GOVERNANÇA E SEGURANÇA DA INFORMAÇÃO

GESTÃO DE RISCOS: GESTÃO DA CONTINUIDADE DO NEGÓCIO E AUDITORIA DE SISTEMAS

Autor: Me. Priscila de Fátima Gonçalves

Revisor: Rafael Maltempe

INICIAR

Introdução

Diante da possibilidade de ocorrências de incidentes relacionados à Segurança da Informação, é necessário que se tenha um plano de continuidade de negócio, para que as organizações saibam quais medidas deverão ser tomadas. Dessa forma, é possível que seja evitado que as atividades de uma organização sejam interrompidas ou garantir que sejam retomadas em um curto espaço de tempo.

Neste capítulo, estudaremos o plano de continuidade de negócio, desde a sua concepção até sua real importância para o negócio, pois hoje em dia não é mais aceitável pelo mercado que as falhas ocorram ao ponto de inviabilizar o negócio.

Abordaremos a importância da auditoria de sistemas, como é realizada, por quem é executada, de que maneira isso ocorre e a importância para o negócio. Veremos, também, algumas ferramentas que auxiliam nesse processo, para que o auditor tenha evidências adequadas, que permitam garantir sua opinião sobre a conclusão de sua auditoria em relação às normas e padrões existentes.

Gestão da Continuidade do Negócio

Com a finalidade de garantir que as atividades de uma empresa sempre ocorram de maneira esperada ou, ainda, caso ocorra algum incidente relacionado a ataques ou ameaças à segurança da informação ou, também, que as atividades sejam retomadas em um tempo hábil, é necessário que seja desenvolvido e implementado um plano de continuidade do negócio, em que deverão constar formas de recuperação, respostas e prevenção.

A gestão de continuidade do negócio engloba ações que se referem aos requisitos estratégicos que sejam relacionados às atividades, às pessoas, aos processos e à infraestrutura da organização.

Segundo Hiles (2011), em relação à tecnologia da informação (TI), ameaças de falhas estão maiores e o tempo para que sejam recuperadas as operações é cada tem sido mais escasso. Dessa forma, as empresas precisam estar prontas para atuar sobre incidentes ou ameaças que tenham qualquer tipo de impacto nos negócios no que se refere às informações e sistemas e softwares que deles dependam.

A continuidade dos negócios é assegurada por meio de um plano de gerenciamento de negócios, chamado BCP (Business Continuity Planning), que tem por base: o entendimento da organização, ferramentas que amparam as operações da organização, em que são realizadas avaliações referentes às perdas dessas ferramentas, bem como a definição de quem trabalhará com a situação de crise e como realizará esse trabalho.

De acordo com Hiles (2007), o BCP protege os recursos críticos de negócios e cria procedimentos que garantem a sobrevivência da organização.

> *Identificação e proteção de processos e recursos críticos de negócios necessários para manter a um nível aceitável, protegendo esses recursos e criando procedimentos para garantir a sobrevivência da organização quando ocorrer um incidente de interrupção (HILES, 2007, p. 27).*

Figura 3.1 - Business Continuity Plan
Fonte: Rabia Elif Aksoy / 123RF.

Para que o plano de gerenciamento de negócios seja realizado, é preciso que ocorra a criação, bem como seja definido o projeto no qual deverão constar: escopo, objetivos, exigências, cronograma, entrega, que tenha a certeza do

apoio da alta gestão da organização e os usuários sejam envolvidos.

A gestão da continuidade de negócios deve ser madura e possuir índices que apresentem e permitam mensurar e gerenciar processos do plano de continuidade de negócios. Esse plano deve ter como objetivo definir pontos críticos das áreas de tecnologia da informação e do negócio da empresa.

Assim, o processo de gestão de continuidade de negócios tem como atribuições capturar e analisar informações que resultarão em uma dada estratégia e em um plano de ação, para que se consiga reagir a incidentes em atividades referentes ao negócio.

A empresa precisa realizar a identificação de processos que componham um conjunto de tarefas realizadas, interligadas às informações sobre as quais realiza manipulação, por meio de recursos e estrutura da empresa. No quadro a seguir, serão apresentados os pontos tidos como de maior criticidade para a empresa e fracionado em seus domínios:

Visão do Negócio	Atendimento aos clientes Atendimento a leis e regulamentação
Processos de Negócio	Processos de negócio de missão-crítica Plano de continuidade de negócios
Aplicações	Aplicações e bases de dados de missão-crítica Processamento de dados Procedimentos de recuperação de desastre
Infraestrutura	Segurança física e lógica Comunicações confiáveis Informações protegidas *Hardware/Software* - redundância

Quadro 3.1 - Pontos mais críticos para o negócio
Fonte: Magalhães (2007, p. 667).

Conforme apresentado no quadro, pode-se dizer que, conforme os pontos críticos para o negócio, a visão do negócio aborda o atendimento aos clientes e às leis e à regulamentação. Os processos de negócio estão representados por processos de negócio de missão crítica e pelo plano de continuidade de negócios. No que diz respeito às aplicações, referem-se a bases de dados de missão-crítica, processamento de dados e procedimento de recuperação de desastre e, no que diz respeito à criticidade de infraestrutura, apresenta-se segurança física e lógica, comunicações confiáveis, informações protegidas e redundância relacionada à *hardware* e *software* .

praticar

Vamos Praticar

A continuidade dos negócios é assegurada por meio de um plano de gerenciamento de negócios, chamado BCP (Business Continuity Planning), que tem por base o entendimento da organização, ferramentas que amparam as operações da organização, em que são realizadas avaliações referentes às perdas dessas ferramentas, bem como a definição de quem trabalhará com a situação de crise e como realizará esse trabalho. Assinale a alternativa que contém os objetivos do plano de continuidade de negócio.

- **a)** Realizar a identificação de processos que componham um conjunto de tarefas realizadas.
- **b)** Definir quem trabalhará com a situação de crise e como realizará esse trabalho.
- **c)** Construir um plano que aborde as premissas da organização conforme a alta gerência.

- **d)** Definir os pontos críticos das áreas de tecnologia da informação e do negócio da empresa.
- **e)** Gerenciar o risco operacional existente e avaliar a adequação das tecnologias e dos sistemas de informação utilizados na empresa.

Plano de Continuidade de Negócios: Estrutura

O plano de continuidade de negócios tem como premissa mostrar que processos de tecnologia da informação são críticos e sustentam o negócio da empresa, bem como o que se faz necessário evitar para que os processos sejam restabelecidos no menor tempo possível e alinhados ao que seja prioritário para a empresa, caso ocorra algum tipo de evento ou incidente.

Para desenvolver um plano de continuidade de negócio, é necessário seguir algumas etapas pelas quais deve ocorrer a definição e criação de um projeto, em que deverá constar o escopo, os objetivos, requisitos, dentre outros. A seguir, abordaremos cada um deles.

Escopo e Cenário: Definição

A definição do escopo e cenário deve ocorrer baseando-se no nível de maturidade atual. Esse plano deve conter diferentes etapas e versões melhores do que as anteriores.

Nessa etapa, definem-se permissões para um aplicativo de negócios específico, como os usuários interagem com o aplicativo e qual a real importância deste para o negócio. Ainda na definição, deve-se verificar se é necessária a presença e avaliação de especialistas que sejam de outras divisões e tratem de outras demandas, além de ter o apoio da alta gerência, para que o plano seja sinônimo de sucesso.

Ameaças e Riscos: Avaliação

A empresa deve fazer uma análise minuciosa de ameaças e possíveis riscos considerando o escopo e cenário traçados anteriormente. Essa avaliação deve ser realizada de forma qualitativa (riscos ou ameaças altas, médios, baixos) e deverá ser realizada por mais de uma pessoa.

Nessa etapa, devem-se identificar e avaliar fatores de risco que estejam no ambiente da empresa, para que ocorra a antecipação aos possíveis incidentes de segurança da informação.

Impacto no Negócio: Análise

Será preciso que passem por todo o processo de análise impactante ao negócio, consequências de desastres, falhas de segurança, privação e disponibilidade de serviços.

Deverão ser mapeados os seguintes itens nessa análise:

- impactos financeiros;
- processos de negócios;
- dependências internas e externas;
- recursos críticos;
- prazos para os impactos, conforme a severidade.

A análise do impacto do negócio trata de descobrir e identificar, dentre os processos, quais são críticos para o sucesso da organização e compreender o

impacto de uma interrupção.

Soluções: Identificação

Conforme as informações anteriores, deverão ser verificadas soluções para processar a informação, e a melhor maneira será utilizada para implementar.

O controle de segurança deverá ser implementado, terá de ser o mais adequado, para que se consiga, de fato, a redução do risco, que tenha menor custo e, que propicie menor impacto negativo para os recursos e funcionalidades. Assim, a probabilidade de ocorrer problemas será menor.

praticar

Vamos Praticar

Existem riscos para todos os tipos de organizações. Esse é um dos motivos pelos quais deve ser desenvolvido e implementado um plano de continuidade de negócios, que garantirá que quaisquer problemas relacionados a incidentes sejam superados. Assinale a alternativa que corresponde às etapas da estruturação do plano de continuidade de negócios, na ordem em que ocorrem.

- **a)** Identificação, análise, avaliação e definição.
- **b)** Análise, avaliação, identificação e definição.
- **c)** Definição, avaliação, análise e identificação.
- **d)** Definição, avaliação, identificação e análise.
- **e)** Análise, identificação, avaliação e definição.

Plano de Continuidade de Negócios: Desenvolvimento

O plano de continuidade de negócios deverá ser desenvolvido como forma de documentos e manuais, que apresentarão de forma clara e sucinta, porém completa, em que sejam mapeados os riscos, pessoas e responsabilidades de cada um, para que possam ser utilizados para solucionar incidentes.

Segundo Magalhães (2007), no plano de continuidade de negócios deve constar os seguintes itens:

I. Sumário executivo, no qual conste o propósito, autoridade e responsabilidades de pessoas habilitadas, emergências que porventura possam ocorrer e o local onde serão gerenciadas as operações.

II. Gerenciamento dos elementos de emergência, apresentando os processos de direção e controle, comunicação, recuperação e restauração, administração e logística.

III. Procedimentos de resposta à emergência: a empresa deverá realizar um *checklist* para manter as ações orientadas conforme o que deve ser feito, para que pessoas fiquem protegidas, equipamentos mantidos, alertas emitidos, pessoas devem ser conduzidas para evacuar o local, operações devem ser encerradas, bem como a proteção dos dados vitais e recuperação das operações.

IV. Documentos de suporte: devem estar anexos ao plano de continuidade de negócios. Por exemplo, lista de telefones de pessoas com envolvimento em algum dos processos, planta de instalações, guias desenhados referentes à infraestrutura de tecnologia da informação, bem como procedimentos para restaurar serviços de tecnologia da informação.

V. Identificar desafios e priorizar atividades: deve ter uma lista de atividades que deverão ser realizadas com a definição de quem as fará e quando as fará, mostrando como os problemas identificados deverão ser abordados e tratados.

Esse plano de continuidade de negócios deve ser testado de forma frequente, pois esses testes poderão apresentar situações que não estão previstas no plano e deverão ser inseridas.

Assim, o plano será cada vez mais completo, com seus cenários e escopos maiores. Ainda, é preciso estar atento, pois as necessidades da empresa podem ser alteradas, e o plano deverá acompanhar essas modificações e se adaptar às mudanças.

saiba mais

Saiba mais

Segundo Paz (2018), em um plano de continuidade de negócios, para cada tipo de incidente há um tratamento diferente indicado, conforme os processos que são

críticos ao negócio. Acesse a página e saiba mais a respeito do plano de continuidade de negócios.

ACESSAR

A seguir, um exemplo de um plano de continuidade de negócios proposto para uma empresa que realiza transporte de cargas.

Plano de continuidade de negócios (PCN)

Identificação de incidentes		Tratamento do incidente	
Incidente	Causas	Plano de continuidade	Plano de recuperação
Falta de energia elétrica	Externa	O *nobreak* atual funciona por até 4 horas. O PCO sugere a instalação de um gerador na matriz, para garantir a continuidade dos serviços até o restabelecimento da energia	Acionamento, na prestadora de energia elétrica, do restabelecimento dos serviços
	Interna	Utilização de *nobreaks* para equipamentos do datacenter, *switches* , antenas *wireless* e microcomputadores dos responsáveis pelos serviços críticos	Acionar o setor de patrimônio, para que sejam feitos reparos à rede elétrica
	Nobreak	Substituição da fonte de energia por outro *nobreak* ou estabilizador	Levar o *nobreak* à manutenção, para reparos

Quadro 3.2 - Plano de continuidade de negócios (PCN)

Fonte: Elaborado pelo autor.

praticar

Vamos Praticar

O Plano de Continuidade de Negócios tem como premissa criar normas e padrões, para que as empresas possam recuperar, retomar e dar prosseguimento aos seus mais importantes processos, evitando que ocorram danos que venham provocar perdas financeiras consideráveis.

Considerando essa afirmação, qual parte de sua estrutura tem como finalidade determinar o planejamento, para que a organização retome o funcionamento operacional normalizado?

- **a)** Plano de contingência.
- **b)** Plano de administração ou gerenciamento de crises.
- **c)** Plano de recuperação de desastres.
- **d)** Plano de continuidade operacional.
- **e)** Plano de contingência de desastres.

Auditoria de Sistemas

Figura 3.2 - Auditoria de Sistemas

Fonte: Rafał Olechowski / 123RF.

A auditoria de sistemas é uma atividade independente, que tem como objetivo gerenciar o risco operacional existente e avaliar a adequação das tecnologias

e dos sistemas de informação utilizados na empresa. Esse processo revisa e avalia os controles, o desenvolvimento de *softwares* , os procedimentos de tecnologia de informação (TI), a infraestrutura, a operação, o desempenho e a segurança da informação.

A auditoria de *software* é uma atividade que gerencia riscos operacionais e avalia se as tecnologias de sistemas de informação utilizadas na organização são adequadas. Portanto, estão em jogo informações críticas, que auxiliam na tomada de decisões. Por sua vez, o processo de desenvolvimento tem como objetivos e responsabilidades medir e constatar a eficácia do sistema, atestar a segurança física e lógica e aferir se essas providências atendem às normas.

Geralmente, quem realiza a auditoria é um auditor e, para tanto, é necessário que ele tenha formação em auditoria de computação. São atribuições desse profissional:

- compreender e analisar o ambiente;
- determinar quais são as possíveis situações sensíveis;
- elaborar e aplicar o *checklist* ;
- analisar simulações;
- opinar sobre o ambiente onde está sendo auditado.

O auditor alocado na área de desenvolvimento deve conhecer a metodologia de desenvolvimento de sistemas, suas etapas, técnicas, formulários e conceitos. Ele também deve conhecer os profissionais da área: o líder de projeto, o analista de sistemas e o próprio desenvolvedor.

Ele possui responsabilidades, tais como: motivar melhorias, ser flexível quando necessário e ser imparcial na obtenção dos fatos. Dispõe de uma série de técnicas para realizar o seu trabalho.

Em razão do aumento de problemas resultantes da ineficiência de softwares em relação à qualidade e à segurança – tais como o aumento do número de fraudes, o crescente número de operações de lavagem de dinheiro, o aumento de erro em instituições financeiras e a perda ou o roubo de informações financeiras –, corporações passaram por uma regulamentação que colocou em cena leis rigorosas. Assim, as empresas passaram a adotar

melhores práticas de gestão de risco e de gestão operacional. Agora, a área de TI das organizações deve estar com todos os seus processos alinhados ao negócio, garantindo melhorias nos processos empresariais – governança de TI.

A governança de TI, segundo o Board Briefing on IT Governance, preocupa-se com o alinhamento e a entrega de valor por parte da TI para o negócio; trata das corretas alocações e medição dos recursos envolvidos e da mitigação de riscos em TI (RAMIRES; SPÍNOLA; KALINOWSKI, 2010).

Técnicas para Auditoria de *Software*

A necessidade global de referências promoveu a criação e o desenvolvimento de melhores práticas, como Control Objectives for Information and related Technology (COBIT), Committee of Sponsoring Organizations (COSO), ISO 27001 e Information Technology Infrastructure Library(ITIL), que abordaremos a seguir.

A governança de TI utiliza ferramentas e aplicações de TI com a finalidade de aumentar a vantagem competitiva das empresas. Foram desenvolvidos diversos institutos internacionais e modelos de gestão que, se aplicados, asseguram a conformidade com as melhores práticas de processos, de segurança da informação e de gerenciamento dos riscos corporativos. Esses modelos formam a base do desenvolvimento de controles internos para as instituições. Cada um possui uma metodologia própria, desenvolvida pelo instituto responsável.

A escolha do modelo de gestão depende dos objetivos que a organização visa alcançar de forma gerenciada. Dentre os modelos, destacam-se os listados a seguir:

- **COBIT** : indicado para governança de TI. A metodologia COBIT fornece um conjunto de melhores práticas relacionadas ao controle de objetivos, à otimização de investimentos, aos mapas de auditoria e às técnicas de gerenciamento. Ela é voltada para todas as empresas, independentemente das plataformas tecnológicas adotadas, e busca

alinhar as práticas de TI ao modelo de negócio, com a finalidade de regulamentar o processo.
- **ITIL** : indicada para a gestão de serviços de TI.
- **DRI** : indicado para a especificação e a operação de planos de continuidade de negócios.
- **ISO 17799** : indicado para a gestão de segurança da informação.
- **CMMI** : define um modelo de gestão para o desenvolvimento de softwares.
- **COSO** : indicado para definir processos para o controle interno das empresas.

A auditoria é realizada por meio de técnicas, como as relacionadas a seguir:

- Questionários: por meio dessa técnica, é possível adequar o ponto de controle em relação aos parâmetros de controle interno, como segurança física, lógica, eficiência, dentre outros.
- Simulação de dados: o auditor afere se a aplicação está dentro das normas, verificando se os dados inseridos no sistema são incompatíveis ou estão em duplicidade.
- Visita in loco: trata-se da atuação dos auditores com as pessoas da organização relacionadas ao sistema e às instalações. Por essa técnica, podem-se anotar procedimentos, nomes de pessoas, analisar a documentação e emitir opinião em relatórios.
- Entrevistas: são reuniões entre os auditores e os auditados. Depois de realizar a entrevista, o auditor pode analisá-la e emitir o seu relatório.
- Análise de logs: nessa técnica, verifica-se a utilização de dispositivos componentes de uma configuração ou rede de computadores e do software aplicativo. Assim, pode-se verificar a ineficiência da utilização do computador, bem como identificar erros de programa e/ou operação, utilização de programas que geram fraudes, tentativas de acesso indevidas e problemas na configuração do computador (análise de dispositivos com folga ou sobrecarregados).
- Análise de programa-fonte (código-fonte): essa técnica consiste na

análise visual do programa. Compara-se, também, a versão do objeto que está sendo executado com o objeto resultante da última versão compilada. Essa técnica analisa se o desenvolvedor cumpriu as normas de padronização do código e a qualidade de estruturação do código-fonte.

A auditoria pode ser conduzida de três maneiras. A primeira é realizada por uma organização para ela própria. A segunda é conduzida por uma organização sobre outra. Já a terceira é realizada por uma terceira organização independente, sem que haja interesse nos possíveis resultados da auditoria.

Processo de Auditoria de *Software*

A auditoria de *software* tem como objetivo verificar e constatar a eficácia do sistema, atestar a segurança física e lógica, garantir a qualidade e ajudar a organização a avaliar e validar normas e padrões preestabelecidos. A auditoria de *software* é dividida em três etapas: planejamento, execução e relatório, nessa ordem.

saiba mais

Saiba mais

Para saber mais a respeito de auditoria de sistemas, leia o artigo a seguir.

ACESSAR

No planejamento, é definido o escopo prévio do trabalho que será realizado, para que o auditado possa preparar-se de maneira adequada. A transparência é de suma importância. Em processos transparentes de auditoria, a validade e toda forma de licenciamento são explícitas. Nessa etapa, identifica-se o objetivo referente a cada auditoria, opta-se por auditar o processo ou o produto e define-se a estratégia, bem como o cronograma, que deve ser conhecido pelos membros do projeto. As auditorias devem ter esse cronograma atualizado com base na visualização e devem ser executadas com uma frequência que depende do projeto ou da organização.

Na etapa da execução, os funcionários da área de TI da empresa (possíveis auditados que serão indicados pelo líder da equipe) são apresentados ao auditor (ou aos auditores). Então, são identificados os critérios de auditoria, assim como as *checklists* , que servirão de guia durante o processo. Nessa etapa, o desenvolvedor executa um aplicativo que coleta as informações e as configurações existentes no servidor. O sistema auditor faz uma análise de servidores, aplicações, *softwares* , homologações, licenças, seriais etc.

Além disso, o auditor questiona o auditado acerca da *checklist* , e todas as informações são anotadas e utilizadas para identificar possíveis não conformidades.

No relatório, o auditor apresenta toda a descrição de produtos e usuários, a comprovação de utilização, as não conformidades e as ações recomendadas.

Isso conforme as informações e evidências coletadas na auditoria. A ideia é que a adoção de modelos maduros de desenvolvimento de *software* dê origem a uma infraestrutura que garanta tal maturidade. Essa infraestrutura deve ser criada com base em *frameworks* (modelos) estabelecidos pela International Organization for Standardization (ISO), o Institute of Electrical and Electronics Engineers (IEEE), o COBIT e a ITIL. O auditor afere, por meio de análise norteada por *checklist* , a conformidade ou não do que foi realizado com o padrão devido.

praticar

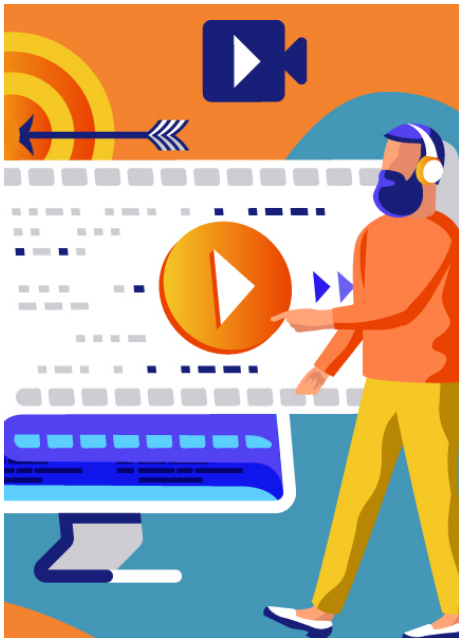
Vamos Praticar

Por meio da auditoria de configuração de *software* , é possível assegurar que a alteração realizada foi implementada de maneira correta, bem como monitorar *baselines* estabelecidas e evitar a violação delas. No que se refere à auditoria de configuração de *software* , é correto afirmar que:

- **a)** Pode-se ter a rastreabilidade das alterações desde a solicitação até a implantação.
- **b)** São verificadas todas as conformidades e não conformidades do sistema.
- **c)** É possível rastrear as alterações até certo ponto, pois chegam somente até a ordem de mudança.
- **d)** As não conformidades deverão ter acompanhamento até o encerramento, considerando a implantação.
- **e)** Identifica-se o objetivo referente a cada auditoria, optando por auditar o processo ou o produto.

indicações

Material Complementar



FILME

Hacker Blackhat

Ano : 2015

Comentário : o filme tem base no mistério que envolve um hacker que explodiu um reator nuclear em Hong Kong, por meio uma intrusão de rede ilegal. Diante disso, o mercado financeiro americano também sofreu danos.

Trata-se de uma reflexão de como códigos podem ser utilizados de maneira errônea para fins ilícitos.

TRAILER

conclusão

Conclusão

Diante do que foi apresentado nesta unidade, pudemos compreender a real necessidade de que as organizações tenham uma gestão de continuidade de negócios, bem como um plano de continuidade de negócios e a realização de auditorias em sistemas/softwares.

O plano de continuidade de negócios tem como premissa mostrar que processos de tecnologia da informação são críticos e sustentam o negócio da empresa, bem como o que é necessário evitar, a fim de que os processos sejam restabelecidos no menor tempo possível e alinhados ao que seja prioritário para a empresa, caso ocorra algum tipo de evento ou incidente.

A auditoria revisa e avalia os controles, o desenvolvimento de softwares, os procedimentos de tecnologia de informação (TI), a infraestrutura, a operação, o desempenho e a segurança da informação.

referências

Referências Bibliográficas

1028-2008: IEEE standard for software reviews and audits. **IEEE** , 2008.

Disponível em: https://standards.ieee.org/standard/1028-2008.html . Acesso em: 14 dez. 2019.

HILES, A. **The definitive handbook of business continuity management** . 2. ed. Chichester: John Wiley & Sons, 2007.

HILES, A. **The definitive handbook of business continuity management** . Chichester: John Wiley & Sons, 2011.

LIMA, I. R. C.; CONSTANTINO, L. O.; ZAMBON, N. **Auditoria de sistemas** . [20-?]. Disponível em: https://edisciplinas.usp.br/pluginfile.php/3344235/mod_resource/content/1/G3_Auditoria%20de%20Sistemas.pdf . Acesso em: 12 dez. 2019.

MAGALHÃES, I. L.; PINHEIRO, W. B. **Gerenciamento de serviços de TI na prática** : uma abordagem com base no ITIL. Porto Alegre: Novatec, 2007.

PAZ, G. **Plano de continuidade de negócios de TI em uma empresa de transporte de cargas fracionadas** . Santa Catarina: Unisul, 2018. Disponível em: https://riuni.unisul.br/bitstream/handle/12345/4950/GUILHERME%20TELES%20PAZ%20-AD6.pdf?sequence=1&isAllowed=y . Acesso em: 20 jan. 2020.

PRESSMAN, R.; MAXIM, B. **Engenharia de software** : uma abordagem profissional. 8. ed. Porto Alegre: AMGH, 2016.

RAMIRES, A. C. S.; SPÍNOLA, R. O.; KALINOWSKI, M. Auditoria de sistemas. **Engenharia de Software Magazine** , v. 28, 2010. Disponível em: http://www-di.inf.puc-rio.br/~kalinowski/publications/RamiresSK10.pdf . Acesso em: 14 dez. 2019.