GESTÃO DE SEGURANÇA DA INFORMAÇÃO

GESTÃO DA CONTINUIDADE DO NEGÓCIO SEGUNDO A NBR ISO/IEC 15999

Olá!

Nesta aula, você irá:

Compreender Gestão da Continuidade do Negócio Segundo a NBR ISO/IEC 15999

1. Objetivo e escopo.

2. Termos e definições.

3. Visão geral da gestão da continuidade de negócios (GCN).

4. Elementos do ciclo de vida da gestão da continuidade de negócios.

Os desastres são eventos de grande magnitude em termos de prejuízo, porém, com probabilidade muito baixa de ocorrência. Um desastre é sempre um incidente, mas só podemos definir se um incidente se tornou um desastre depois de avaliarmos suas consequências.

A diferença entre estes termos é que o incidente é um evento imprevisto e indesejável que poderia ter resultado em algum tipo de dano à pessoa (de um ferimento que leve até a morte), ao patrimônio (próprio ou de terceiros) ou ainda algum tipo de impacto ao meio ambiente (aos ecossistemas, à fauna e à flora), mas não resultou. O desastre é um evento que efetivamente gerou danos humanos, materiais e ambientais.

As características desse tipo de evento, o desastre, fazem com que as organizações tenham a necessidade de implantar planos abrangentes de continuidade de negócio, visando a preservação da integridade física dos colaboradores da organização, bem como proteções adequadas que garantam o funcionamento dos processos e informações no menor espaço de tempo possível que, caso sejam seriamente afetados, possam comprometer a própria existência da organização.

Tipos de desastres

A norma NBR ISO/IEC 15999, é a norma que trata da continuidade de negócios e é dividida em duas partes:

ABNT NBR 15999-1 – Gestão da continuidade de negócios – Parte1: Código de prática

ABNT NBR 15999-2 – Gestão da continuidade de negócios – Parte2: Requisitos

A parte 1 da norma é um código de prática da gestão da continuidade de negócios.

A parte 2 especifica os requisitos para estabelecer um Sistema de Gestão de continuidade de negócio (SGCN) eficaz definido por um programa de Gestão de Continuidade de Negócio (GCN).

NBR ISO/IEC 15999:1

Objetivo e escopo

A norma NBR ISSO/IEC 15999:1 orienta as organizações na estruturação e implementação da continuidade de negócio. Foi elaborada para fornecer um sistema baseado nas boas práticas de gestão da continuidade de negócios. Serve como referência única para a maior parte das situações que envolve a continuidade de negócio, podendo ser usada por organizações de grande, médio e pequeno portes, nos setores industriais, comerciais, públicos e de caráter voluntário.

Termos e definições

A norma NBR ISSO/IEC 15999:1 estabelece alguns termos e definições:

Alta Direção: Pessoa ou grupo de pessoas que dirige e controla um organização em seu nível mais alto.

Continuidade de negócios: Capacidade estratégica e tática da organização de se planejar e responder a incidentes e interrupções de negócios, para conseguir continuar suas operações em um nível aceitável previamente definido.

Estratégia de continuidade de negócio: abordagem de um organização que garante a sua recuperação e continuidade, ao se defrontar com um desastre, ou outro incidente maior ou interrupção de negócios.

Impacto: consequência avaliada de um evento em particular.

Incidente: situação que pode representar ou levar a uma interrupção de negócios, perdas, emergências ou crises.

Interrupção: evento, seja previsto (por exemplo, uma greve ou furação) ou não (por exemplo, um blecaute ou terremoto) que cause desvio negativo imprevisto na entrega e execução de produtos ou serviços da organização de acordo com seus objetivos.

Período máximo de interrupção tolerável: Duração a partir da qual a viabilidade de uma organização será ameaçada de forma inevitável, caso a entrega de produtos ou serviços não possa ser reiniciada.

Planejamento de emergência: desenvolvimento e manutenção de procedimentos acordado de forma a prevenir, reduzir, controlar, mitigar e escolher ações a serem tomadas no caso de uma emergência civil.

Plano de continuidade de negócio(PCN): Documentação de procedimentos e informações desenvolvidas e mantida de forma que esteja pronta para uso caso ocorra um incidente, de forma a permitir que a organização mantenha suas atividades críticas em um nível aceitável previamente definido.

Plano de gerenciamento de incidentes: Plano de ação claramente definido e documentado, para ser usado quando ocorrer um incidente que basicamente cubra as principais pessoas, recursos, serviços e outras ações que sejam necessárias para implementar o processo de gerenciamento de incidentes.

Programa de gestão de continuidade de negócio: Processos contínuos de gestão e governança que são suportados pela alta direção e que recebem os recursos apropriados para garantir que os passos necessários estão sendo tomados de forma a identificar o impacto de perdas em potencial, manter estratégias e planos de recuperação viáveis e garantir a continuidade de fornecimento de produtos e serviços por meio de treinamentos, testes, manutenção e análise críticas.

Resiliência: capacidade de uma organização de resisitir aos efeitos de um incidente.

Visão geral da Gestão da Continuidade de Negócios (GCN)

A gestão de continuidade de negócio permite uma visão total da organização e facilita o relacionamento com as diversas áreas. É um processo da organização que estabelece uma estrutura estratégica e operacional adequada para:

- Melhorar proativamente a resilência da organização contra possíveis interrupções de sua capacidade em atingir seus objetivos;
- Prover uma prática para resstabelecer a capacidade de uma organização fornecer seus principais produtos e serviços, em um nível previamente acordado, dentro de um tempo previamente determinado após uma interrupção;
- Obter reconhecida capacidade de gerenciar uma interrupção no negócio, de forma a proteger a marca e reputação da organização.

É importante que a GCN esteja no nível mais alto da organização para garantir que as metas e objetivos definidos não sejam comprometidos por interrupções inesperadas, que podem ter consequências tanto para a reputação

da organização como até mesmo sua sobrevivência. Além disso a GCN deve ser vista como uma complementação à estrutura da gestão de risco que busca entender os riscos das operações e negócios e suas consequências. Neste caso a GCN irá identificar os produtos e serviços dos quais a organização depende para sobreviver e será capaz de identificar o que é necessário para que a organização continue cumprindo suas obrigações.

Elementos do ciclo de vida da Gestão da Continuidade de Negócios

O ciclo de vida da Gestão de continuidade de negócios é composto por seis elementos obrigatórios e que podem ser implementados em todos os tipos de organizações de diferentes tamanhos e setores. Cada organização ao implementar a gestão da continuidade de negócios deverá adaptar as suas necessidades: o escopo, a estrutura do programa de GCN e o esforço gasto.

Para o estabelecimento do programa de GCN é necessário entender a organização para definir a priorização dos produtos e serviços da organização e a urgência das atividades que são necessárias para fornecê-los.

A determinação da estratégia de continuidade de negócio permite que uma resposta apropriada seja escolhida para cada produto ou serviço, de modo que a organização possa continuar fornecendo seus produtos e serviços em um nível operacional e quantidade de tempo aceitável durante e logo após uma interrupção.

O desenvolvimento e implementação de uma resposta de GCN resulta na criação de uma estrutura de gestão e uma estrutura de gerenciamento de incidentes, continuidade de negócios e planos de recuperação que irão detalhar os passos a serem tomados durante e após um incidente , para manter ou restaurar as operações.

A organização precisa verificar se suas estratégicas e planos estão completos, atualizados e precisos. O GCN deverá ser testado, mantido, analisado criticamente, auditado e ainda identificada as oportunidades de melhorias possíveis.

Para que às partes interessadas tenham confiança quanto à capacidade da organização de sobreviver a interrupções, a Gestão de continuidade de negócio deverá torna-se parte dos valores da organização, através da sua inclusão na cultura da empresa.

A gestão do programa possibilita que a capacidade de continuidade de negócios seja estabelecida e mantida de forma apropriada ao tamanho e complexidade da organização.

Gestão do programa de GCN

Para que um programa de GCN seja implementado nas organizações e alcance os objetivos definidos na Política de Continuidade de Negócios a gestão deste programa deverá envolver as seguintes atividades:

Atribuição de responsabilidades

A organização deverá nomear um ou mais pessoas para implementar ou manter o programa de GCN e documentar os papéis e responsabilidades nas descrições de trabalho e grupos de habilidades da organização.

A documentação de um GCN deverá incluir os seguintes documentos:

- Política de GCN: declaração de escopo e termos de referência ;
- Análise de impacto danos negócios (BIA);
- Avaliação de riscos e ameaças;
- Estratégias de GCN;
- Programa de conscientização;
- Programa de treinamento;
- Planos de gerenciamento de incidentes;
- Planos de continuidade de negócio;
- Planos de recuperação de negócios;
- Agenda de testes e relatórios;
- Contratos e acordos de níveis de serviço.

Implementação da continuidade de negócios na organização

desenvolvimento e implementação do programa. Nesta fase é importante que a organização comunique as partes interessadas de forma que todos os envolvidos tenham acesso as informações sintam-se envolvidos pelo processo. Realize capacitação da equipe envolvida e ainda teste a capacidade de continuidade de negócios da organização.

Gestão contínua da continuidade de negócios

Esta atividade deve assegurar que a continuidade de negócios seja incorporada na cultura e atividade da organização. O processo se dá através da realização da análise crítica, do exercício e da atualização de cada componente envolvido neste processo.

Para que seja realizada a manutenção continua e independentemente de como sejam alocados os recursos para a continuidade de negócio na organização, algumas atividades desse ser executadas:

- Definição dos escopo, papéis e responsabilidades;
- Nomeação de uma ou mais pessoas para gerenciar o GCN;
- Manutenção do programa de GCN através da implementação das melhores práticas utilizadas;
- Promoção da continuidade de negócios por toda a organização de forma ampla;
- Administração do programa de testes.
- Análise crítica e atualização da capacidade de continuidade de negócios, análise de riscos e nálise de impacto de negócio (BIA);
- Manutenção da documentação do GCN;
- Gerenciamento dos custos associados à GCN;
- Estabelecimento e monitoramento do gerenciamento de mudanças;

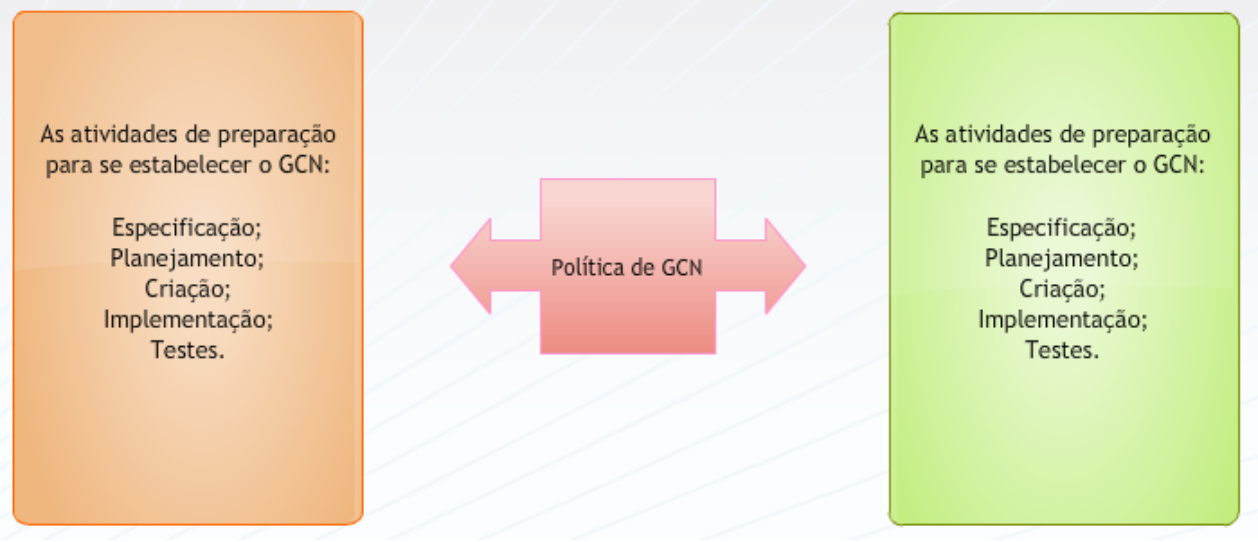
Política de gestão da continuidade de negócios

Segundo a norma NBR ISO/IEC 15999 os propósitos de se estabelecer uma política de continuidade de negócio são:

Garantir que todas as atividades de GCN sejam conduzidas e implementadas de modo controlado e conforme o combinado;

Alcançar uma capacidade de continuidade de negócios que vá ao encontro das necessidades do negócio e que seja apropriada ao tamanho, complexidade e natureza da organização; e implementar uma estrutura claramente definida para a capacidade contínua de GCN.

A política de GCN deverá estabelecer os processos para:



Análise do Impacto do negócio (BIA)

É imprescindível que a equipe responsável pela elaboração e implementação da continuidade de negócio defina e documente o impacto das atividades que suportam seus produtos e serviços. A esse processo damos o nome de

análise de impacto nos negócios e que é conhecido mundialmente por BIA (Business Impact Analysis). A análise do impacto dos negócios é fundamental para fornecer informações para o perfeito dimensionamento das demais fases de elaboração do plano de continuidade de negócio.

O objetivo desta análise é levantar o grau de relevância dos processos ou atividades que compõe a entrega de produtos e serviços fundamentais para a organização e dentro do escopo do programa de GCN. Deve ser mapeado os ativos físicos, tecnológicos e humanos, assim como quaisquer atividades interdependentes que também precisem ser mantidos continuamente ou recuperados ao longo do tempo de cada processo ou atividade, para então apurar os impactos quantitativos que poderiam ser gerados com a sua paralisação total ou parcial.

	Incêndio	Greve	Interrupção de energia	Ataque Denial of Service	Sabotagem	Tolerância
PN1	X		X		X	48 horas
PN2	X					5 horas
PN3	X	X	X	X		24 horas
PN4				X	X	15 horas

É possível neste momento, estabelecer o período máximo de interrupção tolerável de cada atividade através da relação entre o:

- Tempo máximo decorrido de interrupção tolerável de cada atividade;
- Nível mínimo no qual a atividade tem que ser desempenhada após o seu reinicio;
- Tempo máximo até a retomada dos níveis normais de operação;

Quando falamos de impacto estamos nos referindo aos impactos que a organização considere que estejam relacionados com os seus objetivos de negócio. Eles podem ser:

Impacto ao bem-estar das pessoas;

Dano ou perda de instalações, tecnologias ou informação;

Não cumprimento de deveres ou regulamentações;

Danos à reputação;

Danos à viabilidade financeira;

Deterioração da qualidade de produtos ou serviços;

Danos ambientais.

Identificação das atividades críticas

Após a realização do levantamento e da análise do impacto do negócio, a organização deve categorizar suas atividades de acordo com suas prioridades recuperação.

Mas como classificar as atividades?

Atividades cuja perda, baseado no resultado do BIA, teriam o maior impacto no menor tempo e que necessitem ser recuperadas mais rapidamente devem ser chamadas de atividades críticas.

A organização deve considerar também que existem outras não consideradas críticas mas que devem ser recuperadas dentro do seu período máximo de interrupção tolerável.

Processos de negócios / Escala	PN1	PN2	PN3	PN4	PNn
Não considerável					
Relevante	X				
Importante			X		
Crítico				X	
Vital		X			

Saiba mais

O período de tempo máximo para a restauração das atividades pode variar entre segundos e meses, dependendo da natureza da atividade.

A organização deverá estimar os recursos que cada atividade necessitará durante sua recuperação :

- Recursos de pessoal (quantidade, habilidades e conhecimento);
- Localização dos trabalhos e instalações necessárias;
- Tecnologia, equipamentos e plantas que suportam o negócio;
- Informação sobre trabalhos anteriores ou trabalhos atualmente em progresso, de forma a permitir que as atividades continuem no nível acordado;
- Serviços e fornecedores externos;

Identificação das ameaças das atividades críticas

A organização deverá no contexto da GCN entender os nível do risco no que diz respeito às atividades críticas da organização e aos riscos de uma interrupção destas. Desta forma é importante que a organização entenda as ameaças e vulnerabilidades de cada recurso envolvido e o impacto que haveria se uma ameaça se tornasse um incidente e causasse uma interrupção no negócio, através de uma análise de risco.

Determinando a estratégia de continuidade de negócios

A organização deve implementar medidas apropriadas para reduzir a probabilidade de ocorrência de incidentes e seus efeitos. Na adoção destas medidas deverão ser levado em consideração os seguintes fatores:

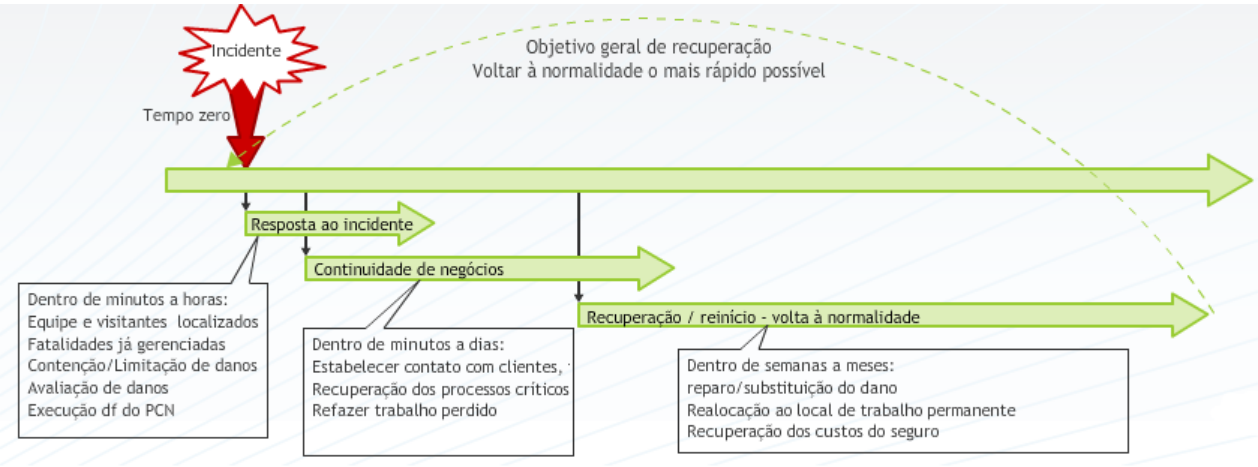
- O período máximo de interrupção tolerável da atividade crítica;
- Os custos de implementação de cada estratégia;
- As consequências não se tomar uma ação;

A organização deve considerar que para a continuidade dos negócios podem ser necessárias o estabelecimento de estratégias para todos os recursos envolvidos nos processos considerados críticos, tais como: pessoas, instalações, tecnologia, informação, suprimentos e partes interessadas.

Determinando a estratégia de continuidade de negócios

A organização deve definir uma estratégia de resposta a incidente que permita uma resposta efetiva e uma recuperação pós-incidente e também a implementação de uma estrutura que caso ocorra um acidente possa rapidamente ser formada. Esta equipe pode receber a denominação de equipe de gerenciamento de incidente ou equipe de gerenciamento de crise.

A estrutura implementada deve possuir: planos, processos e procedimentos de gerenciamento de incidentes, ferramentas de continuidade de negócio, planos para ativação, operação, coordenação e comunicação de resposta ao incidente.



No caso de um incidente a organização deverá ser capaz de:

- Confirmar a natureza e extensão do incidente;
- Tomar controle da situação;
- Controlar o incidente;
- Comunicar-se com as partes interessadas;

Os planos elaborados, sejam de gerenciamento de incidentes, continuidade ou de recuperação de negócios, devem ser concisos, de fácil leitura e compreensão e estar acessíveis à todos que tenham responsabilidades definidas nesses planos e devem conter:

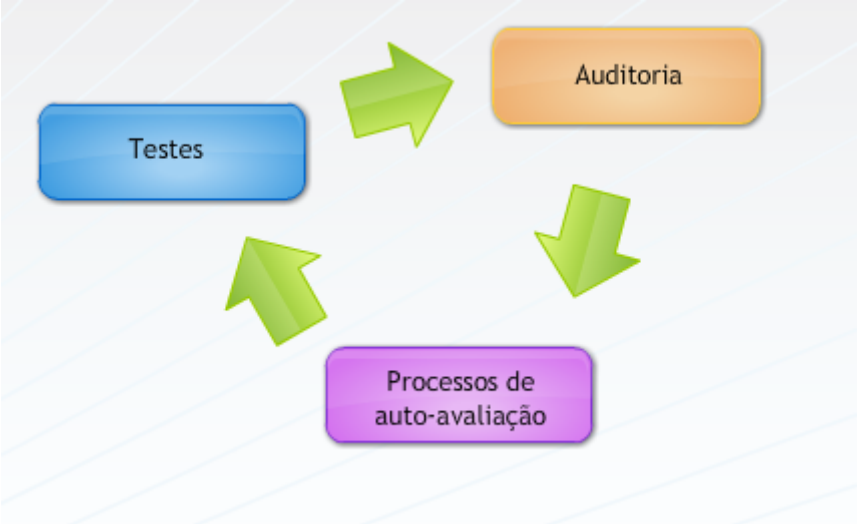
- Objetivo e escopo;
- Definição dos papéis e responsabilidades;
- O método como o plano será colocado em prática;
- Responsável pelo plano;
- Mantenedor do documento do plano (análise crítica, correção e atualização do plano);

Determinando a estratégia de continuidade de negócios

Para que a organização garanta que as implementações de continuidade de negócios e de gerenciamento de incidentes sejam considerados confiáveis e que estão atualizados é necessário que sejam verificados através de testes, auditoria e auto-avaliação.

Deve implementar também um programa de manutenção do GCN claramente definido e documentado. O programa deve garantir que quaisquer mudanças internas ou externas que causem um impacto à organização sejam analisadas criticamente quanto à GCN, inclusive a inclusão de novos produtos e serviços.

A realização da análise crítica da capacidade de GCN da organização, irá garantir sua aplicabilidade, adequação, funcionalidade e conformidade com a política de GCN da organização, leis, normas e melhores práticas. Pode ser realizada através de auditoria ou auto-avaliação.



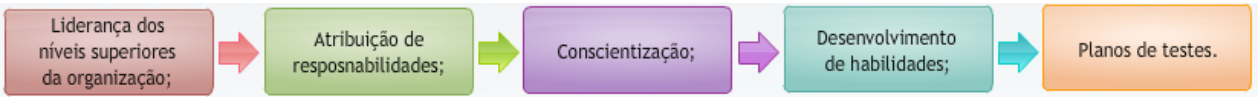
A organização deve implementar um programa de teste deve estar consistente com o escopo do plano de continuidade de negócios,levando em consideração a legislação e as regulamentações em vigor e deve garantir que o PCN funcionará como previsto quando necessário e ainda melhore a capacidade de GCN da organização. Os testes devem ser realistas e planejados cuidadosamente e acordados com as partes interessadas, de modo que haja um risco mínimo de interrupção nos processos de negócio.

A organização deve implementar um processo de auto-avaliação para verificar os objetivos da organização e garantir que tem competência e capacidade de GCN sólidas, eficazes e adequadas. Ele irá verificar qualitativamente a capacidade da organização de se recuperar de um incidente.

A organização deve realizar auditoria para avaliar sua competência de GCN e sua capacidade de identificar falhas reais e potenciais. É necessário que seja implementado e mantido procedimentos para lidar com a auditoria.

Incluindo a GCN na cultura da organização

Para que a continuidade de negócios tenha êxito na organização, é necessário que se torne parte da gestão da organização. Em cada fase do processo de GCN, existem oportunidades de se introduzir e melhorar a cultura de GCN na organização, tornando-se parte dos valores básicos e da gestão da organização. Este processo é divido basicamente nas fases de desenvolvimento, promoção e incorporação da cultura pela organização, sendo suportado por:



A organização deve estabelecer um processo para identificar e implementar os requisitos de conscientização de GCN por meio da educação permanente, além de um programa de informação para toda a equipe. É necessário também a avaliação permanente desta implementação com o objetivo de avaliar a eficiência.

Saiba mais

Clique aqui:

http://estaciodocente.webaula.com.br/cursos/gsgisi/docs/09GSI_doc02.pdf

O que vem na próxima aula

Tema: Estratégias de Proteção

•Assunto 1: Proteção em camadas.

•Assunto 2: Melhores práticas: Cuidados com senhas, Educação dos usuários, Controle de acessos, Uso eficaz de antivírus e antispywares, Backups (cópia de segurança), Plano de continuidade de negócios, Criptografia e certificação digital

CONCLUSÃO

Nesta aula, você:

- Conheceu o processo de Gestão da Continuidade do Negócio segundo a NBR ISO/IEC 15999.
- Conheceu seu objetivo, escopo, termos e definições.
- Compreendeu o processo de gestão e o ciclo de vida da continuidade de negócios (GCN) dentro das organizações.