REVISTA DA MOSTRA DE TRABALHOS DE CONCLUSÃO DE CURSOS CONGREGA
Congrega Urcamp 2017
Realização: URCAMP

PROPOSTA DE UM PLANO DE CONTINGENCIAL EMPRESARIAL NO RAMO SECURITÁRIO EM BAGÉ/RS

PROPOSAL FOR A BUSINESS CONTINGENCY PLAN IN THE SECURITY BRANCH IN BAGÉ / RS

[1]Lenon Couto Machado, [2]Fabio Josende Paz

RESUMO: O plano de contingência é um documento que deve ser parte da política de segurança de uma organização, devendo integrar o planejamento estratégico de cada empresa (Freitas, 2013). Aonde estão definidas as responsabilidades estabelecidas em uma organização, contendo ainda, informações detalhadas sobre as características da área ou sistemas envolvidos. É um documento desenvolvido com o intuito de treinar, organizar, orientar, facilitar, agilizar e uniformizar as ações necessárias às respostas de controle e combate às ocorrências anormais (GORAYEB, 2012). Dessa maneira o presente trabalho trata-se de um plano de contingência empresarial, desenvolvido para prevenção de perdas de conteúdo ou dados, os quais podem ser vulneráveis ao acesso externo, contemplando a empresa com um ambiente mais seguro e organizado. Tendo como principal objetivo, analisar a segurança da informação atual e desenvolver um plano de contingência para auxiliar uma empresa securitária. Sendo assim é necessário subdividir o processo em etapas para ser possível atingir o objetivo proposto, como: identificar as áreas de risco; conhecer a metodologia da empresa e funcionamento dos sistemas; averiguar a segurança de softwares; sugerir melhorias de segurança nos sistemas informatizados da empresa. O plano proposto foi o de otimizar a relação entre os diversos setores da empresa para que as medidas de proteção sejam bem executadas, tanto do ponto de vista interno quanto do ponto de vista externo para atender esse objetivo foi necessário identificar os principais processos de funcionamento da empresa, no ramo de seguros, identificar as dificuldades para a prevenção dos dados no modelo de plano desenvolvido e propor métodos para as principais dificuldades que foram encontradas na empresa.
Palavras chave: Riscos, Prevenção, Segurança da Informação.

ABSTRACT: *The contingency plan is a document that must be part of the security policy of an organization and must integrate the strategic planning of each company. Where the responsibilities established in an organization are defined, also containing*

[1] Bacharel em Sistemas de Informação - URCAMP
[2] Prof. Me. do Curso de Sistemas de Informação da Universidade da Região da Campanha (URCAMP)

detailed information about the characteristics of the area or systems involved. It is a document developed with the purpose of training, organizing, guiding, facilitating, streamlining and standardizing the actions necessary to control responses and combat abnormal occurrences (GORAYEB, 2012). In this way the present work is a business contingency plan, developed to prevent loss of content or data, which may be vulnerable to external access, contemplating the company with a more secure and organized environment. Its main objective is to analyze current information security and develop a contingency plan to assist a security company. Therefore, it is necessary to subdivide the process into stages in order to achieve the proposed objective, such as: identifying the risk areas; Know the methodology of the company and the functioning of the systems; Check the security of software; Suggest security improvements in the company's computer systems. The proposed plan was to optimize the relationship between the various sectors of the company so that the protection measures are well executed, both from the internal point of view and from the external point of view to meet this objective, it was necessary to identify the main processes of operation of the company. Company in the field of insurance, identify the difficulties for data prevention in the developed plan model and propose methods for the main difficulties that were found in the company.
***Keywords**: Scratchs, Prevention, Information Security*

INTRODUÇÃO

O plano de contingência é um documento que deve ser parte da política de segurança de uma organização, devendo integrar o planejamento estratégico de cada empresa. Contingencia significa algo incerto ou eventual, enfatiza a probabilidade de um evento ser afetado por outro. Mediante disso em um plano de contingência são citados procedimentos estabelecidos a serem analisados nas tarefas de recuperação do ambiente de sistemas e negócios. (FREITAS, 2013). Neste estão definidas as responsabilidades estabelecidas em uma organização, contendo ainda, informações detalhadas sobre as características da área ou sistemas envolvidos. É um documento desenvolvido com o intuito de treinar, organizar, orientar, facilitar, agilizar e uniformizar as ações necessárias às respostas de controle e combate às ocorrências anormais (GORAYEB, 2012).

O plano de contingência quando bem planejado nos dá a oportunidade de organizar e minimizar erros futuros em qualquer gestão empresarial. Empresas hoje no qual concentram toda sua base de dados, muitas vezes de forma interna, com conteúdo no qual podem ser danificados ou perdidos facilmente quando executado

[1] Bacharel em Sistemas de Informação - URCAMP
[2] Prof. Me. do Curso de Sistemas de Informação da Universidade da Região da Campanha (URCAMP)

equivocadamente por seres humanos ou até mesmo por softwares, quando esses erros vêm a acontecer, podem afetar a estrutura das empresas de uma forma geral (GALVES, 2000).

I mprevistos e falhas são inevitáveis, mas o impacto destes, ou seja, o colapso da produção de um sistema, a interrupção no fornecimento do serviço, a perda de dados e a consequente falta de lucros, podem ser evitados pelo uso adequado de técnicas viáveis e de fácil compreensão.

O problema é que nem sempre as empresas conseguem entender e visualizar a importância dos dados e conteúdo que possuem para de fato criar um plano de contingência relevante de maneira a evitar problemas que podem surgir em um futuro distante. Com um investimento em um plano de contingência, esses problemas poderiam ser resolvidos aplicando nos momentos críticos da empresa.

As empresas normalmente hesitam na hora de adotar um plano de negócios ou um plano de contingência, pois geralmente tem consigo o medo da mudança e/ou o custo benefício. Devendo antes analisar a verdadeira condição da necessidade de introduzir as precauções com perdas, ainda podendo reduzir o impacto causado por incidentes que não poderiam ser evitados pelas medidas de segurança. O plano de contingência irá auxiliar na segurança da informação e reduzir problemas causados por situações inesperadas, como perdas de dados?

Algumas empresas possuem em seu ambiente de trabalho suas vulnerabilidades, sejam elas justificadas por erros humanos, de hardware e/ou software. Com isso, algumas vezes, o responsável pela tomada de decisão não consegue localizar de forma exata onde está surgindo o problema, seja ele, perda de informação, perda de conteúdo ou até mesmo um procedimento mal executado. Pensando nisso, o melhor método para prevenir e garantir a segurança da informação da empresa seria adotar um plano de contingência. Esse documento irá descrever o que precisa ser feito caso algum desses problemas aconteçam de fato. Para elaborar, faz-se necessário que se conheça e entenda a realidade da empresa e o que pode acontecer com a mesma. Sendo assim a empresa poderá prevenir

[1] Bacharel em Sistemas de Informação - URCAMP
[2] Prof. Me. do Curso de Sistemas de Informação da Universidade da Região da Campanha (URCAMP)

gastos desnecessários, gerar segurança de seus dados e conteúdo, podendo assim ter sempre um planejamento de segurança, onde a própria empresa define a melhor forma de manutenção, melhorias e procedimentos que irá adotar.

Dessa maneira o presente trabalho trata-se de um plano de contingência empresarial, desenvolvido para prevenção de perdas de conteúdo ou dados, os quais podem ser vulneráveis ao acesso externo, contemplando a empresa com um ambiente mais seguro e organizado. Tendo como principal objetivo, analisar a segurança da informação atual e desenvolver um plano de contingência para auxiliar uma empresa securitária. Sendo assim é necessário subdividir o processo em etapas para ser possível atingir o objetivo proposto, como: identificar as áreas de risco; conhecer a metodologia da empresa e funcionamento dos sistemas; averiguar a segurança de softwares; sugerir melhorias de segurança nos sistemas informatizados da empresa.

REFERENCIAL TEÓRICO

Segurança da informação

Conforme Beal (2005), a Segurança da informação é o processo de proteção da informação das ameaças a sua integridade, disponibilidade e confidencialidade. Com relação a Integridade da informação tem como objetivo garantir a precisão da informação, zelando que pessoas não autorizadas não possam alterar, adicionar ou remover, seja por forma intencional ou acidental. Já a Disponibilidade garante que só os autorizados a acessarem a informação possam executar comandos sempre que necessário e quando quiserem, (BEAL,2005).

Referente a Confidencialidade da informação é a segurança de que apenas pessoas autorizadas terão acesso a ela, resguardando de acordo com o alto nível de sigilo do seu conteúdo. Netto e Silveira (2007) acrescentam a estes objetivos a Legalidade, que é a garantia de que a informação foi desenvolvida em concordância com a lei; E também a Autenticidade, garantia de que em um método de

[1] Bacharel em Sistemas de Informação - URCAMP
[2] Prof. Me. do Curso de Sistemas de Informação da Universidade da Região da Campanha (URCAMP)

comunicação os remetentes consistem exatamente em o que dizem ser e que a informação não foi violada após o seu envio ou validação.

Netto e Silveira (2007) ainda definem a segurança da informação como: uma área do conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade. Ainda para os autores as empresas devem adotar um enfoque de gestão baseado nos riscos específicos para o negócio, com isso, os ativos da informação estarão protegidos de riscos e ameaças, mesmo que o custo e o nível de complexidade sejam elevados, ela irá manter seus níveis de confidencialidade, integridade e disponibilidade.

Segundo Moraes, Terence e Filho (2004), nenhuma empresa pode resistir aos efeitos causados pela revolução da informação. Sendo assim, as empresas devem entender que a informação é um item tão importante quanto os recursos humanos, pois está diretamente ligada ao sucesso ou fracasso das tomadas de decisões.

Simch e Tonetto (2007) salientam que hodiernamente a informação é um dos principais patrimônios da empresa e ainda assim estão diariamente sob risco e ataques constante. Diante da identificação das necessidades da empresa, o plano de contingência tem como sua estratégia a agilidade nos processos, de forma rápida e objetiva para que junto disso a empresa tenha o mínimo de prejuízo com relação aos gastos no período em que estiver em manutenção. Integrando como estratégia a redução de processos, resolvendo a situações eventuais que surgirem de uma forma sucinta, seguindo cada passo do plano de contingência sugerido. Ainda pode ser definido como estratégia dentro do plano, métodos com maior e menor relevância, adotando como maior relevância processos em que a empresa será afetada, podendo até mesmo parar de funcionar por conta do peso em que a contingência surgir e menor relevância métodos em que a empresa consegue ter tempo para resolver os eventos sem afetar o funcionamento como um todo.

[1] Bacharel em Sistemas de Informação - URCAMP
[2] Prof. Me. do Curso de Sistemas de Informação da Universidade da Região da Campanha (URCAMP)

Plano de Contingência

Segundo Fagundes et al (2010), o plano de contingência é peça fundamental para a segurança e privacidade de uma organização, pois assim estará completando o planejamento estratégico desta. Neste são colocados procedimentos e detalhes a serem seguidos nas tarefas de recuperação do ambiente de sistemas e negócios, de modo a minimizar o impacto causado por acidentes improváveis.

De acordo com Castro (2010), todas informações desempenham papéis importantes na definição e na execução de uma estratégia no plano de contingência. Com isso elas ainda ajudam na identificação das ameaças e das oportunidades para que cada empresa crie o cenário para uma resposta objetiva e mais eficaz no momento de execução. Para Silva et al (2007) um plano de contingência é umas das respostas para uma situação de emergência, como: operações de backup e recuperação de ativos atingidos por uma falha ou desastre. Assim tendo como objetivo o de assegurar a disponibilidade de recursos de sistema críticos, recuperar um ambiente avariado e promover o retorno à sua normalidade.

O Plano de Contingência é o documento escolhido para o trabalho, baseado nos estudos realizados, nele estão definidas as responsabilidades estabelecida em uma organização tendo como foco o atendimento de uma emergência e também por conter informações detalhadas sobre as características da área ou sistemas envolvidos. É um documento desenvolvido com o intuito de treinar, organizar, orientar, facilitar, agilizar e uniformizar as ações necessárias às respostas de controle e combate às ocorrências anormais. Assim, o plano de contingência está integrado com a tecnologia da informação abrangendo uma gama de produtos de hardware e software capazes de coletar, armazenar, processar e acessar números e imagens, que são usados para controlar equipamentos e processos de trabalho e conectar pessoas, funções e escritórios dentro das empresas e também entre elas (MORAES, TERENCE E FILHO, 2004).

Muitas organizações se dizem preparadas quando possuem um plano de contingência, porém é importante lembrar que o gerenciamento de continuidade são

[1] Bacharel em Sistemas de Informação - URCAMP
[2] Prof. Me. do Curso de Sistemas de Informação da Universidade da Região da Campanha (URCAMP)

coisas diferentes uma da outra. A contingência pode ser entendida como backup. Para a empresa que faz seu backup diariamente, pode se dizer que essa tem uma contingência. Porém em caso de ter que recuperar um backup, quanto tempo a organização vai esperar para voltar a atuar? Quanto menor este tempo, maior a continuidade que está sendo oferecida. (JUSSANI E LOPES).

Fases do Plano de Contingência

Para CELEPAR (2009), o processo de desenvolvimento de um plano de contingência eficaz pode ser dividido em seis etapas fundamentais: Identificação das necessidades; Avaliação de seu impacto; Seleção de medidas adequadas; Estratégias de recuperação; A construção e manutenção; Os testes e treinamentos.

Para que o plano possa ser escrito é necessário realizar previamente as seguintes reflexões de cada item abordado: No início do processo érealizada a identificação das necessidades, sendo essas relacionadas aos sistemas e métodos de utilização durante o serviço, assim sendo são anotados os principais pontos para o seguimento do plano. Na segunda etapa, é avaliado o impacto que o plano poderá causar, como por exemplo em casos de perda de dados, pode se dizer que o plano de contingência executado impactara na redução de tempo e valores. Após avaliar o impacto é descrita a seleção de medidas adequadas, essas serão descritas cada medida a ser executada, levando em consideração cada tipo de contingência que surgir, sem cruzar informações e procedimentos indevidos. Durante o processo são elaboradas as estratégias de recuperação, sendo uma delas o plano de backup, assim irão auxiliar no momento de turbulência para que a empresa e ou setores voltem a normalidade o mais breve possível seguindo os passos estabelecidos no plano. A construção e manutenção do plano, passa pela criação de todos passos abordados até a manutenção prévia, atualizando sempre que necessário quando as informações sofrerem alterações e atualizações mais novas. Os testes e treinamentos fazem parte da etapa final para concluir que o plano passou por todos

[1] Bacharel em Sistemas de Informação - URCAMP
[2] Prof. Me. do Curso de Sistemas de Informação da Universidade da Região da Campanha (URCAMP)

os testes sugeridos durante a criação e estabelecendo os treinamentos para que seja bem aplicado no momento de crise.

Tipos de Planos de Contingência

Para Silva et al (2009), na maioria das vezes mais de um plano faz-se necessário para complementar o plano de contingência, para cada processo do negócio um modelo de procedimentos é detalhado para atender a situação de contingência. Segundo Cassillhas (2008), um Plano de Continuidade de Negócios (PCN) A continuidade do Negócio e um processo essencialmente proativo, cujo planejamento visa preservar que uma organização resista a um desastre ou acontecimento inesperado que promova destruição ou faça estrago em algum de seus ativos críticos, colocando em risco quaisquer de suas funções chaves. Portanto, a Continuidade do Negócio visa a manutenção da operacionalidade da organização em um nível aceitável, previamente definido, em resposta a qualquer interrupção, quando provocada por incidentes.

Plano de Gerenciamento de Crises (PGC) este documento tem o propósito de definir as responsabilidades de cada membro das equipes envolvidas com o acionamento da contingência antes, durante e depois da ocorrência do incidente. Além disso, tem que definir os procedimentos a serem executados pela mesma equipe no período de retorno à normalidade. O comportamento da empresa na comunicação do fato à imprensa é um exemplo típico de tratamento dado pelo plano.

Plano de Continuidade Operacional (PCO) inclui o propósito de definir os procedimentos para contingenciamento dos ativos que suportam cada processo de negócio, objetivando reduzir o tempo de indisponibilidade e, consequentemente, os impactos potenciais ao negócio. Orientar as ações diante da queda de uma conexão à Internet, exemplificam os desafios organizados pelo plano.

Plano de Recuperação de Desastres (PRD) tem o propósito de definir um plano de recuperação e restauração das funcionalidades dos ativos afetados que

[1] Bacharel em Sistemas de Informação - URCAMP
[2] Prof. Me. do Curso de Sistemas de Informação da Universidade da Região da Campanha (URCAMP)

suportam os processos de negócio, a fim de restabelecer o ambiente e as condições originais de operação, no menor tempo possível.

METODOLOGIA

O presente estudo tem uma abordagem qualitativa, do tipo descritivo. Abordará e agregará informações não quantificáveis, levando em consideração os fatos obtidos nas entrelinhas das informações e sua subjetividade. Onde valores, crenças, emoções e atitudes deverão ser observados (MINAYO, 2010). Segundo Minayo (2010) as pesquisas qualitativas estimulam os entrevistados a pensarem livremente sobre determinado tema, atingem motivações não explícitas, ou mesmo conscientes, de maneira espontânea. Para a mesma autora a pesquisa qualitativa é favorável para revelar interações sociais pouco exploradas referentes a grupos particulares, propiciando a formação de novas abordagens e novas opiniões. A influência mútua entre o pesquisador e os sujeitos pesquisados é fundamental para a afirmação de vínculos e o entendimento das situações vivenciadas.

O estudo descritivo pretende apresentar com precisão os fatos e fenômenos de determinada realidade (TRIVIÑOS, 2006). O estudo do tipo descritivo permite ainda uma observação e uma análise detalhada dos episódios, no local onde eles ocorrem, objetivando produzir uma descrição minuciosa dos sujeitos do estudo (MINAYO, 2010). Para o trabalhado elaborado, foi feito uma pesquisa de qual seria a melhor forma de criação para o plano de contingência da empresa. Mediante isso foi adotado o modelo de plano de contingência da CELEPAR.

Caracterização do Estudo

O presente trabalho foi realizado em uma empresa do ramo comercial, especializada em seguros. Os sujeitos estudados serão os setores internos, equipamentos informatizados, especificamente softwares e banco de dados.

[1] Bacharel em Sistemas de Informação - URCAMP
[2] Prof. Me. do Curso de Sistemas de Informação da Universidade da Região da Campanha (URCAMP)

Conteúdos e informações no qual podem estar sujeitos a perdas e danos, tendo em vista a segurança dos dados e precaução de danos a empresa. Para garantir o anonimato dos sujeitos, estes não serão citados durante o estudo.

Para criar o plano de contingência, foi realizado um estudo em uma empresa securitária do ramo comercial da cidade de Bagé/RS, durante o período de setembro de 2016 a maio de 2017. Para isso foi realizada uma entrevista com o gestor da empresa sendo possível conhecer sua metodologia e informações nela contida. Esta é uma instituição privada, que tem como finalidade a venda de seguros de diversos ramos. Durante o período de estágio na empresa, os locais estudados foram setores das áreas informatizadas, pontos que podem ser de maior fragilidade, como: notebooks com softwares e equipamentos informatizados no qual fazem parte do trabalho da empresa. Com isso foi utilizado a metodologia de um plano de contingência, elaborando sugestões contra perdas ou falhas empresariais, baseados na parte de segurança e tecnologia da mesma.

Para participar da pesquisa os sujeitos obedecem aos seguintes critérios: ser uma empresa que trabalhe com dados internos e/ou externos; não ter um plano de contingência, trabalhar com software, banco de dados e componentes direcionados a sistemas da informação, principalmente direcionados a conteúdos privados. Tendo todos os critérios selecionados, foi estudado os pontos no qual aborda a criação do plano de contingência e segurança da informação, assim sugerindo informações e métodos para problemas específicos que podem ser evitados.

RESULTADOS

Mediante o estudo realizado foi necessário identificar as necessidades da empresa, sendo uma das principais necessidades a criação de backup e a criação de um plano de contingência. Ainda fazendo o processo de identificação, foi avaliado o impacto do plano na empresa, obtendo uma relevância considerável, levando em conta a agilidade nos processos e redução de tempo nas atividades paradas. As seleções de medidas adotadas foram: setores com pontos vulneráveis e

[1] Bacharel em Sistemas de Informação - URCAMP
[2] Prof. Me. do Curso de Sistemas de Informação da Universidade da Região da Campanha (URCAMP)

equipamentos informatizados com pouca segurança, assim sendo importadas todas informações para a criação de um plano, o método de consulta dos dados foi através de entrevista com o gestor da empresa. A tabela 01 a seguir aponta algumas necessidades encontradas na empresa a serem controladas, diante da ocorrência dos eventos que forem surgindo, ou seja, da efetivação do risco.

Tabela 01: Necessidades e Medidas

NECESSIDADES ENCONTRADOS	SELEÇÃO DE MEDIDAS
Treinamentos	-Criar treinamentos para softwares. -Informar atualizações aos colaboradores. -Organizar métodos para uso dos programas.
Falta de tonner	-Entrar em contato com a área de reposição da empresa e solicitar reabastecimento de tonner. -Efetuar procedimento de compra de um tonner reserva, para abastecimento imediato.
Site inoperante junto as companhias conveniadas	-Habilitar meio de contingência manual. -Entrar em contato com a cia via telefone para solucionar o problema do Link inoperante.
Roteador estragado.	-Substituir o roteador. -Elaborar e executar projeto de estabilização da rede elétrica.
Banco de dados (Backup)	-Instalar softwares específicos para detecção e prevenção de intrusão ao banco e sistema. -Manter backup dos dados diariamente. -Comprar Case para salvar dados em momentos de urgência.
Acessos no sistema	-Elaborar acesso pessoal para cada pessoa, em sistemas de uso comum. -Limitar acessos em software de uso especifico.
Contaminação por vírus.	-Realizar escaneamento para remoção de vírus. -Efetuar a atualização dos softwares antivírus e antispyware de modo a evitar a entrada de novos softwares maliciosos na rede.
Fim de contrato de licenciamento	-Verificar prazo para renovação de contrato. -Solicitar renovação do contrato de licenciamento.

Fonte: Dados Primários (2017**)**

Posteriormente foi criada as estratégias de recuperação, sendo estabelecidos métodos para serem seguidos nos momentos de crise, sendo um deles a instalação de software para proteção dos dados e descrevendo como um dos principais métodos a utilização de backup para recuperação do conteúdo em caso de perdas.

[1] Bacharel em Sistemas de Informação - URCAMP
[2] Prof. Me. do Curso de Sistemas de Informação da Universidade da Região da Campanha (URCAMP)

Diante de todos processos previamente realizados foi feita a criação do plano adotando todas medidas estudadas. Por fim o plano deverá passar por alguns testes e treinamentos, colocando todos os processos em prática, para concretizar que o plano de contingência está devidamente pronto para atender as necessidades.

Plano de Contingência para Empresa Securitária

O Plano de Contingência é o documento escolhido para o trabalho, baseado nos estudos realizados, nele estão definidas as responsabilidades estabelecida em uma organização tendo como foco o atendimento de uma emergência e também por conter informações detalhadas sobre as características da área ou sistemas envolvidos. É um documento desenvolvido com o intuito de treinar, organizar, orientar, facilitar, agilizar e uniformizar as ações necessárias às respostas de controle e combate às ocorrências anormais. Plano sugerido para empresa securitária, baseado na metodologia CELEPAR (2009), com procedimento adequados para eventos específicos da empresa, sendo elaborado para dar um auxilio nos momentos de crise.

[1] Bacharel em Sistemas de Informação - URCAMP
[2] Prof. Me. do Curso de Sistemas de Informação da Universidade da Região da Campanha (URCAMP)

Evento	Procedimentos
Perda de dados ou conteúdo	• Chamar profissional com conhecimento da área de informática; • Passar programa para tentar recuperar os dados perdidos; • Consultar backup para atualizar conteúdo perdido. Impacto: Recuperação dos dados para continuidade nos processos.
Evento	Procedimentos
Perda de dados ou conteúdo	• Chamar profissional com conhecimento da área de informática; • Passar programa para tentar recuperar os dados perdidos; • Consultar backup para atualizar conteúdo perdido. Impacto: Recuperação dos dados para continuidade nos processos.
Evento	Procedimentos
Armazenamento e Backup Procedimentos	• Criar servidor com capacidade de média/grande porte; • Fazer backup diariamente; • Consultar verificação da cópia de backup. Impacto: Guardar dados em grande volume e manter cópias para eventos de contingência.
Evento	Procedimentos
Proteção dos dados	• Instalar softwares de proteção; • Criar senhas, com: letras, números e caracteres especial; • Comprar HD externo para momentos de emergência.

[1] Bacharel em Sistemas de Informação - URCAMP
[2] Prof. Me. do Curso de Sistemas de Informação da Universidade da Região da Campanha (URCAMP)

	Impacto: Proteger o capital da empresa e prevenir perda de conteúdo.
Evento	Procedimentos
Internet/Rede	• Verificar cabeamento da rede; • Chamar profissional para verificar rede e distribuição da internet; • Ativar rede para uso. Impacto: Minimizar o tempo de espera sem conexão à internet.
Evento	Procedimentos
Vírus nos sistemas	• Executar programa de escaneamento para exclusão dos vírus; • Chamar profissional com conhecimento da área de informática; • Ativar antivírus com rastreamento diário. Impacto: Evitar que espalhe vírus nos sistemas e travamento dos equipamentos.
Evento	Procedimentos
Site/Sistema inativo	• Verificar se o problema é interno; • Ligar para empresa responsável pelo sistema; • Proceder de forma manual. Impacto: Reduzir o tempo de espera para continuidade de negócios.
Evento	Procedimentos
Acessos nos sistemas	• Cadastrar individualmente cada usuário • Limitar permissões de cada usuário; Impacto: Identificar usuários que cometem falhas e limitar usuários com permissões.
Evento	Procedimentos
Atualizações de sistema	• Atualizar para versão mais recente; • Manter sistemas atualizados. • Ligar para responsável da área; Impacto: Melhorar funcionamento de uso dos sistemas mais atuais
Evento	Procedimentos

[1] Bacharel em Sistemas de Informação - URCAMP
[2] Prof. Me. do Curso de Sistemas de Informação da Universidade da Região da Campanha (URCAMP)

Falta de toner para impressora	• Ligar para empresa que presta serviço • Solicitar recarga do toner • Comprar toner reserva Impacto: Reduzir o tempo de espera para impressões de documentos
Evento	Procedimentos
Contratos e Licenças	• Acompanhar prazo dos contratos e licenças de software; • Ligar para empresa responsável; • Renovar contratos dentro do prazo. Impacto: Manter documentos em dia sem parar os processos
Evento	Procedimentos
Treinamentos nos sistemas	• Ensinar usuários a manusear sistemas; • Criar treinamentos para usuários; • Treinar pessoas para substituir ausências. Impacto: Reduzir margem de erros dos usuários e manter colaboradores capacitados
Observações	• Manter lista de contatos a disposição de responsável de cada setor; • Definir períodos de treinamentos; • Escolher pessoas especificas para acessos nos sistemas; • Escolher profissional ou empresa para suporte; • Planilhas de contatos para responsáveis das cias; • Pasta com prazos de renovações dos contratos.

Fonte: Dados Primários (2017)

O plano de contingência deverá ser atualizado conforme os novos eventos que surgirem de acordo com o período que for usado, para que assim tenha relevância diante dos procedimentos sugeridos. Esses procedimentos podem ser

[1] Bacharel em Sistemas de Informação - URCAMP
[2] Prof. Me. do Curso de Sistemas de Informação da Universidade da Região da Campanha (URCAMP)

contidos no plano de contingência, visando evitar novas incidências, mitigando as vulnerabilidades dos riscos apresentados.

Fazendo uma análise do plano de contingência acima, conforme as necessidades identificadas e a seleção de medidas sugeridas, é possível orientar que um dos principais tópicos abordados na identificação é o backup de dados e a utilização dos sistemas, pois nesses abrange os dados da empresa, para isso foi sugerido algumas ações a serem feitas tendo como uma das principais a realização de backup diariamente, para reduzir a probabilidade de que algum evento posso prejudicar a empresa com a perda de informações.

CONSIDERAÇÕES FINAIS

O plano proposto foi o de otimizar a relação entre os diversos setores da empresa para que as medidas de proteção sejam bem executadas, tanto do ponto de vista interno quanto do ponto de vista externo para atender esse objetivo foi necessário identificar os principais processos de funcionamento da empresa, no ramo de seguros, identificar as dificuldades para a prevenção dos dados no modelo de plano desenvolvido e propor métodos para as principais dificuldades que foram encontradas na empresa.

Conforme sugestão, o novo modelo de plano de contingência trará agilidade para a recuperação dos setores quando afetados por algum problema, sendo atribuído métodos ágeis para que a empresa não pare com seu funcionamento e ao mesmo tempo tenha medidas de prevenção a seguir. Por fim, o plano de contingência proposto, poderá ajudar a empresa em relação as falhas e segurança de seus conteúdos, fazendo com que se tenha uma proteção melhor, sendo oferecido um questionário de métodos a seguir para os transtornos causados, para assim minimizar os danos aos colaboradores da empresa e seus respectivos setores. Ainda foi sugerido a aplicação do plano de contingência no local estudado, junto da proposta também foi sugerido a criação de uma área de TI.

[1] Bacharel em Sistemas de Informação - URCAMP
[2] Prof. Me. do Curso de Sistemas de Informação da Universidade da Região da Campanha (URCAMP)

REFERÊNCIAS

ABRAPP- Associação Brasileira das entidades fechadas de previdência complementar. Comissão Técnica Regional Sudeste de Governança da ABRAPP. Guia de boas práticas para planos de continuidade de negócios. São Paulo-SP. Disponível em: http://www.abrapp.org.br/Documentos %20Pblicos/guiaboaspraticas.pdf Acesso em: 20 nov. 2016.

ANDRADE, D, VINICIUS, E, MAFRA, G, FLÁVIO, L, HENRIQUE, M, SEPULVEDO, U, SILVA, E. Plano de contingência de ti: preparando sua empresa para reagir a desastres e manter a continuidade do negócio. **PósGraduação Em Segurança Da Informação, Faculdade Senac, Brasília-DF**, 2011.

CASSILHAS, I.A.P. Uma análise das atividades de teste de plano de continuidade de negócio e sua conformidade com a norma ISSO 17799:2005. Brasília, 2008. Disponível em:

https://dsic.planalto.gov.br/documentos/cegsic/monografias_1_turma/idilson_alexandre.pdf Acesso em: 22 nov. 2016.

CASTRO, V.S. Gestão da informação com sistemas informatizados - Um estudo de caso da secretaria de estado da saúde do Paraná. Curitiba-PR, 2010. Disponível em: http://www.bibliotecavirtual.celepar.pr.gov.br/arquivos/File/MonografiaseArtigos/Mono_Vanderlei.pdf Acesso em: 20 nov. 2016.

CELEPAR. Tecnologia Da Informação e Comunicação Do Paraná. Guia para Elaboração de Plano de Contingência Metodologia, 2009. Disponível em: http://www.documentador.pr.gov.br/documentador/pub.do?action=d&uuid=@g tf-escriba@4938adcd-20be-4a6c-b14a-ae05505a9b1b.Acesso em: 10 nov. 2016.

[1] Bacharel em Sistemas de Informação - URCAMP
[2] Prof. Me. do Curso de Sistemas de Informação da Universidade da Região da Campanha (URCAMP)

FAGUNDES, L.L, KARL, F, BAPTISTA, L, ROSA, R.S. Estratégias deContingência para Serviços de Tecnologia da Informação e Comunicação. Universidade do Vale do Rio dos Sinos – UNISINOS. **X Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais**. Disponível em: http://ceseg.inf.ufpr.br/anais/2010/04_minicursos/minicurso_06.pdf Acesso em: 22 nov. 2016.

FREITAS, T.R. Plano de contingência de negócios e serviços. 2013. **Dissertação, Universidade Tecnológica Federal Do Paraná, Departamento Acadêmico De Eletrônica, Curso Superior De Tecnologia Em Sistemas De Telecomunicações, Curitib**a, 2013. Disponível em:http://repositorio.roca.utfpr.edu.br/jspui/bitstream/1/3025/1/CT_COTEL_2013_2_01.pdf Acesso em: 17 nov. 2016.

Fundação Santo André - Pós-Graduação em Sistemas de Informações. Gerência de Informática. Disponível em: http://www.sardano.net/turma98/Linear1/index.html Acesso em: 18 nov. 2016.

GALVES, J.W.G. Planos de contingência em TI. Disponível em: www.techoje.com.br/site/techoje/categoria/abrirPDF/219 Acesso em: 24 nov. 2016.

GORAYEB, D.M.C. Gestão de Continuidade de Negócios aplicada no ensino presencial mediado por recursos tecnológicos. **Dissertação. São Paulo-SP**, 2012. Disponível em: www.teses.usp.br/teses/disponiveis/3/.../Dissertacao_Diana__M_da_C_Gorayeb.pdf Acesso em: 20 nov. 2016.

Grupo de Segurança da Informação. A Importância do Plano de Continuidade de Negócios. Disponível em: http://iso27000.com.br/ Acesso em: 16 nov. 2016.

JUSSANI, P.H, LOPES, L.F.B. Plano de contingência de banco de dados.**Universidade Paraense-UNIPAR. Paranavaí-PR**. Disponível em:

[1] Bacharel em Sistemas de Informação - URCAMP
[2] Prof. Me. do Curso de Sistemas de Informação da Universidade da Região da Campanha (URCAMP)

http://docplayer.com.br/13604969-Plano-de-contingencia-de-banco-dedados.html Acesso em: 16 nov. 2016.

MARINHO F. Plano de Contingência, Continuidade ou Recuperação de Desastres? O que é mesmo que você precisa? Disponível em: http://blogsucessoempresarial.com/lano-de-contingencia-continuidade-ourecuperacao-de-desastres-o-que-e-mesmo-que-eu-preciso/ Acesso em: 27 nov. 2016.

MORAES G.D.A, TERENCE, A.C.F, FILHO, E.E. A tecnologia da informação como suporte à gestão estratégica da informação na pequena empresa. **Revista de Gestão da Tecnologia e Sistemas de Informação**. Vol. 1, No. 1, pp. 27-43. São Paulo-SP, 2004. Disponível em: http://www.scielo.br/pdf/jistm/v1n1/03.pdf Acesso em: 20 nov. 2016.

NETTO, A.S, SILVEIRA, M.A.P. Gestão da segurança da informação: fatores que influenciam sua adoção em pequenas e médias empresas. **JISTEM - Journal of Information Systems and Technology Management**. vol.4, no.3. São Paulo-SP, 2007. Disponível em:

RAMOS R. Plano de Contingência. Disponível em:http://www.infoescola.com/administracao_/plano-de-contingencia/ Acesso em: 19 nov. 2016.

RAZA, C. Sua empresa tem um plano de contingência? Ou plano B? Disponível em: http://www.administradores.com.br/artigos/tecnologia/suaempresa-tem-um-plano-de-contingencia-ou-plano-b/11466/ Acesso em: 17 nov. 2016.

SILVA, R, MOURA, V.C, DEPONTI, E, ROSA, V. Plano de Continuidade de Negócios. **Universidade Católica de Brasília (UCB) Brasília-DF**. Disponível em: http://iso27000.com.br/index.php?option=com_content&view=article&id=52:importpcn&catid=34:seginfartgeral&Itemid=53 Acesso em: 28 nov. 2016.

[1] Bacharel em Sistemas de Informação - URCAMP
[2] Prof. Me. do Curso de Sistemas de Informação da Universidade da Região da Campanha (URCAMP)

SILVEIRA, M.F.R, CARVALHO, M.A.A. A importância da auditoria de plano de contingência**. Faculdades Integradas Antônio Eufrásio de Toledo**, Presidente Prudente-SP, 2012. Disponível em: http://intertemas.unitoledo.br/revista/index.php/ETIC/article/viewFile/3933/3696 Acesso em: 10 nov. 2016.

SIMCH, M.R.V, TONETTO, T.S. Auditoria dos sistemas de informação aliada à gestão empresarial. Disponível em: https://periodicos.ufsm.br/contabilidade/article/view/39 Acesso em: 21 nov. 2016.

[1] Bacharel em Sistemas de Informação - URCAMP
[2] Prof. Me. do Curso de Sistemas de Informação da Universidade da Região da Campanha (URCAMP)