chatos de rotina, mas sim como oportunidades de aprender e melhorar os planos do SGCN.

Exercitando e Testando

Mantenha sempre um relatório com os resultados de cada simulação;

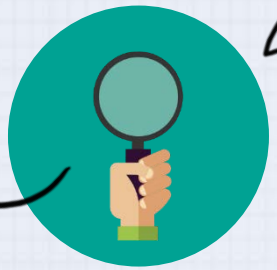
Escolha focar no próximo exercício daquele ponto que teve o pior resultado na simulação anterior;

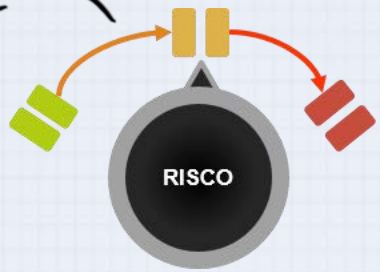
Considere quais as mudanças que ocorreram entre as simulações.

No relatório de exercícios, não se esqueça de colocar data, nome do responsável pela simulação, objetivos do teste, método e roteiro.

O responsável deve, ao final, escrever sobre suas percepções sobre o cumprimento ou não dos objetivos.

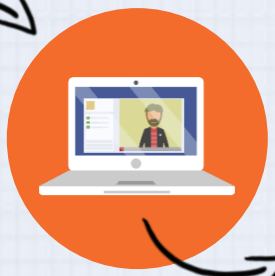
Manutenção dos Planos





O trabalho não acaba com os planos prontos, muito menos com uma simulação bem-sucedida.

Por isso, a empresa que depende da tecnologia deve revisar o seu SGCN com mais frequência.



Deve revisar o plano de seu setor.

Revisa os planos que não são interdependentes.

Revisão Pós Incidente

Faz parte de um bom SGCN a criação de uma documentação sobre a reação aos eventos, e o que pode ser apreendido deles.

Não precisa ser imensamente detalhado.

Na hora de revisar o incidente, tenha em mente os objetivos que foram estabelecidos no SGCN originalmente.

O que aconteceu?

Por que isso aconteceu?

Como foi a reação ao acontecimento?

A recuperação se deu no tempo previsto ou foi necessário mais tempo?

Os recursos foram suficientes ou não?

Revisão Pós Incidente

Alguns recursos se mostraram mais valiosos do que se imaginava?

O incidente teve uma causa inesperada, ou esteve ligado de alguma forma a outra ação?

Algum risco foi esquecido ou menosprezado?

Monitoramento e Avaliação de Desempenho

Inclua neste processo uma definição das métricas que serão utilizadas para medir o desempenho.

Crie os procedimentos para o monitoramento do desempenho e inclua medidas qualitativas e quantitativas

- Política
- Objetivos
- Metas
- Desempenho dos processos
- Procedimentos e funções
- Requisitos legais
- Monitorando as falhas
- Incidentes
- Não conformidades

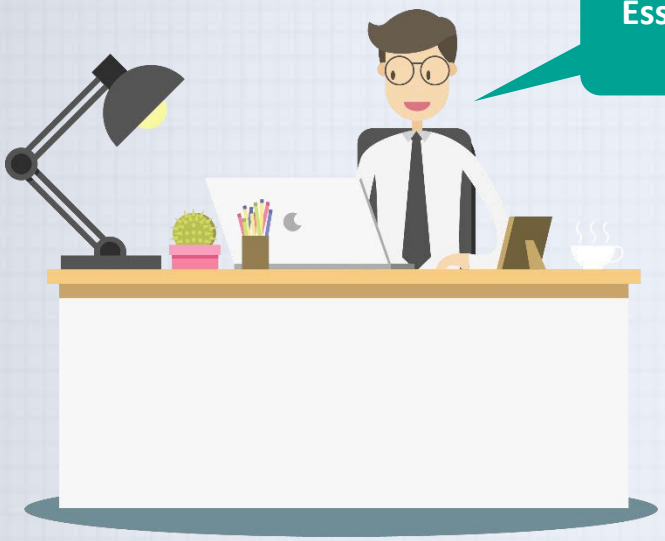
Grave e armazene todos estes dados e resultados de monitoramento para facilitar uma análise posterior das ações corretivas.

INDICADORES DE DESEMPENHO

- Quantitativos
- Qualitativos

- Com que frequência?
- Quem monitora?
- Quais métodos serão utilizados?
- Quem fará a avaliação?
- Para quem informar os resultados?

Avaliação dos Procedimentos de Continuidade



Essas avaliações devem ser feitas sempre que houver mudanças na política, estratégia, objetivos ou outros elementos do SGCN.

Auditorias internas | **Auditorias externas** | **Autoavaliação**

PROGRAMA DE AVALIAÇÃO DE CONTINUIDADE DE NEGÓCIOS

- Deve verificar se todos os principais produtos e serviços e suas atividades e recursos foram identificados e inclusos na estratégia de continuidade de negócios da organização.

Política de continuidade dos negócios

Estratégias

Estrutura e procedimentos de continuidade de negócios

Soluções de continuidade

O processo de manutenção da continuidade dos negócios da organização

Avaliação dos Procedimentos de Continuidade

- Se os programas de testes e exercícios foram efetivamente implementados
- E se as melhorias foram identificadas durante um incidente
- Ou até mesmo durante um exercício
- Deve avaliar se a organização possui um programa contínuo de capacitação e conscientização
- Se os procedimentos de continuidade do negócio foram efetivamente comunicados
- E se os processos de controle de mudança operam efetivamente.

Gerar evidências documentadas que as mudanças na organização foram incorporadas na continuidade, que de fato está sendo feito a gestão do SGCN

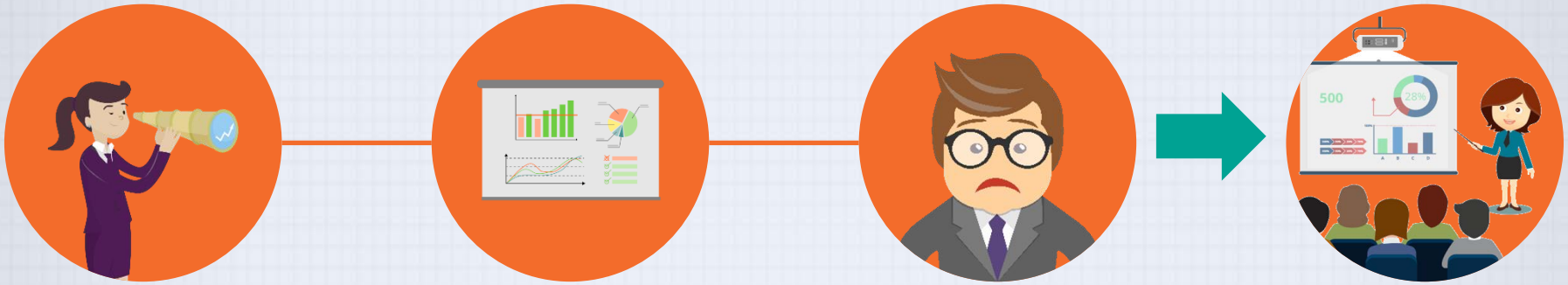
Verificar se as pessoas chave que devem implementar a estratégia e procedimentos de continuidade do negócio são treinadas e se tem competência para tal

E verificar o acompanhamento e controle dos riscos de continuidade do negócio enfrentados pela organização.

Avaliação dos Procedimentos de Continuidade

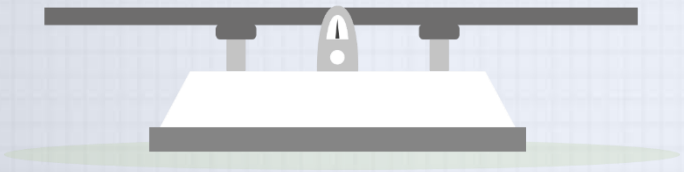
1. Deve haver uma revisão pós-incidente que identifique a natureza e a causa do incidente
2. Avaliar o tempo gasto na recuperação
3. A preparação dos funcionários para o incidente
4. E identificar as melhorias a serem feitas na continuidade do negócio.

Monitoramento e Medição



Objetivos simples

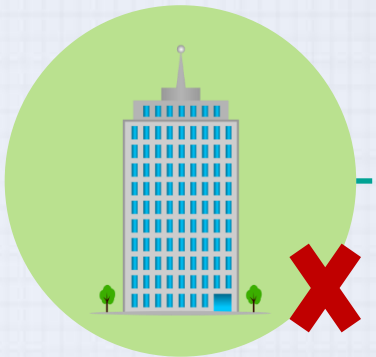
Objetivos mais complexos



IMPORTANTE manter os métodos de monitoramento e mensuração bem explicados na documentação do SGCN, e de registrar e guardar os resultados de todas as mensurações, para que os resultados possam ser comparados, ano após ano, para ver se está havendo, de fato, melhorias.

Auditoria Interna

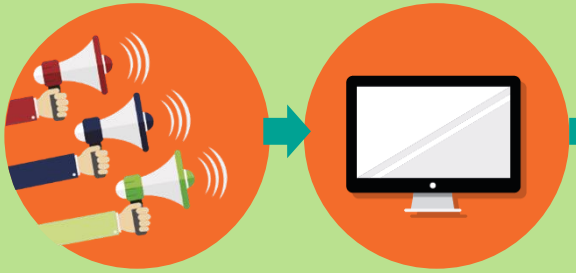
- Antes
- Durante
- Depois da implementação do SGCN



Uma auditoria bem-feita muda toda a percepção do SGCN, e ajuda a identificar erros pontuais. Não é um luxo e não gera desconforto. É uma questão de preparação, treinamento e planejamento.

Auditoria Interna

A melhor opção é escolher dois auditores internos:



O serviço de auditoria é mais ou menos padronizado.

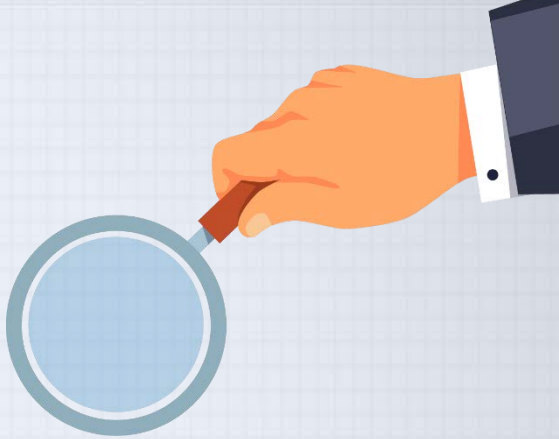
- Para pequenas empresas, uma auditoria anual é suficiente.
- Para empresas maiores, pode ser mais interessante e organizado dividir as auditorias de acordo com os setores, e programar um setor por mês para ser auditado.

- **No caso de escolher funcionários como auditores, é obrigação da gerência apontar os funcionários que exercerão esta função.**
- **E definir as regras de auditoria e depois analisar o relatório com os resultados observados pelos auditores.**

Auditoria Interna

- Defina antes quem fará a auditoria
- Será um auditor interno em tempo integral
- Tempo parcial
- Ou será um auditor interno "externo"
- Execute uma série de pequenas auditorias ao longo do ano
- Use o mesmo auditor e regras para todos os padrões ISO
- E escreva um procedimento e programa de auditoria interna

Certificação e Auditoria Externa



Pense bem se sua empresa necessita passar por esta prova de fogo que, além do mais, será repetida de tempos em tempos.

Se todos os concorrentes da sua área já tiverem a certificação, caso esta seja necessária para expandir sua lista de clientes....

O Que Esperar de Uma Auditoria Externa

planejar → **testar** → **monitorar** → **modificar** → **e auditar internamente o seu SGCN**

Sério → Também certificado → Com boa reputação no mercado

Veja se é possível realizar uma auditoria conjunta ou integrada, que envolva a observância de critérios de mais de um sistema de qualidade. Uma opção é auditar, de uma vez só, a implementação da ISO 9001 e do SGCN na empresa.

A REVISÃO DOS DOCUMENTOS:

- É feita apenas pelo auditor.
- É a parte teórica da auditoria, na qual o auditor confere se todos os documentos obrigatórios estão presentes no SGCN, e se a redação deles está correta.

1

A AUDITORIA PRINCIPAL:

2

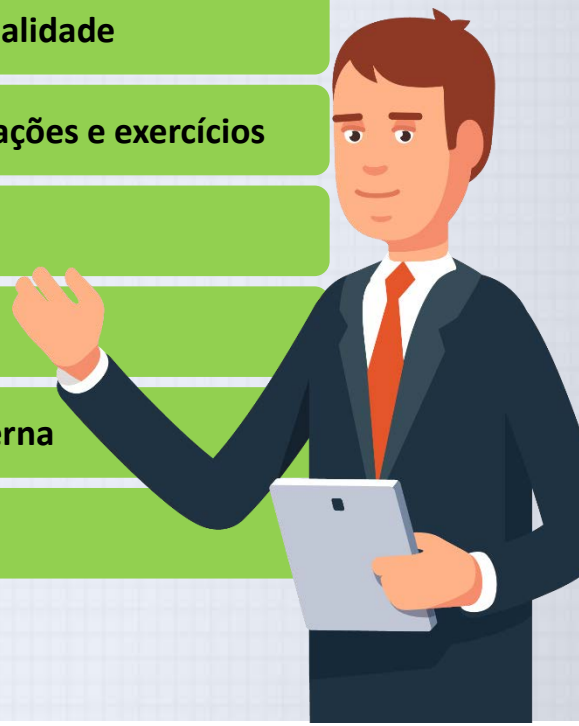
- É na auditoria principal que o auditor avalia se os planos do SGCN foram de fato colocados em prática. Ele chega a esta conclusão através da observação da rotina da empresa, de entrevistas mais ou menos formais com os colaboradores e especialmente, através da análise de relatório da organização.

Documentos Obrigatórios para Auditoria

- Documento determinando o contexto da organização
- Requisitos legais e ambientais obrigatórios
- Escopo do SGCN
- Política da continuidade dos negócios
- Objetivos da continuidade dos negócios
- Competências dos colaboradores
- Plano de comunicação para as partes interessadas
- Análise de riscos e impactos ao negócio
- Procedimentos da continuidade dos negócios
- Procedimentos para reação aos incidentes mais prováveis

Documentos Obrigatórios para Auditoria

- **Plano de comunicação para impactos dos incidentes**
- **Plano de comunicação para autoridades sobre os incidentes**
- **Relatórios sobre os incidentes que aconteceram e / ou testes e simulações**
- **Procedimentos para recuperação, restauração dos negócios e o retorno à normalidade**
- **Dados e resultados de monitoramento e mensuração de incidentes e/ou simulações e exercícios**
- **Resultados do relatório pós-incidente e/ou pós-simulação**
- **Resultados da auditoria interna**
- **Análise crítica ou revisão e comentários da direção / CEO sobre a auditoria interna**
- **Relatório com ações de melhorias.**



Objetivos do Auditor

O auditor externo vai procurar as não conformidades, ou seja, as situações que não estejam conforme o especificado na parte escrita, ou, se os documentos não estejam redigidos conforme as normas.

Não Conformidade Leve

Poderá emitir a certificação, mas voltará em 12 meses para observar se o problema foi resolvido.

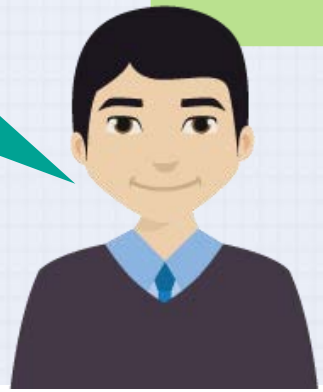
Não Conformidade Grave

A certificação não será emitida, mas você terá uma nova chance:

Se a não conformidade grave for solucionada em um prazo estabelecido pelo auditor a certificação será finalmente liberada.

90 dias

A falta ou falha encontrada poderá causar ou piorar um incidente?



Objetivos do Auditor

Não conformidade LEVE

É apenas uma falha.

Não conformidade GRAVE

Ocorre quando falta todo um sistema de gestão, ou este sistema tem falhas graves o suficiente para prejudicar a organização.

- **A certificação é válida por três anos e precisa ser renovada após este período.**
- **É comum que o auditor externo visite sua empresa anualmente para controle e verificação do SGCN, mesmo após a certificação ter sido emitida sem problemas.**

Análise Crítica da Direção

Análise crítica da direção. → *Management Review* → Revisão Gerencial → Revisão de Gerenciamento

Frequência mínima: 1 ano

REUNIÕES → Plano original → Relatórios das últimas atividades

- Quais melhorias e mudanças são necessárias;
- Se os objetivos estabelecidos foram atingidos, e o que aconteceu caso não tenham sido atingidos;
- Quais mudanças orçamentárias foram aprovadas e quais precisam passar por novos planos ou mais adequações;
- Se já está na hora de modificar alguma parte do plano;
- Se já é o momento de tentar a certificação externa.

Fatores que Desencadeiam uma Análise Crítica

BIA e RA:

O SGCN deve ser revisado sempre que uma BIA ou avaliação de risco for completada. Os resultados podem ser usados para determinar se o SGCN aborda adequadamente ou não os riscos que a organização enfrenta.

Mudanças de tendências do setor ou indústria.

- **Melhores práticas**
- **Técnicas de planejamento de continuidade operacional**

Requisitos regulamentares;

Experiência em incidente

Ativado

A revisão deve levar em consideração o histórico do procedimento de resposta, como funcionou, por que foi ativado, etc.

Não ativado

A revisão deve examinar por que, e se essa foi uma decisão apropriada;

Resultados de teste e exercício.

Fatores que Desencadeiam uma Análise Crítica

Exemplos de procedimentos, sistemas ou processos que podem afetar o SGCN:

- Mudanças na política;
- Mudanças na organização e seus processos de negócios;
- Mudanças no escopo do SGCN;
- Mudanças nas premissas da BIA e da RA;
- Mudanças de pessoal (colaboradores como os contratados), incluindo as suas informações de contato;
- Alterações na cadeia de fornecedores e suprimentos;
- Mudanças de tecnologia e dos processos;
- Mudanças no software e aplicativos;
- Mudanças nas ameaças e perigos;
- Lições aprendidas com exercícios e testes;
- Lições aprendidas com os incidentes de outras;
- Problemas descobertos durante a implementação de procedimentos de continuidade de negócios;
- Mudanças no ambiente externo;

Ações Corretivas

Melhorias

Ações corretivas

- Solucionar problemas com produtos ou serviços
- Desenvolver novos produtos para atender à demanda dos consumidores
- Reajustar preços para se manter competitivo, e muitos outros.

Atualizações

Updates

- Devem ser feitos de tempos em tempos.
- Qualquer funcionário pode sugerir uma ação corretiva ou uma atualização.

Ao adotar as ações no dia a dia, use os mesmos procedimentos que são comuns no SGCN, incluindo os relatórios e modos de arquivamento.

Junto aos documentos do SGCN, deve haver um documento com normas a serem seguidas com as ações corretivas mais comuns e mais fáceis de serem previstas.

Ações Corretivas

"Não conformidades"

- Devem ser relatadas, revistas, e precisa ser decidido como resolvê-las.

As entradas para as ações corretivas seriam aquelas

"Criadas por alguém"

Os incidentes

Uma auditoria interna

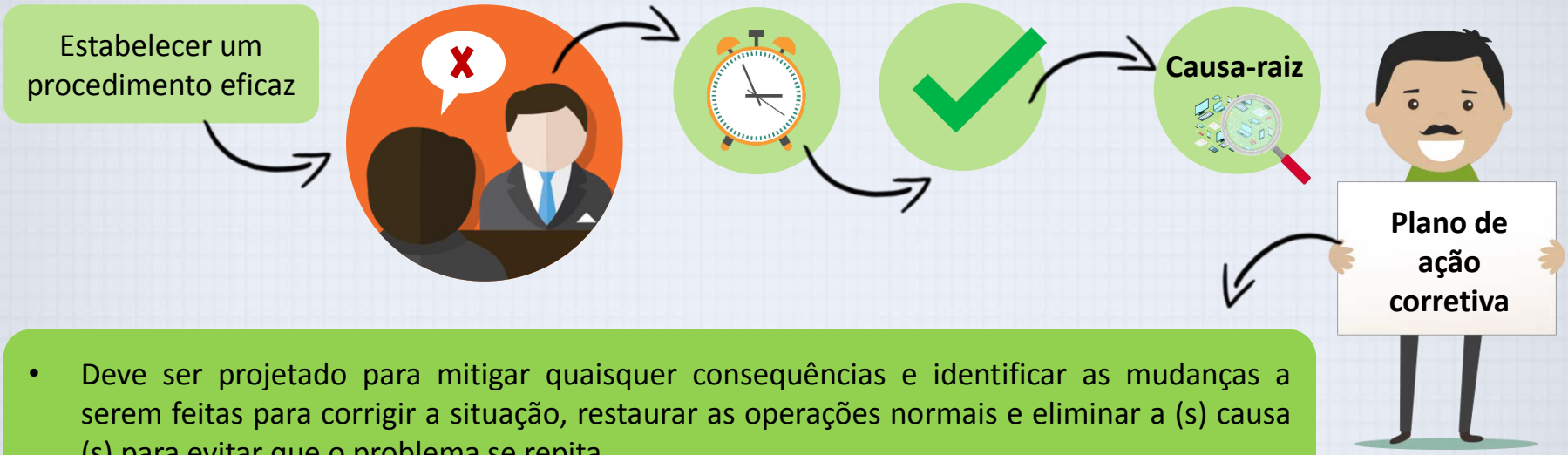
Resultados dos testes e exercícios

Pedido de melhoria

Análise crítica da direção

Não Conformidades

Além de IDENTIFICAR as NÃO CONFORMIDADES, a empresa deve tomar MEDIDAS para controlar, conter, corrigi-las, lidar com suas consequências e avaliar a necessidade de ação para eliminar suas causas.



- Deve ser projetado para mitigar quaisquer consequências e identificar as mudanças a serem feitas para corrigir a situação, restaurar as operações normais e eliminar a (s) causa (s) para evitar que o problema se repita.

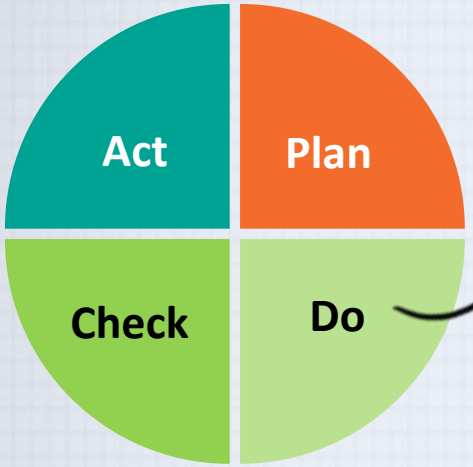
- Um potencial problema pode ser identificado até durante o processo interno de auditoria, exercícios e testes. A identificação de uma potencial não conformidade também pode fazer parte das responsabilidades rotineiras de pessoas que já tenham consciência da importância de observar e comunicar problemas potenciais ou reais.

Não Conformidades

As ações necessárias para eliminar a causa das não conformidades são:

1. Revisar as não conformidades;
2. Determinar o que as causou;
3. Avaliar a necessidade de ações para garantir que elas não se repitam;
4. Determinar e implementar ações adequadas que sejam necessárias;
5. Revisar a eficácia das ações corretivas tomadas.

Melhoria Contínua



- No nível SGCN, o tempo de ciclo é de um ano até vários anos;
- No nível do programa de continuidade do negócio, o tempo de ciclo pode ser de seis meses até um ano;
- Alguns elementos do programa podem ter um tempo de ciclo de alguns meses.

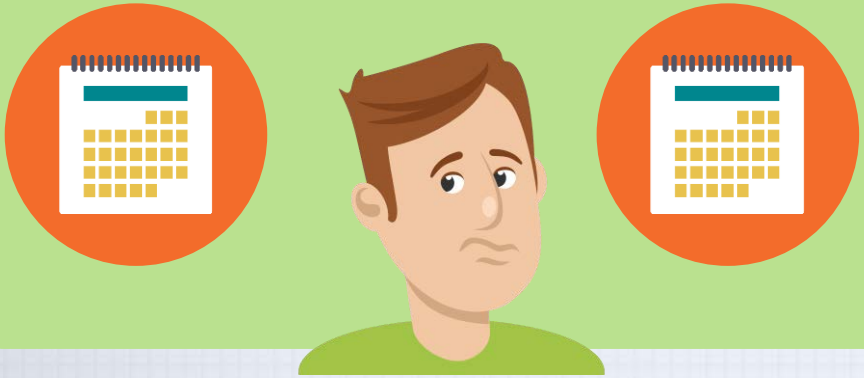
complexidade | **natureza** | **tamanho**

MELHORIA CONTÍNUA:

- Política de continuidade do negócio;
- dos objetivos;
- dos resultados de auditoria
- da análise de eventos monitorados
- das ações corretivas
- e da análise crítica da direção

Melhoria Contínua

- Exige também um processo que identifique adequadamente os problemas e as não conformidades e, em seguida, devem ser corrigidos.
- Este processo deve abordar a natureza do problema e o ambiente dentro do qual este existe, e incluir a mudança do ambiente para garantir que o problema não se repita.
- Cada passo deve melhorar o anterior, para que a melhoria englobe mais do que apenas o problema identificado originalmente, e que tenha um efeito mais amplo e mais significativo na organização.
- Cada implementação de ações corretivas deve ser validada e marcada como eficaz. Cada ação deve ter uma data estimada de conclusão.



Não conformidade | **Causa-raiz** | **Ação corretiva**

Outros Sistemas de Gestão

Mesmo que você não faça parte da área administrativa da organização, deve saber que a administração não é uma atividade separada, e que todos os sistemas são interligados. Com o SGCN não é diferente.

Não é apenas uma questão de moda: a **VISÃO HOLÍSTICA DA ADMINISTRAÇÃO** de uma empresa é, atualmente, a mais útil e segura para garantir o bom funcionamento de todos os setores.

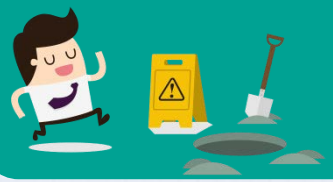
Integrar as novas operações, que surgem com o SGCN a um software de Gestão Integrada permitirá não apenas que os processos do SGCN sejam também otimizados, mas que todos os demais processos também se tornem mais seguros.

Conclusão

1. O SGCN é um conceito relativamente novo, mas muito importante.

2. O SGCN entra na gestão holística, e para ter sucesso precisa envolver todos os setores da empresa.

3. Definir os riscos que a empresa está exposta, e a partir desta lista descobrir quais são os riscos que trariam os maiores prejuízos.



4. Inclui várias etapas de convencimento da direção sobre a importância do SGCN e o treinamento dos funcionários, para reagir aos riscos e mudar determinados comportamentos, adquirindo hábitos mais seguros no ambiente de trabalho

5. É hora de reavaliar o que foi feito, através de testes e simulações, nos quais se pode observar a dinâmica entre os funcionários em um ambiente controlado. A partir desta observação, mudanças nos planos do SGCN devem ser feitas para que ele fique otimizado e garanta mais segurança para a empresa.

Pronto para o próximo?