FACULDADES INTEGRADAS DE CARATINGA

FACULDADE DE CIÊNCIA DA COMPUTAÇÃO

SEGURANÇA DA INFORMAÇÃO: CONTINGÊNCIA E GESTÃO DA INFORMAÇÃO EM EMPRESAS

WESLLEY JEFERSON PINTO

CARATINGA

2012

Weslley Jeferson Pinto

Segurança da Informação: Contingência e Gestão da Informação em Empresas

Monografia apresentado à Faculdade de Ciência da Computação das Faculdades Integradas de Caratinga como exigência parcial da disciplina de Trabalho de Conclusão de Curso I, sob orientação da professora Msc. Fabrícia Pires Souza Tiola.

CARATINGA

2012

Weslley Jeferson Pinto

Segurança da Informação: Contingência e Gestão da Informação em Empresas

Monografia submetida à Comissão examinadora designada pelo Curso de Graduação em Ciência da Computação das Faculdades Integradas de Caratinga como requisito para obtenção do grau de Bacharel.

_____

Prof. Msc. Fabrícia Pires Souza Tiola

Faculdades Integradas de Caratinga

_____

Prof. Msc. Jacson Rodrigues Correia da Silva

Faculdades Integradas de Caratinga

_____

Prof. Msc. Míriam de Souza Monteiro

Faculdades Integradas de Caratinga

Caratinga, 10/12/2012

AGRADECIMENTOS

Agradeço primeiramente a Deus por me guiar e sustentar para chegar até aqui, a minha família por sempre me apoiar e me dar forças para conquistar meus objetivos.

Minha gratidão aos professores que, com muita paciência e atenção, nos passaram o conhecimento, a turma por todos os obstáculos vencidos e todos os momentos bons juntos.

"A provação vem, não só para testar o nosso valor, mas para aumentá-los; o carvalho não é apenas testado, mas enrijecido pelas tempestades"

(Lettie Cowman)

RESUMO

Atualmente as empresas estão cada vez mais dependentes de sistemas computacionais, de bancos de dados e de tecnologias de informação e comunicação. A informação é um ativo imprescindível para os negócios das empresas na atual sociedade e como consequência disso deve ser protegida tornando assim, fundamental que essas empresas invistam na segurança da sua informação.

Para agregar valor às empresas a informação deve ser protegida e mantida de forma confidencial, íntegra e disponível para acesso de seus funcionários. Para garantir tais características são propostas metodologias, normas e boas práticas as quais auxiliam na elaboração de uma política de segurança da informação. Tais políticas são utilizadas para prever, avaliar e indicar medidas caso haja alguma ocorrência com sistemas, equipamentos ou as informações das empresas. Este plano é denominado Plano de contingência.

Um plano de contingência deve ser implementado proporcionando políticas que visem alta disponibilidade de suas informações nas quais o objetivo é garantir que o acesso à informação seja eficiente, seguro em quaisquer máquinas de acesso a rede e proteger todos os equipamentos de TI (Tecnologia da Informação) de qualquer tipo de tragédias ou incidentes.

O objetivo principal deste trabalho é fazer um levantamento sobre o conhecimento das normas e a aplicação de metodologias de segurança da informação em empresas da cidade de Caratinga/MG. Sabe-se que esta cidade já foi acometida de fenômenos da natureza como enchentes que resultaram grandes prejuízos a sociedade.

Com este estudo pode ser avaliado a preocupação das pessoas em relação à proteção das informações e indicar aos profissionais da TI o atual cenário que as empresas do município se enquadram, podendo levar às organizações, indicadores e reflexões sobre a importância de uma política de segurança da informação e o papel de cada funcionário envolvido nela, dando ênfase a sua obrigação de zelador destes dados.

Palavras Chaves: informação, segurança da informação, contingência da informação, gestão de TI.

ABSTRACT

Nowadays, the companies are each time more dependant of computer systems, data Banks and informations Technologies and communications. Information is an indispensable asset for business in the current society's companies and as a consequence of that, it should be protect, thus making, primordial for those companies invest in security of information.

To assemble value to the companies, the information should be protected and kept confidential, in full, available for its employees access. To ensure such features, methodologies are proposed, standards and best practices which assist in the elaboration of an information security politic. Those politics are used to foresee, evaluate and indicate paths if any occurrence with systems, equipment or information of companies happens. This plan is called a contingency plan.

A contingency plan should be implemented providing politics which aim high availability of its information in which the goal is ensure that the access to the information be efficient, secure in any machines with network Access and protect all the equipments of IT (information technology) from any kind of tragedy or incident.

The main purpose of this work is to do a survey about the knowledge of the Standards and the application of methodologies of information security in companies from Caratinga/MG. It is known that this city has already been affected for natural phenomena such as floods resulting in large losses to society.

Through this study, people's concern about the protection of information can be evaluated and indicates to the IT professionals the current scenario in which companies of this county are fit, leading to the organizations, indicators and reflections about the importance of a politic of information security and the role of each employee engaged in it, emphasizing their obligation as a keeper of those data.

Keywords: information, information security, information contingency, IT management.

LISTA DE ILUSTRAÇÕES

LISTA DE GRÁFICOS

LISTA DE SIGLAS

TI	TECNOLOGIA DA INFORMAÇÃO
SGSI	SISTEMA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO
ERP	ENTERPRISE RESOURCE PLANNING
ACL	ACCESS CONTROL LIST

SUMÁRIO

1. INTRODUÇÃO

Há aproximadamente duas décadas o mundo entrou no auge da era da informação com surgimento de equipamentos avançados e o uso da Internet como uns dos principais meios de comunicação utilizada pela população. A Internet expandiu o conhecimento da humanidade, fornecendo acesso rápido e fácil as informações, possibilitando a qualquer pessoa se comunicar com outras pessoas em qualquer lugar do mundo.

A Internet contribui e muito na prestação de serviços, garantindo assim a qualidade destes, possibilitando uma visão de futuros negócios e agilidade na busca de informações, sendo importante para a continuação dos negócios. Ela é uma base para as melhorias e pode indicar novas oportunidades de negócios para uma empresa e, por isso, é alvo constante de ataques por pessoas mal-intencionadas e que buscam uma certa vantagem sobre a sua concorrência.

Por ser um ativo, a informação é importante para as empresa, devendo ser guardada com total zelo pelas organizações. Para Silva, Carvalho e Torres (2003) todas as medidas de segurança independentemente do seu objetivo, necessitam serem implementadas antes da concretização do risco, ou seja, antes do incidente ocorrer. A segurança da informação é feita previamente, portanto, é necessário levantar os riscos e vulnerabilidades de uma rede de uma empresa e tomar medidas cautelares evitando uma exploração desta falha por parte de algum usuário ou invasor. Segundo Boran (1996), existem três princípios básicos que garantem a segurança da informação: Confidencialidade; Disponibilidade; Integridade.

Existe vários modelo de contingência. A contingência da informação consiste em uma prevenção de um fator de risco que pode acontecer. Tem como objetivo recuperar um sistema após um desastre através de medidas previamente realizadas, como operações de *backup,* portanto, deve-se criar um modelo de contingência adequado para cada tipo de empresa, na qual cada empregado tenha um papel a desenvolver.

Um plano de contingência é importante para a continuidade dos negócios de uma corporação, segundo Andrade et al (2011) ele é dividido em três planos complementares: Plano de Administração de Crise que tem como objetivo definir tarefas a serem executadas até o retorno do sistema da empresa; Plano de Continuidade Operacional que, tem a finalidade organizar procedimentos que possibilitem a continuidade das operações no

período em que o sistema sofreu um desastre; Plano de Recuperação de Desastres que tem como objetivo garantir a integridade dos dados e a recuperação do sistema.

Para o sucesso de uma política de segurança da informação é necessário uma combinação de diversos elementos, como os sistemas utilizados pela corporação, a estrutura da empresa, o envolvimento e o comportamento dos funcionários desta empresa, já que todos são partes importantes dessa política.

Este trabalho apresenta como a gestão de TI é tratada em corporações, como ela protege suas informações e seus equipamentos, sobre a necessidade de proteger melhor as redes para evitar prejuízos, de investir e motivar funcionários para adquirir um melhor conhecimento sobre riscos e ameaças de um determinado sistema e sobre criação de políticas de segurança da informação mais eficientes.

Para isso, foi elaborado um questionário e aplicado à algumas empresas. Após o levantamento das medidas adotadas por cada uma e estudo delas, o objetivo é discutir a real situação do plano de contingência da informação, política de segurança da informação e como agem quando há um momento de crise ou falha do sistema, apontando assim, as principais características do modelo de contingência implantado, conscientizando sobre a importância de uma política de segurança da informação eficaz e adoção de medidas preventivas.

O trabalho irá apresentar um estudo sobre os conceitos necessários para elaboração de uma boa política de segurança da informação em seu referencial teórico; em metodologia será apresentado como foi feita a pesquisa para descobrir como cada empresa se protege e guarda a suas informações, como os dados colhidos foram tratados e qual ferramenta utilizada para a coleta de dados; por fim, em resultados será apresentado todos os dados obtidos pela pesquisa e após um cruzamento com o referencial teórico será apontadas possíveis melhorias.

2. REFERÊNCIAL TEORICO

2.1. A INFORMAÇÃO

A informação tem um valor altamente significativo e pode representar grande poder para quem a possui. Este valor se refere a processos, pessoas e tecnologias (LAUREANO, 2005). A informação é um dado interpretado e, seu uso pode agregar valores a uma pessoa, através de jornais, televisão, revistas e outros. Mas para isso é necessário compreender o que aquele dado representa. A interpretação de um dado pode ser uma tarefa complicada a partir do momento em que não tem conhecimento dos meios, como por exemplo, uma pessoa que nunca teve conhecimento de finanças poderá ter problemas ao tentar entender um documento de controle de caixa.

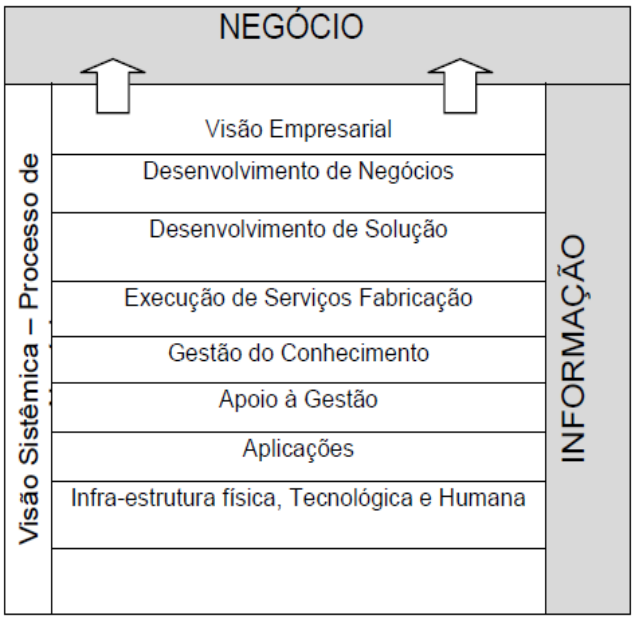


Figura 1: A importância da informação na empresa
Fonte: da Silva (2009)

A Figura 1 apresenta a informação nos processos de negócios de uma empresa, nas quais a infraestrutura física, tecnológica e humana, serve como base para continuação dos negócios que esta empresa realiza, gerando ao final, uma visão empresarial mais ampla que possibilitará o sucesso de seu comércio.

A classificação da informação é importante para que as organizações possam determinar o nível de proteção das suas informações, de modo que a segurança das informações importantes para as organizações possa ser garantida (SPANCESKI 2004).

Nas corporações, as informações tem o poder de fazer grandes negócios, ela é um bem crucial para a empresa. Segundo Boran (1996), elas são classificadas em quatro níveis:

- Secreta – São informações importantes para os negócios de uma empresa e é acessada por um nível muito restrito de pessoas de forma a mantê-la sempre íntegra;
- Confidencial – São informações que devem ficar apenas no ambiente empresarial, o seu acesso pode ser feito para o desempenho satisfatório por parte de seus usuários;
- Interna – Essas informações devem ser utilizadas apenas no ambiente corporativo;
- Pública – As informações públicas podem ser acessadas por qualquer pessoa, sendo ela cliente, usuários internos da empresa e/ou qualquer pessoa interessada nela.

2.2. **POLÍTICA DE SEGURANÇA DA INFORMAÇÃO**

Pelo o fato da informação de uma empresa ter um valor altamente significativo, é importante que haja um investimento na sua proteção. Com o aumento da tecnologia e as facilidades de adquirir um computador, cada dia que passa mais pessoas se interessam em invadir sistemas. Com isso, diariamente centenas de empresas sofrem ataque e quando bem sucedidos podem causar grandes prejuízos as estas empresas, corrompendo e/ou alterando seus dados, podendo até levá-las a falência.

Segundo da Silva (2009), um sistema pode ser ameaçado de várias formas como: acidentes naturais, fogo, enchentes, descargas elétricas, entre outros. Portanto, para traçar uma política de segurança da informação eficiente, é necessário identificar o que se deve proteger e levantar tudo que pode ameaçar essa rede; tanto quanto ao patrimônio da empresa, como: vigilância contra roubos, aonde esta empresa se localiza e seus riscos naturais, entre outros; como também em nível de softwares, como: quais serão o meio de acesso a informação, quais funcionários podem usa-las, quais podem modifica-la, etc. Ainda de acordo com da Silva (2009), a segurança da informação depende primeiramente de uma análise de risco (vulnerabilidades + ameaças).

A participação de todos os funcionários da empresa também é importante na implantação de uma de segurança da informação. Afinal, a disponibilidade e a integridade das informações é de total responsabilidade de quem a utiliza e com qualquer erro humano pode causar grandes perdas da informação a esta empresa e ainda, no momento de possíveis auditorias dos dados que trafegam na rede, a falta de conhecimento dos funcionários com relação à política de segurança existente podem acarretar em processos judiciais, pois, todas as informações pessoais deste funcionários poderá ser analisados pelo administrador da rede.

Conforme Simch e Tonetto (2008), para manter a informação segura, se faz necessário elaborar, divulgar e manter atualizado o documento que descreve a política de segurança da informação. Portanto, a contínua revisão dos processos e o acréscimo de possíveis melhorias se fazem necessário a uma política de segurança, que dever ser bem clara, flexível e abrangente e de forma suportar possíveis alterações no futuro.

De acordo com a ABNT NBR ISO/IEC 27000 (2006), a segurança da informação e caracterizada pela prevenção da:

- Confidencialidade – garantir que as informações sejam acessíveis apenas aqueles autorizados a terem acesso;
- Integridade – salvaguardar a exatidão e inteireza das informações e métodos de processamento;
- Disponibilidade – garantir que os usuários autorizados tenham acesso as informações e ativos associados quando necessários. ABNT NBR ISO/IEC 27000 (2006).

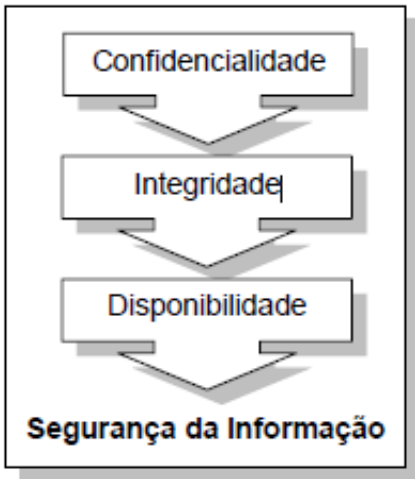


Figura 2: Classificação da Informação
Fonte: Da Silva (2009)

A Figura 2 apresenta que os três pontos cruciais da segurança da informação que se deve manter a informação de uma empresa acessível apenas aos integrantes da mesma, confiável e sempre disponível para usuários autorizados, garante uma politica de segurança da informação bem estruturada, possibilitando a continuidade dos negócios da empresa e gerando mais ativos seguros para esta rede.

Existem várias formas de uma empresa criar uma política de segurança da informação, uma delas é a certificação através da ABNT NBR ISO/IEC 27000. Também conhecida como "Gestão de Segurança da Informação – Especificação e diretrizes para uso", a ABNT NBR ISO/IEC 27000 é um conjunto de normas e especificação de requisitos para a criação, implementação, monitoramento, revisão, manutenção e melhorias do sistema de gestão de TI.

2.3. **METODOLOGIAS DE SEGURANÇA DA INFORMAÇÃO**

Para uma melhor qualidade de serviços prestados por parte das empresas, é de extrema importância que haja um grande investimento na área de segurança e um plano de acesso nas quais apenas pessoas autorizadas podem acessar esses ativos. Segundo Luz

(2010), a informação pode existir e ser manipulada de diversas formas, ou seja, por meio de arquivos eletrônicos, mensagens eletrônicas, Internet, bancos de dados, em meio impresso, verbalmente, em mídias de áudio e de vídeo etc.

> O planejamento da política de segurança deve ser feito tendo como diretriz o caráter geral e abrangente de todos os pontos, incluindo as regras que devem ser obedecidas por todos. Essas regras devem especificar quem pode acessar quais recursos, quais são os tipos de usos permitidos no sistema, bem como os procedimentos e controles necessários para proteger as informações. (DA SILVA, 2009).

É importante que haja um levantamento das informações contidas em uma rede empresarial e que seja feito um plano de segurança da informação que torne as tentativas de invasão a esta rede, inviável para o intruso. Também tornar-se importante estabelecer uma lista de serviços que esta rede terá, quais setores podem acessá-la e quem administrará esses serviços. Segundo Dias (2010) é importante que a política estabeleça ainda as responsabilidades das funções relacionadas com a segurança e discrimine as principais ameaças, riscos e impactos envolvidos.

Quanto aos serviços que uma rede corporativa pode oferecer, existem duas metodologias que podem ser adotadas pelo administrador da rede, a primeira é bloquear todos os serviços e ir liberando de acordo com a necessidade de uso. Esta forma é muito mais segura, pois, o administrador saberá exatamente o que está liberado na rede, mas esta requer mais trabalho na parte de configuração. Outra forma é permitir tudo e ir bloqueando o que não se faz necessário. Esta forma é menos segura porque todos os buracos do sistema ficam aparentes, porem é mais fácil a sua configuração.

> Em um país, temos a legislação que deve ser seguida para que tenhamos um padrão de conduta considerado adequado às necessidades da nação para garantia de seu progresso e harmonia. Não havia como ser diferente em uma empresa. Nesta, precisamos definir padrões de conduta para garantir o sucesso do negócio. (LAUREANO, 2005).

As leis servem para lembrar ao cidadão de uma nação o que é certo ou errado de se fazer, dando como retorno a este país, possibilidades de progresso diante de uma ordem. Como uma nação, uma corporação deve criar padrões de condutas para o uso e manipulação de suas informações que deverá ser seguida por todos os funcionários da

empresa, garantindo assim, um progresso harmônico da mesma, e possibilitando uma ampliação de seus negócios no futuro.

Uma política de segurança da informação deve atender vários propósitos, como descrever: o que está sendo protegido e o porquê; o que deve ter prioridade; os riscos que ameaçam uma rede, tanto físico como lógicos; condutas de usuários e hierarquias para acesso das informações. A partir destes propósitos é possível criar boas práticas de uso da informação, nas quais todos os funcionários terão funções específicas a fazer em uma rede corporativa, acesso apenas ao que lhe é permitido e prevenção de perdas, pois todos os dados possivelmente corrompidos terão os registros de quem o fez.

2.4. **CONTINGÊNCIA DA INFORMAÇÃO**

O plano de contingência consiste em levantar incidentes que uma rede empresarial pode sofrer, e trabalhar na prevenção e na recuperação deste sistema caso esses incidentes ocorram. Por exemplo, em uma empresa onde pode haver o risco de inundação e, consequentemente, perdas de equipamentos, seu plano de contingência deve apresentar um procedimento de como prevenir e como agir nesta situação.

> O plano de contingência é composto pelos planos onde estão definidas as respostas iniciais a um incidente por parte de todas as áreas da Empresa, quer este ocorra com ou sem aviso prévio. Incluem todos os procedimentos de emergência, descrição das equipes que os executam, informação facilitadora da execução e indicação dos eventos que despoletam os procedimentos. (SILVA, CARVALHO E TORRES 2003).

Para Andrade et al (2011) o plano de contingência é divido em três partes: O plano de Administração de Crise, o Plano de Continuidade Operacional e o plano de recuperação de desastre. A definição dos mesmos, segundo este autor são:

- Plano de Administração de Crise: O seu principal objetivo é definir, passo a passo o funcionamento das equipes e os procedimentos a serem executados até o retorno das atividades durante um desastre em uma empresa;
- Plano de Continuidade Operacional: Tem como finalidade prover a organização de procedimentos, controles e regras que possibilitem a continuidade das operações, ou seja, manter as operações vitais de uma organização, mesmo na eventualidade de um desastre em suas instalações, minimizando perdas de negócios e impactos na entrega de produtos e serviços aos seus clientes e usuários;
- Plano de Recuperação de Desastres: Para assegurar a continuidade do negócio é necessário mitigar os riscos, porém é impossível eliminar todas as vulnerabilidades de um sistema, principalmente de um sistema de grande porte, e, além disto, há situações que não podem ser facilmente previstas, o que justifica a criação de um plano de recuperação de desastres, este, deve oferecer a descrição das ações necessárias para a retomada dos serviços, ou ao menos os serviços críticos, descrevendo os passos para disponibilizar os ativos envolvidos no desastre. (ANDRADE et al, 2011).

Esses três planos complementares definem o que fazer antes, durante e depois de um desastre a um sistema, especificando o que cada indivíduo da empresa deve fazer quando ocorre uma situação de perda de sistema e como recuperá-lo causando o mínimo de prejuízo possível a esta corporação.

Com o avanço da tecnologia, a necessidade de eficiência em serviços prestados tendo como consequência a informatização das empresas faz com que bons planos de contingência sejam criados para prevenir uma corporação de grandes perdas no caso de um desastre. O aumento de pessoas com acesso e interesse em disciplinas na área da informação também se torna uma grande ameaça, pois com acesso a um sistema exposto e conhecimento, o invasor pode causar grandes prejuízos. O Plano de Contingência norteia a organização no sentido de prevenção de incidentes bem como a recuperação em caso de desastres e em momentos de crise (ANDRADE et al, 2011). O número de ameaças a uma rede empresarial aumenta a cada dia, aumentado a preocupação com sistemas expostos durante certo tempo. A revisão destes planos é essencial para a continuidade dos serviços prestados por essas corporações (DA SILVA, 2009).

Mas contingência da informação não consiste em apenas proteger a infraestrutura da rede contra desastres e a parte lógica de invasores, ou mesmo de funcionários com

intenções não boas, a proteção contra roubos também é importante. Um equipamento roubado pode causar grandes prejuízos a uma empresa, não só pelo custo do patrimônio, mas também pela perda de informações que este equipamento pode ter em sua mídia de armazenamento, mesmo que o ladrão não consiga acessá-la.

Empresas que se preocupam com a segurança da sua informação investem em equipamentos de vigilância 24 horas, para inibir ladrões e funcionários que queiram, de alguma forma, prejudicar a empresa. E até mesmo no caso de houver a consumação do fato, aumentar as suas possibilidades de recuperação de seus equipamentos.

2.5. **NORMAS DE SEGURANÇA**

Com intuito de auxiliar pessoas e empresas a criarem redes mais seguras, as normas de segurança da informação definem regras, padrões de boa condução no momento da elaboração e manutenção de uma politica de segurança e para certificações na área, em todo mundo.

Uma norma muito utilizada por parte das empresas na qualificação de funcionários de segurança da informação e na implementação, implantação, manutenção e auditoria de um SGSI (Sistema de Gestão de Segurança da Informação), é a ISO 27001.

Esta norma adota um modelo chamado de PDCA, ou *Plan-Do-Check-Act*, que é a divisão da mesma em quatro etapas em forma de um círculo perpetuo, sendo elas: planejar, fazer, checar e agir (Figura 3). Faz uma abordagem de forma a encorajar seus usuário a entenderem sobre os requisitos de segurança da informação de uma determinada empresa e a importância de se estabelecer uma politica de segurança da informação, baseando-se nos riscos no contexto de negócios que a corporação possui, criando assim, critérios para o uso de equipamentos e sistemas passando a eles, uma certa segurança quanto a confidencialidade e a integridade das informações.

Outro ponto, também abordado por esta norma, diz a respeito da manutenção e eficácia do SGSI. É de suma importância a verificação periódica da política de segurança da informação das empresas. Os investimentos e incentivo por parte dos empresários, em treinamentos de pessoal para lidar com situações de riscos e a verificação de ataques à rede ou mesmo aos sistemas ocorridos, riscos físicos aos equipamentos, como por exemplo,

roubos e incêndios, entre outros, e a analise crítica de tudo isso, pode ser muito proveitoso e resultar em bons frutos para a empresa e para o SGSI.

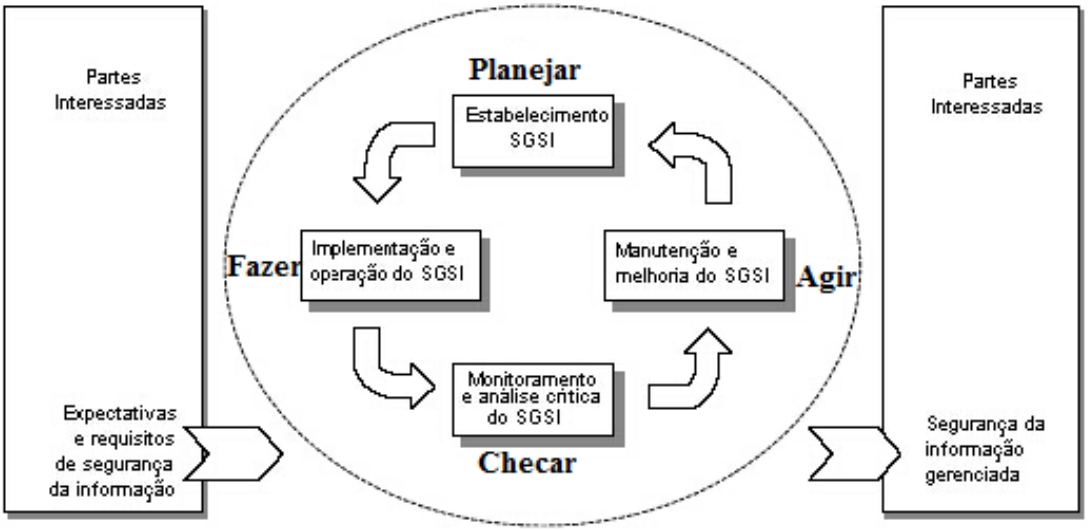


Figura 3: Modelo PDCA implantado em uma SGSI
Fonte: ABNT NBR ISO/IEC 27000 (2006)

Como pode ser visto na Figura 3, o modelo PDCA da norma ABNT NBR ISO/IEC 27000 consiste um círculo dividido em quatro fases do SGSI, na qual a cada iteração resultará em uma melhora da política de segurança da informação. A primeira fase deste círculo é o planejamento, nesta fase será estabelecida uma política ou mesmo um processo a um SGSI. A fase denominado fazer, se implementa a política ou a adição que será feita. A próxima fase trata-se de checar, que é medir e avaliar esse processo e dar um retorno de sua viabilidade. Na ultima fase, agir é onde executa as correções tendo como base os resultados obtidos na fase anterior.

Outra norma utilizada é a ABNT NBR ISO/IEC 17799 (2005). Esta norma possui as principais referências sobre segurança da informação com exemplos desde como elaborar uma política de segurança da informação, até exemplos práticos e implantação da mesma. Faz também uma abordagem sobre o risco que podem ameaçar a informação contida em uma rede apresentando, como fazer uma avaliação e formas possíveis de se tratá-lo.

Assim como as duas ISOs brevemente apresentadas, há outras normas que podem auxiliar empresários a melhorarem seus sistemas de segurança da informação. A segurança

da informação, por ser um setor da empresa que não apresenta um lucro direto, é deixado de lado por muitos empresários, facilitando assim para pessoas má intencionadas a exploração, modificação e roubo de informações na rede e tendo como consequência perdas irreparáveis e grandes prejuízos.

2.6. **BACKUP E RESTAURAÇÃO DO SISTEMA**

O *backup* é uma forma de manter os arquivos de uma empresa íntegros e diminuir os riscos de perda, contudo, é preciso criar critérios do que se deve ser copiado e qual sua importância. Um desses critérios é o tempo que este *backup* ficará armazenado. Sendo importante mantê-lo durante tempo suficiente para que um possível dano em alguma informação seja percebido por alguém. Outro critério é sobre o período que será feito o *backup*. Ele deve ser feito periodicamente e devem-se testar os procedimentos de restauração, garantindo assim a continuidade do funcionamento deste sistema. Existem programas que auxiliam na criação de cópias de arquivos. É importante criar critérios e recomendações para *backup* e recuperação das informações de uma rede empresarial, garantindo a integridade, disponibilidade e confidencialidade, relacionadas à segurança. (DA SILVA, 2009).

Deve-se guardar em local seguro, pelo menos uma cópia do *backup*. Caberá ao responsável pela rede identificar e monitorar o tempo de vida do mesmo. Existem os sistemas de *backup* e *recovery*, isto é, os dados mais importantes devem possuir cópias evitando transtorno em caso de acontecimentos inesperados, verificando sempre se essas cópias estão seguras evitando problemas (LAUREANO, 2005).

É importante que uma empresa invista em mídias para *backup*, uma vez que esse processo é muito importante na contingência de suas informações. Como toda informação é ativa, uma empresa sofre diariamente um crescimento, tornando-se necessárias mídias de gravações de dados mais ágeis para fazer o *backup*.

3. METODOLOGIA

A seguir será detalhado o método utilizado para se descobrir como algumas corporações se protegem e guardam a suas informações. Políticas de segurança da informação utilizadas pelas empresas; conhecimentos de seus funcionários de gestão de TI; nível de investimentos, preocupação e conhecimento do assunto por parte de seus diretores e seus sistemas e recursos de TI.

3.1. EMPRESAS ENTREVISTADAS

Para descobrir a situação da segurança da informação das empresas da região de Caratinga, foi realizada uma entrevista com um questionário que aborda como estas tratam a área de TI e suas metodologias de manipular e proteger seus dados. O questionário foi aplicado no mês de outubro do corrente ano, em treze empresas que atuam em diversos segmentos como: comércio, tecnologia, prestação de serviço e governamental. Foram escolhidas as empresas de mais destaque em suas respectivas áreas de atuação.

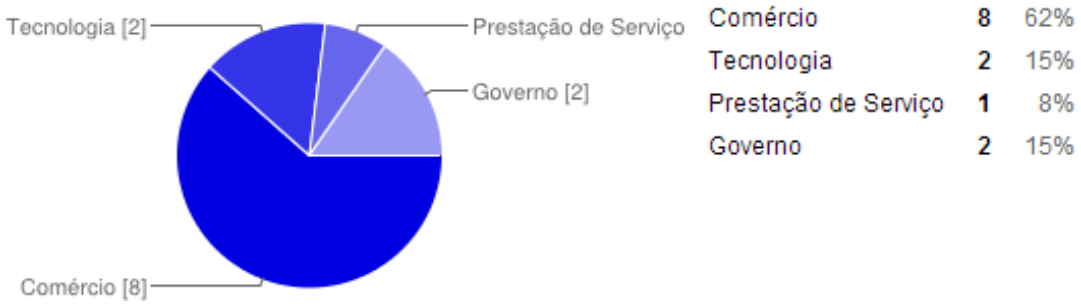


Gráfico 1: Ramo de Atuação das Empresas Entrevistada
Fonte: Pesquisa Questionário

No Gráfico 1 consta as porcentagens para cada segmento, sendo oito participantes no segmento comércio e apenas um participante no segmento de prestação de serviço.

Essas corporações possuem diferentes números de funcionários e cada uma apresenta metodologias de proteger a informação que trafega em sua rede (Gráfico 2) no

qual, 85% das empresas entrevistadas, possuem um departamento voltado apenas para a gestão de TI.

Foi perguntado a quantidade de funcionários das organizações. O Gráfico 2 apresenta os percentuais:

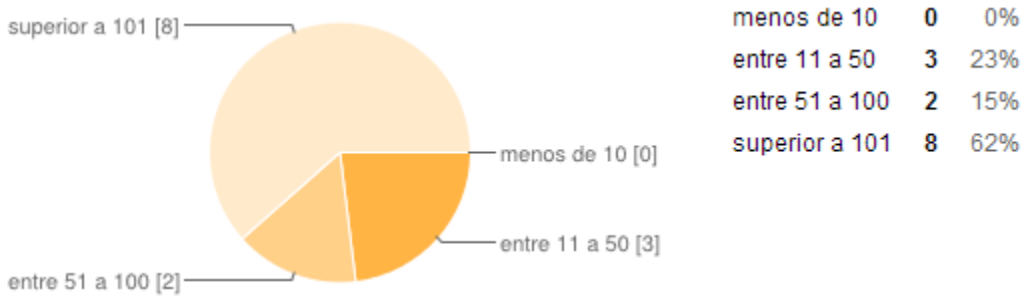


Gráfico 2: Funcionários por Empresa
Fonte: Pesquisa Questionário

Este Gráfico apresenta que a maioria das empresas entrevistadas é considerada grande, ou seja, com mais de cem funcionários, sendo oito participantes que assinalaram esta opção e apenas dois participantes escolheram a opção entre 51 a 100 funcionários.

O objetivo é abranger o máximo de ramos de atuações possíveis e diferentes tamanhos de empresa para tentar aborda de maneira mais ampla a situação, retornando assim, melhores resultados.

3.2. **INSTRUMENTO DE COLETA DE DADOS**

Para coletar os dados foi aplicado um questionário que foi baseado na proteção dos dados e privacidade dos mesmos em uma rede, manter estas informações sempre disponíveis, mas apenas para pessoas autorizadas, podendo ser manipulados, somente por funcionários que possuem esta liberdade e garantir a integridade da rede quanto a invasões de pessoas externas e roubo de informações.

As questões foram elaboradas visualizando normas de segurança da informação como a ABNT NBR ISO/IEC 17799 (2005) e ABNT NBR ISO/IEC 27000 (2006) e suas regras de gestão da informação.

3.3. **TRATAMENTO DOS DADOS**

Os dados foram tabulados na ferramenta gratuita da Google denominada “Formulário Google”. Para melhor discutir as informações foi utilizado o cruzamento com as informações levantadas no referencial teórico deste trabalho, analisando assim, as condutas adotadas pelas corporações para elaboração de um plano de segurança da informação.

O objetivo deste cruzamento de informações é fazer uma comparação da situação de gestão de TI na região, levantando o que pode ser melhorado para conscientizar as corporações sobre a importância de investimentos em segurança da informação, treinamento de pessoal em gerenciamento da TI e, principalmente, sobre medidas preventivas que podem ser adotadas para melhorar a segurança de seus sistemas de informações.

4. RESULTADOS

4.1. RESULTADO DO QUESTIONÁRIO

Os próximos tópicos detalharam os resultados colhidos pela pesquisa apresentando como é a segurança da informação de cada empresa entrevistada, como é feita a auditorias de TI e elaborada possíveis melhorias em sua politica de segurança da informação e como se dá a prevenção de perdas de dados importantes para a corporação.

4.1.1. A Segurança da Informação nas Empresas Entrevistadas

O objetivo do questionário era levantar a real situação da segurança da informação das empresas da região. Após o termino das entrevistas, pôde-se perceber um resultado alarmante quanto ao perigo que correm as empresas entrevistadas.

Quanto se trata de departamento de TI, 15% das empresas entrevistadas, responderam que não possuem um departamento próprio para lidar com essa área Isso poderia ser facilmente explicado já que entre as empresas entrevistadas, algumas podem ser filiais que utilizam esse setor de sua matriz ou ser uma empresa pequena na qual o funcionários de outro departamento também tem a função de cuidar da área de TI, o popular “garoto do computador”.

Das empresas entrevistadas, 54% afirmaram possuir um departamento de segurança da informação. Isso pode significar que os empreendedores se preocupam e têm consciência da importância da informação. Quanto ao restante, podemos concluir que podem ser empresas de porte menor, portanto, os seus administradores não acham que estas são visadas a ponto de receber invasões ou ataques. Isso pode ser um grave problema, pois qualquer rede corporativa pode ser atacada tendo varias motivações, sendo elas: espionagem de uma empresa rival, funcionários revoltado com a empresa por algum motivo entre outros.

O Gráfico 3 apresenta a quantidade de funcionários que trabalham em departamentos relacionados à segurança da informação, quanto à formação que possuem.

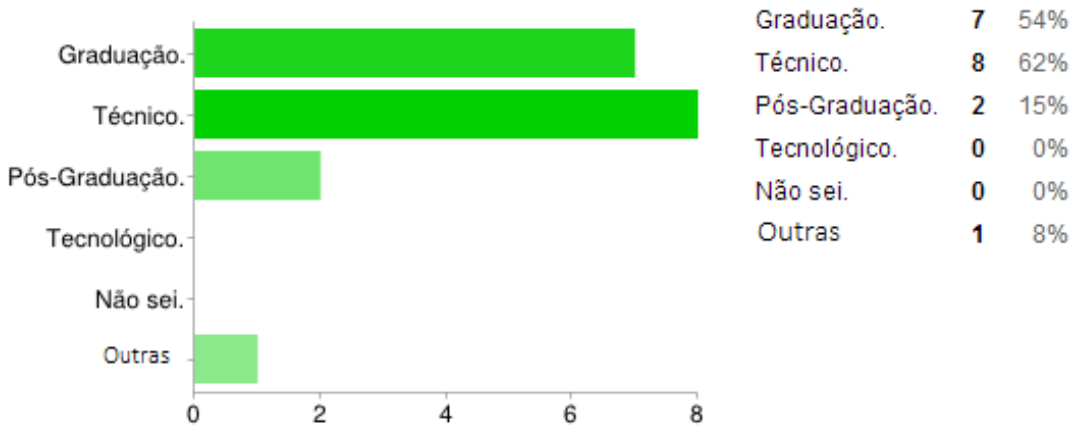


Gráfico 3: Formação de Funcionários Relacionada à Área de Segurança de TI

Fonte: Pesquisa Questionário

Nele é possível notar que existem muitas pessoas especializadas trabalhando na área de TI. Isso significa que a responsabilidade está nas mãos de quem já conhece o assunto, ou que pelo menos já estudou sobre assuntos relacionados à gestão de TI.

Ao serem questionados sobre o uso de sistemas de controle de caixa, estoque, etc, apenas uma empresa não possui algum tipo de sistema. Das doze empresas restantes, a grande maioria possui um sistema de ERP (*Enterprise Resource Planning*). Um ERP é um sistema de gestão empresarial, abrange todos os processos de uma empresa, desde compra e vendas a processos gerenciais (DE PINA, 2011). Pelo fato destas empresas utilizarem um sistema ERP, a maioria de seus funcionários tem acesso a esse sistema, sempre com utilização de senhas e *login* contendo uma hierarquia de acesso onde cada funcionário ou setor da corporação acessa apenas o que é permitido pelo seu *login*. Destes, 77% possuem *logins* com registro das operações realizadas por cada usuário, permitindo saber o que cada funcionário faz no sistema. O procedimento destas empresas quando um funcionário se desliga dela, é a exclusão ou suspensão do *login* de acesso ao sistema.

De acordo com os respondentes, a maioria das empresas entrevistadas utilizam o sistema operacional híbrido, mesclando sistema Linux com sistema proprietário, cerca de 45% como apresentado no Gráfico 4. Uma grande dificuldade de utilizar sistema proprietário é o gasto com a ativação do produto pode ser muito caro. Uma empresa que

possui sistemas proprietário tem que ter uma chave de ativação para máquina que possui esse sistema, ou seja, para cada computador com uma versão de sistema proprietário deve-se comprar uma chave de ativação. Todas as empresas entrevistadas procuram sempre manter seus *softwares* atualizados.

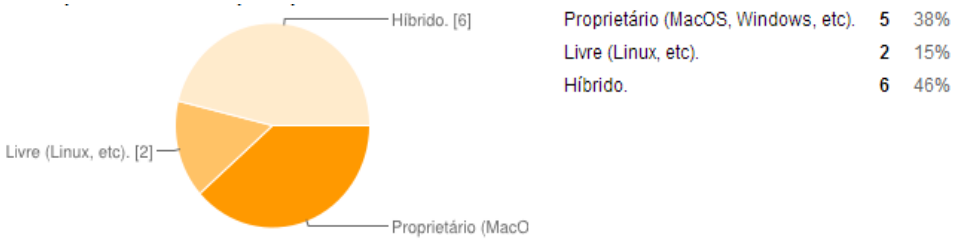


Gráfico 4: Software Utilizado Pela Empresa

Fonte: Pesquisa Questionário

O Gráfico 5, apresenta um problema no qual 38% das empresas não tratam o assunto de segurança da informação em suas reuniões. Esse assunto é necessário ser tratado sempre, pois, ataques podem acontecer a qualquer momento e o que está em risco são informações importantes da empresa que na posse de pessoas mal-intencionadas, podem acarretar grandes prejuízos a estas empresas.

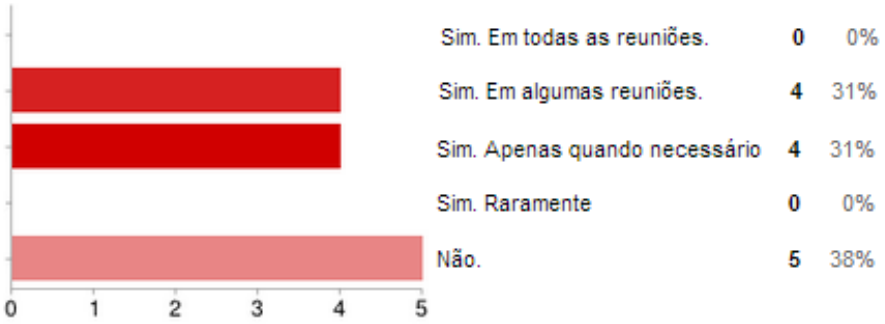


Gráfico 5: O Tema “Segurança da Informação” em Reuniões de Diretoria.

Fonte: Pesquisa Questionário

Quando perguntado sobre o interesse quanto ao tema segurança da informação (Gráfico 6), 77% das empresas entrevistadas se interessam pelo tema sendo que 4 (quatro) participantes responderam que o interesse é muito e apenas 3 (três) participantes. Ou seja, 23% responderam que não possuem interesse nenhum sobre o tema.

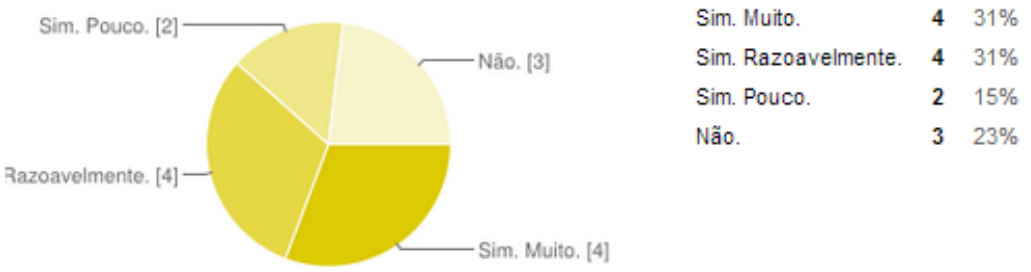


Gráfico 6: Interesses das Empresas Sobre o Tema.

Fonte: Pesquisa Questionário

Diante dos resultados obtidos até aqui, pode-se perceber que a maioria das empresas entrevistadas conhece sobre o assunto segurança da informação, pois trabalham com sistemas compartilhados em uma rede corporativa e possuem certa preocupação com relação à proteção dos dados que circulam na mesma.

4.1.2. **Políticas e Auditoria de TI**

Foi perguntado sobre a existência de uma politica de segurança da informação. 38% dos respondentes assinalaram não possuir, conforme Gráfico 7.

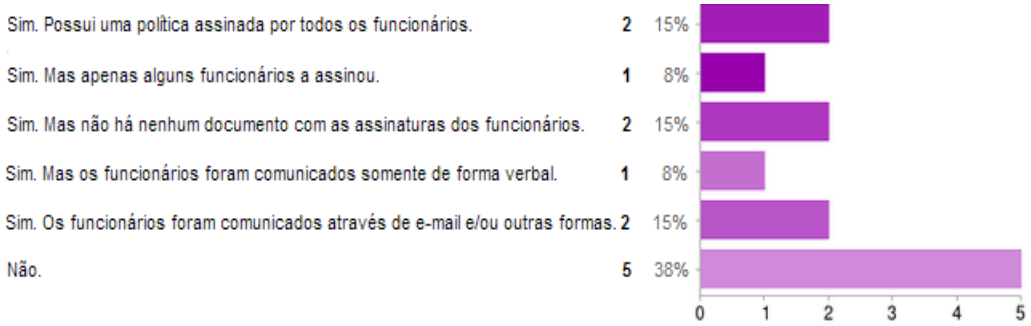


Gráfico 7: Política de Segurança da Informação

Fonte: Pesquisa Questionário

Uma política da informação busca prover a segurança da informação de uma empresa, é um conjunto de normas flexíveis a serem seguidas para o uso e manipulação da

informação dentro da corporação a serem executadas por todos os funcionários, auditadas periodicamente e quando necessário melhorado para garantir melhor eficiência.

Existem várias maneiras de controlar os acessos dos funcionários a conteúdos da Internet utilizando ACL (*Acess Control List*, ou em português, lista de controle de acessos). Foi perguntado as empresas entrevistadas sobre a existência de uma ACL e o Gráfico 8 apresenta os percentuais.

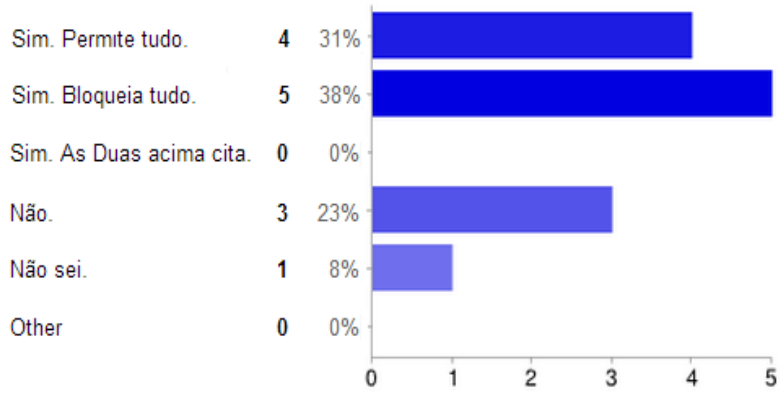


Gráfico 8: Uso de ACL.

Fonte: Pesquisa Questionário

Apenas 23% das empresas entrevistadas responderam não possuírem uma ACL e 69% responderam que possuem alguma maneira de controlar o acesso dos funcionários a conteúdos da Internet. Uma ACL pode ser configurada de três maneiras: A primeira é permitir tudo, é uma forma mais fácil de elaborar, pois, nesta opção, todos os conteúdos e serviços são permitidos e são bloqueados a medida que, a partir de uma analise, são considerados sem proposito para a corporação. Outra forma é bloquear tudo, esta opção é mais segura, porque, diferente da primeira, nela tudo é bloqueado e, a partir de uma análise, libera-se o que é necessário para ser utilizado pelos funcionários. A terceira é utilizar as duas políticas juntas, podendo utilizar a opção permitir tudo, quando usar serviços de uma rede interna da corporação, e a opção bloquear tudo quando se trata de uso de serviços ou conteúdos externos, ou seja, acesso a Internet.

Das empresas entrevistadas apenas três não fazem nenhum tipo de monitoria aos equipamentos de TI. 46% possuem alguma política voltada para o uso de terceiro, na qual parte utiliza uma política simples, se não trabalha na empresa não tem acesso a computadores dela. Outras que possuem prestadoras de serviços que precisam utilizar

algum computador da empresa possuem computadores reservados para o acesso monitorado destas pessoas. Apenas 31% das empresas entrevistadas possuem uma política de uso de mídia de armazenamento em seus equipamentos.

Para o caso de desastre na rede, seja ele por invasão, queda momentânea de energia, enchentes, etc., 53% das empresas entrevistadas possuem procedimentos a serem seguidos para garantir a menor perda possível e a continuidade dos negócios da empresa. 15% das empresas apresentaram procedimentos que não são eficientes para todo o tipo de desastre.

O Gráfico 9 apresenta as respostas das empresas entrevistadas quando a pergunta foi sobre o período de análise de riscos que ameaçam sua rede:

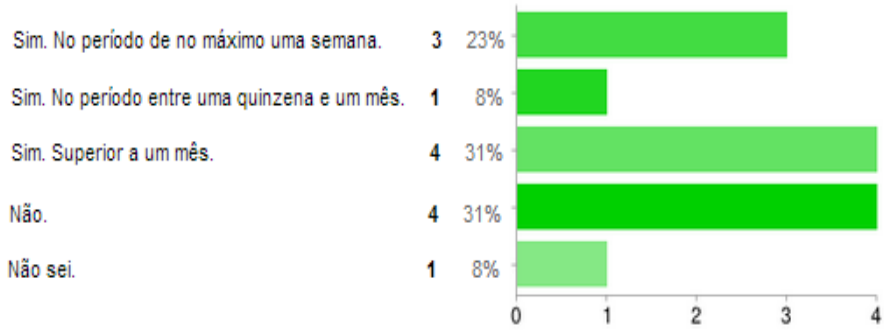


Gráfico 9: Período de Análise de Riscos.

Fonte: Pesquisa Questionário

Das respondentes, 62% fazem a análise dos riscos que ameaçam a sua informação, nas quais, 23% fazem sua análise no período de no máximo uma semana; 8% no período entre quinze dias a um mês e 31% no período superior a um mês. Isso pode auxiliar estas corporações as manterem sempre atualizadas e garante uma melhor proteção de seus dados.

A próxima questão a ser levantada foi se as empresas entrevistadas se baseiam em alguma norma de segurança para formular a sua política interna. Vide o Gráfico 10.

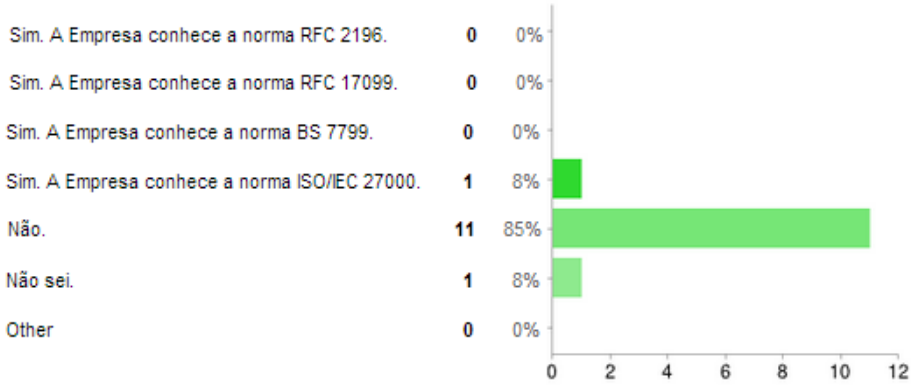


Gráfico 10: Normas Conhecidas Pelas Empresas.

Fonte: Pesquisa Questionário

Uma norma da segurança da informação fornece: regras e base para auditoria de dados; apresenta requisitos para a criação de uma norma de segurança da informação e forma dela ser melhorada e um gerenciamento de riscos para uma corporação sem impor controles de segurança. Grande parte das empresas, não se baseia em uma norma de segurança para elaborar sua política interna de segurança da informação. Isto pode resultar em política inflexível e ineficaz, não garantindo a segurança da sua informação. E, pode ser explicado pelo fato de que apenas uma empresa possui funcionário(s) com certificação em alguma norma de segurança.

4.1.3. **Prevenção de Perda**

Para diminuir a taxa de acidentes ou perdas por invasão, se utiliza sistemas para detecção de intrusos. Esses sistemas detectam e informam se aquela rede está sendo atacada por alguém. Além de detectar um invasor, um sistema de prevenção de intrusos, pode também bloquear o atacante, baseando-se em um conjunto de regras.

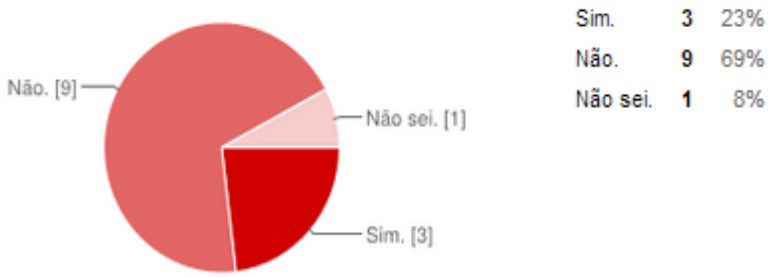


Figura 15: Uso de Sistemas de Prevenção e/ou Detecção de Intrusos.

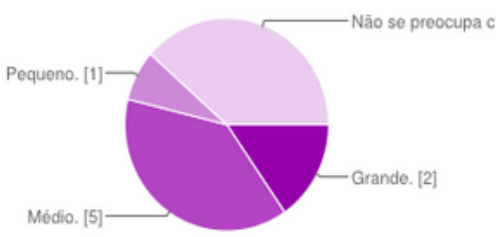
Fonte: Pesquisa Questionário

O *firewall* controla todo o tráfego de entrada e saída de rede ou mesmo de uma determinada máquina. Também pode conter sistemas de prevenção no qual, através de um conjunto de regras, bloqueia qualquer intruso que podem ameaçar a rede. Das empresas entrevistadas 92% afirmaram possuir um *firewall*. A mesma porcentagem disse possuir sistema de anti-virus, em sua maioria sistemas livres.

Das empresas entrevistadas, 46% afirmaram nunca terem sofrido nenhum tipo de invasão ou acidente em TI. Este fator pode significar que o tráfego de rede não esta sendo monitorado como deveria. Mesmo possuindo uma política de segurança da informação boa, nenhuma empresa está livre de sofrer ataques, uma política de segurança são regras que auxiliaram a empresa a diminuir as taxas de invasão e perdas de dados. Outros 46% afirmaram que os ataques são classificados como gravidade baixa e 8% de gravidade média.

A maioria das empresas não se preocupam em investir em mídias de *backup* mais eficientes e duráveis (54%). Isto pode ser explicado pelo fato das mesmas já obterem uma mídia durável e que atenda os requisitos para armazenamento de seus dados. 76% afirmou possuir um sistema de *backup* responsável por criar cópias de segurança dos arquivos da empresa e apenas 15% utilizam o *backup* criptografado, o que garante uma maior segurança, até mesmo no caso de roubo do *backup*. Com o *backup* criptografado, dificilmente o ladrão conseguirá ter acesso às informações nele contida.

O Gráfico 11 apresenta que maioria dos empresários estão preocupados e investem ou incentiva seus funcionários a melhorarem seus conhecimentos quanto ao tema TI e Segurança da Informação.



Grande.	2	15%
Médio.	5	38%
Pequeno.	1	8%
Não se preocupa com isso.	5	38%

Gráfico 11: Investimento na Preparação dos Funcionários de TI

Fonte: Pesquisa Questionário

Cinco participantes responderam não se preocuparem com investimento na preparação dos funcionários de TI e oito participantes responderam se preocuparem com a preparação de seus funcionários.

Ainda não temos nas empresas a gestão de tecnologia da informação como deveria ser tratada, mas, com investimentos e incentivos de funcionários, a segurança da informação das empresas pode ser melhorada e se tornar mais eficiente para a prevenção de ataque, mantendo a informação sempre disponível e íntegra aos seus funcionários. É importante de que os empresários tenham conhecimento sobre a importância da informação que uma rede corporativa contém, e que os riscos que à cercam são reais e podem causar sérios prejuízos à sua empresa. Com esta conscientização dos empresários, teremos muito mais investimentos em equipamentos de TI, melhores políticas de segurança da informação e mais contratação de pessoal especializado no assunto.

4.2. **MEDIDAS A SEREM ADOTADAS**

A entrevista mostra que 46% das empresas não possuem um departamento de segurança da informação. Para melhorar essa situação, o ideal é que cada empresa ter um departamento voltado para esta área, com pessoal qualificado para administrar toda a informação que circula na rede da empresa e protege-la de qualquer ameaça interna ou externa. A quantidade de funcionários neste setor deve ser de acordo com a necessidade de cada empresa. Cabe a este setor, a criação de uma política de segurança flexível, impressa e assinada por cada funcionário que trabalha na corporação, ou seja, uma política que permita determinadas alterações futuras, como por exemplo, não se deve especificar o

tamanho da mídia de *backup*, pois, o tamanho dos dados desta empresa irá crescer com o tempo.

No caso de uso de algum programa de gestão dentro da corporação, o ideal é que haja, para cada funcionário um *login* com senha de acesso, que ficará disponível apenas os privilégios que cabe a ele, para executar sua função dentro da empresa e um histórico de operações realizadas por cada *login* cadastrado neste sistema. A entrevista mostra que todas as empresas entrevistadas possuem um *logins* de acesso. Este *login* é de caráter pessoal no qual cada um deve conter uma senha com sequência de caracteres aleatórios, ou seja, que não formem palavras conhecidas, para dificultar a descoberta por outras pessoas que não sejam o titular do *login*. Lembrando que um *login* de acesso na mão de uma pessoa mal-intencionadas, seja ela, funcionários que trabalham na mesma empresa que você ou não, pode representar um grande dano para a empresa e para o titular do *login*. O procedimento correto a ser executado por parte da empresa com a saída de um funcionário é o cancelamento do *login*, tornando-o inativo. É importante que não sejam apagados os registros de ações realizadas por este no sistema, para a necessidade de fazer uma pesquisa, ou mesmo um balanço geral de tudo que foi realizado no sistema em um determinado período.

A pesquisa mostra que os sistemas menos utilizados nas empresas, são os sistemas livres. O grande problema na utilização de softwares proprietários é a ativação de sistema, que requer uma chave ou uma autenticação do fabricante deste sistema. Uma empresa que utiliza sistemas proprietários deve conter para cada máquina, um sistema original, evitando assim, multas, acusações de pirataria por possíveis fiscalizações e até mesmos problemas de atualização dos mesmos.

É muito importante que as empresa tenha grande interesse e levem para suas reuniões, o assunto “Segurança da Informação”. Das empresas entrevistas, 38% não leva o tema para suas reuniões de diretoria. Para uma contínua melhora da segurança, o assunto deve ser sempre tratado, baseados em avaliações semanais dos riscos que cada rede corporativa sofre. Isso ajuda a melhorar a política de segurança da informação da empresa. É evidente a necessidade de investimentos em equipamentos melhores e softwares mais eficazes, principalmente de segurança da informação, pois, trata-se de uma rede que possivelmente passa todas as informações cruciais de uma empresa e, sua integridade e confiabilidade devem ser mantidas.

Das empresas entrevistadas, 5 (cinco) não se preocupam em investimentos ou incentivos na preparação de seus funcionários de TI e 6 (seis) não se preocupam em investimentos ou incentivos na preparação de funcionários de segurança da informação, para melhorar essa situação, investimentos e incentivos na formação dos funcionários do setor de gestão de TI são importantes, principalmente, quando se trata de segurança da informação. Uma rede corporativa possui informações cruciais, esta informação pode ser desejada por pessoas que desejam obtê-las para beneficio próprio ou mesmo com o intuito de prejudicar a empresa. As vulnerabilidades são cada vez mais exploradas, conhecer uma norma de segurança pode ajudar na elaboração de uma política de segurança da informação mais eficiente, até mesmo, uma melhora na gestão de TI da empresa.

Os equipamentos de TI de uma empresa, também devem ser protegidos por um controle de patrimônios. Um plano de contingência da informação é responsável por manter a disponibilidades das informações para os funcionários executarem suas obrigações dentro da empresa. Existem várias maneiras para proteger os equipamentos de TI, de roubos ou danos que podem prejudicar o andamento dos processos de uma corporação. Uma forma eficiente de fazer isso é o uso da câmera de vigilância, áreas com acesso restrito e monitoração via Internet, essas ações combinadas podem ser boas para empresas de porte menor, porque, com ele é possível identificar o momento da queda do serviço, o que está acontecendo na sala onde ficam os equipamentos de TI naquele momento, e para o caso de roubo, a possibilidade de reconhecimento do indivíduo que praticou o ato. Apenas o uso da Internet não é recomendável, pois uma queda de serviço pode se dar por vários motivos como, por exemplo, a queda da Internet. Outra forma de fazer essa proteção é utilizando CPD, pois, todos os dados importantes ficam armazenados em outro local fora da empresa.

Possuir uma política voltada para o uso de terceiros da rede ou sistemas da empresa, conforme 46% das empresas entrevistadas possuem, também ajudará a manter a integridade das informações. Ela consiste em regras a serem seguidas para o acesso a rede de outras pessoas que não sejam funcionários, ou mesmo, fornecedores e parceiros da empresa e uso dispositivos de armazenamento em hosts que pertencem à rede. Para o acesso destes, deve-se haver a monitoração de cada ação efetuada na rede por este “visitante”, mesmo quando esta rede é aberta ao público.

O uso de *firewall* e programas de detecção e prevenção de intrusos pode manter

afastado da rede, possível invasores. Esses programas controlam todo o tráfego de rede desta corporação e identificando invasores e podendo bloquear o acesso destes na rede.

Um *backup* deve ser feito periodicamente e mantido durante muito tempo porque, dependendo do tamanho dos dados da empresa, um possível erro em alguma informação pode ser descoberto depois de muito tempo. 76% das empresas entrevistadas afirmaram possuírem um sistema de *backup* das quais 69%, mantem seus *backups* por uma semana ou mais antes da remoção.

23% das empresas entrevistas não se preocupam com o local de armazenamento da mídia de *backup*. O ideal é que ele seja mantido em locais com a temperatura certa para cada mídia e de preferência em locais fora da empresa, evitando assim, a perda dos dados no caso de inundação, incêndio ou qualquer outro desastre que venha a acontecer a essa empresa.

A partir dessas medidas, o que irá garantir o sucesso de uma política é a constante revisão dos riscos que ameaçam a informação de uma empresa e especialização de funcionários do setor para. A partir disto, haverá melhorias em sua política de segurança.

5. CONCLUSÃO

Diante de uma sociedade cada dia mais informatizado, os riscos de ataque a uma rede corporativa, só aumenta. Adotar algumas medidas preventivas e sempre discutir sobre possíveis ameaças, pode resultar em bons frutos para as corporações.

Para garantir uma segurança das informações de uma rede de uma determinada rede, é necessário um grande investimento na área de gestão de TI, mesmo que esse investimento não traga um retorno imediato às empresas. A Segurança da informação na verdade é uma forma de prevenção de perda nas quais; o empregador garante que a informação contida em uma rede, sempre se estará disponível, confiável e íntegro para seus funcionários acessa-las, mantendo-se assim, continuidade dos processos realizada por esta empresa; e que não caia em mãos de pessoas mal-intencionadas.

Ainda temos muito a melhor nas corporações de Caratinga/MG, mais investimentos na área de TI e principalmente, a adoção de políticas de Contingência da Informação, podem ajudar a prevenir perdas e grandes prejuízos em uma tragédia ou um incidente. Uma política de segurança da informação melhor e qualificação de funcionários possibilita manter a informação contida em uma rede íntegra e segura. Isso começa do empresário que, em cidades pequenas, pensam apenas em lucros imediatos e não muito em investimentos, principalmente, no setor de gestão de TI. É importante que os empresários compreendam a importância da informação e que um investimento no setor de gestão de TI, poderá não trazem um retorno direto, mas matem a sua empresa em atividade e segura de pessoas mal-intencionadas.

6. TRABALHOS FUTUROS

Aplicar um questionário a nível nacional, levantando assuntos como normas de segurança da informação e índice de incidentes em uma rede corporativa. Este questionário poderia ser aplicado online onde varias empresas de segmentos diversos, poderiam acessa-lo e responde-lo.

Depois de feito o questionário e estudado as respostas, levaria para as empresas envolvidas, sugestões para melhorarem a sua segurança da informação.

REFERÊNCIAS

ABNT NBR ISO/IEC 17799. **Tecnologia da Informação – Tecnicas de Segurança – Código de prática para gestão da segurança da Informação.** Associação Brasileira de Normas Técnicas. Rio de Janeiro, 2005.

ABNT NBR ISO/IEC 27000. **Tecnologia da Informação – Tecnicas de Segurança – Código de prática para gestão da segurança da Informação.** Associação Brasileira de Normas Técnicas. Rio de Janeiro, 2006.

ANDRADE, Daniel; VINICIUS, Eric; MAFRA, Gabriel; FLÁVIO, Lúcio; HENRIQUE, Marcos; SEPULVEDO, Ulisses; SILVA, Edilberto. **Plano de Contingência de TI: Preparando Sua Empresa Para Reagir a Desastres e Manter a Continuidade do Negócio,** 2011. Pós-Graduação em Segurança da Informação da Faculdade SENAC/DF, Brasília.

BORAN, Sean. IT **Security Cookbook,** 1996. Disponível em http://www.boran.com/security/. Acesso em: 21/05/2012.

CANONGIA, Claudia; JÚNIOR, Admilson Gonçalves; JUNIOR, Raphael Mandarino; **Guia de Referência Para a Segurança das Infraestruturas Crítica da Informação**. Presidência da República. Brasília/DF, 2010.

DA SILVA, Valdir Teixeira; **Gestão de Segurança da Informação, um estudo de caso da política de segurança da informação (POL-01-100) da Cia do Metropolitano de São Paulo,** 2009. Monografia apresentada no curso de Tecnologia em Informática para Gestão de Negócios – Faculdade de Tecnologia da Zona Leste. São Paulo.

DE PINA, Eurisandra Mafalda da Silva; **Sistemas Integrados para Gestão Empresarial – O caso da PHC e a sua utilização na gestão do Supermercado Palácio Fenícia,** 2011. Monografia apresentada à Universidade Jean Piaget de Cabo Verde. Cabo Verde.

DIAS, Cláudia; **Segurança e Auditoria da Tecnologia da Informação.** Axcel Books. Rio de Janeiro, 2010.

FERNANDES II, Aguinaldo Aragon e DE ABREU, Vladimir Ferraz; **Implantando a**

Governança de TI da Estratégia à Gestão dos Processos e Serviços. Brasport Livros e Multimídia Ltda. São Paulo, 2008.

LAUREANO, Marcos Aurelio Pchek; **Gestão de Segurança da Informação,** 2005. Disponível em: http://www.mlaureano.org/aulas_material/gst/apostila_versao_20.pdf. Acessado em 25/08/2012.

LUZ, Mário Sergio da Silva; **Políticas de Segurança da Informação,** 2010. Trabalho de Segurança de Redes – União Educacional de Brasília. Disponível em: http://www.ebah.com.br/content/ABAAAAq3kAL/politicas-seguranca-informacao. Acessado em 31/05/2012.

MARCIANO, João Luiz Pereira; **Segurança da informação: Uma abordagem social,** 2006. Tese apresentada ao Departamento de Ciência da Informação e Documentação da Universidade de Brasília. Disponível em: http://repositorio.bce.unb.br/bitstream/10482/1943/1/Jo%C3%A3o%20Luiz%20Pereira%20Marciano.pdf. Acessado em: 10/09/2012.

OLIVEIRA, Alessandra Aparecida; **A Segurança da Informação na Micro Empresa Auto Escola Master de Gurupi,** 2008. Trabalho de Conclusão do Curso de Administração – Faculdade UNIRG, Gurupi/TO. Disponível em: http://www.unirg.edu.br/cur/adm/arq/TCC2008_1/TCC%20-%20Alessandra%20Aparecida%20Oliveira.pdf. Acessado em 25/03/2012.

PINHEIRO, José Maurício S. **Auditoria e Análise de Segurança da Informação: Segurança Física e Lógica.** 2009. Centro Universitário Geraldo Di Biase. Disponível em: http://www.projetoderedes.com.br/aulas/ugb_auditoria_e_analise/ugb_apoio_auditoria_e_analise_de_seguranca_aula_02.pdf. Acessado em 20/08/2012.

PINHEIRO, José Maurício Santos; **Conceitos de Redundância e Contingência,** 06/12/2004. Disponivel em: http://www.projetoderedes.com.br/artigos/artigo_conceitos_de_redundancia.php, Acessado em 24/05/2012.

RODRIGUES, Walton Alencar. **Boas Práticas em Segurança da Informação**. 2º edição. Tribunal de Contas da União. Secretaria de Fiscalização de Tecnologia da Informação.

Brasília, 2007. Disponível em: http://portal2.tcu.gov.br/portal/pls/portal/docs/2059162.PDF. Acessado em 20/04/2012.

SERPRO, Empresa do Ministério da Fazenda. **Política de Segurança da Autoridade Certificadora do SERPRO (PS SERPROACF)**. 2006. Disponível em: http://blog.fimes.edu.br/milena/files/2011/11/poltica_seg_AC_serpro_acf_v2.0.pdf. Acessado em 05/05/2012.

SILVA, Pedro Tavares; CARVALHO, Hugo e TORRES, Catarina Botelho; **Segurança dos Sistema de Informação – Gestão Estratégica da Segurança Empresarial.** Centro Atlântico, Lda. Lisboa, Portugal, 2003.

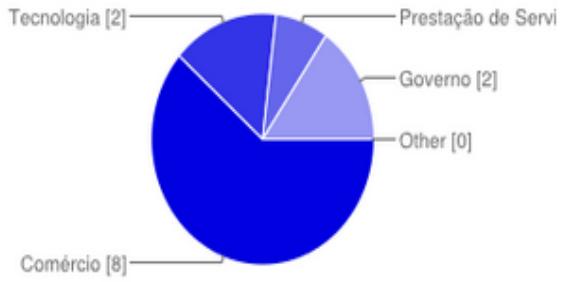
SIMCH, Maicom Rafael Victor; TONETTO, Tiago Squinzani. **Auditoria dos Sistemas de Informação Aliada à Gestão Empresarial**, 2008**.** Disponível em: http://w3.ufsm.br/revistacontabeis/anterior/artigos/vIVn02/t005.pdf. Acessado em 20/04/2012.

SPANCESKI, Francini Reitz; **Política de Segurança da Informação – Desenvolvimento de um Modelo Voltado para Instituições de Ensino,** 2004. Disponível em: http://www.mlaureano.org/aulas_material/orientacoes2/ist_2004_francini_politicas.pdf. Acessado em 24/03/2012.

ANEXOS

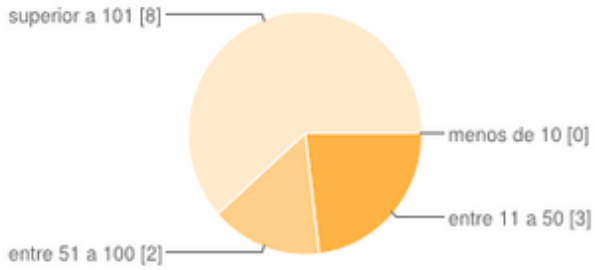
1. TABULAÇÃO DOS RESULTADOS

Em qual ramo a empresa que você trabalha atua?



Comércio	8	62%
Tecnologia	2	15%
Prestação de Serviço	1	8%
Governo	2	15%
Other	0	0%

Quantos funcionários trabalham nesta empresa?



menos de 10	0	0%
entre 11 a 50	3	23%
entre 51 a 100	2	15%
superior a 101	8	62%

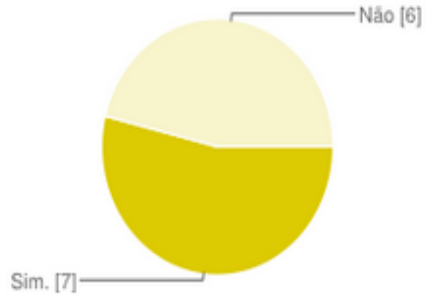
Existe um departamento de Tecnologia da Informação (TI)?

Sim.	11	85%
Não	2	15%

Quantos funcionários trabalham neste departamento?

1 7 12 | 6 3 8 4 8 2 2 3 |

Há um setor de segurança da informação?

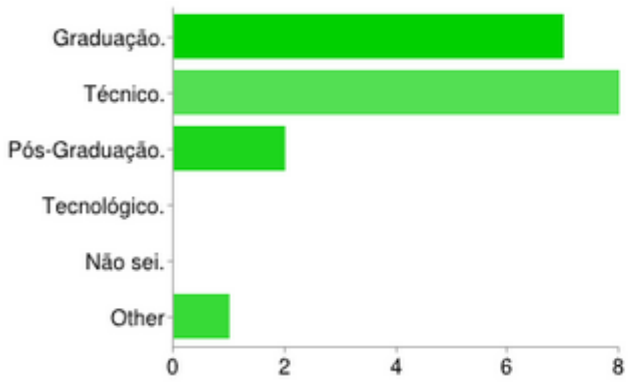


Sim.	7	54%
Não	6	46%

Quantos funcionários estão envolvidos nesse processo?

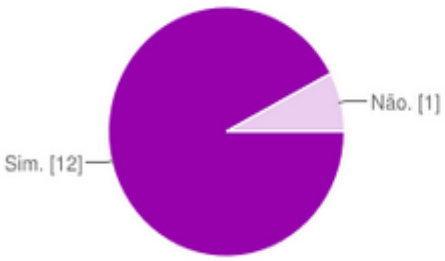
0 2 3 2 4 3 2 3

Os funcionários deste departamento possuem qual formação em TI?



Graduação.	7	54%
Técnico.	8	62%
Pós-Graduação.	2	15%
Tecnológico.	0	0%
Não sei.	0	0%
Other	1	8%

A empresa utiliza algum sistema para controle de caixa, de estoque, etc?

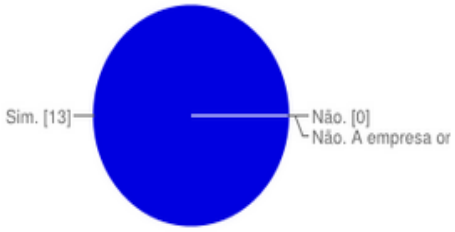


Sim.	12	92%
Não.	1	8%

Qual tipo de sistema? Quantas pessoas utilizam este sistema?

Todas as pessoas utilizam este sistema, o sistema localiza-se em um servidor e todos os clientes executam de lá as suas funções. É um ERP completo, onde controla entrada e saída de mercadorias, além de pagamentos de boletos e etc. O sistema e um ERP que possui a função de controle de caixa e demais funcionalidades de ERP possui! As pessoas que trabalham neste sistema são o departamento financeiro, e o departamento de TI pois os software e próprio. Controle contabil, controle de marcação de consultas e exames. 3 pessoas ERP - aproximadamente 150 pessoas | CRM - Aproximadamente 50 pessoas - BI - ...

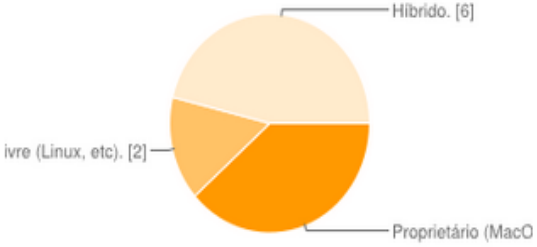
Há um registro de usuários do(s) sistema(s) com a utilização de senhas de acesso?



Sim.	**13**	100%
Não.	**0**	0%
Não. A empresa onde trabalho não possui nenhum sistema.	**0**	0%

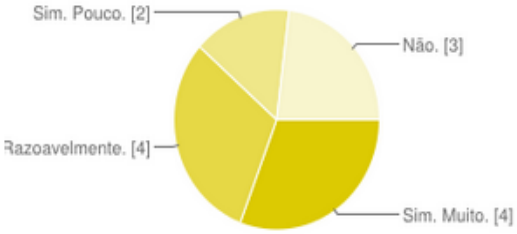
Interesse da Empresa na Área de TI

Que tipo de software a empresa possui?



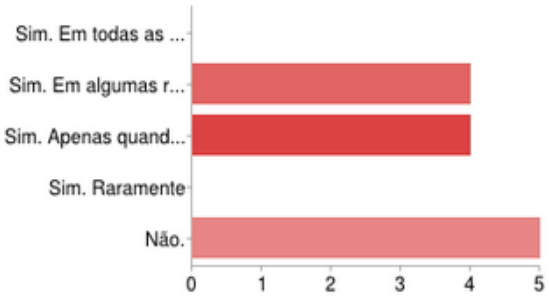
Proprietário (MacOS, Windows, etc).	**5**	38%
Livre (Linux, etc).	**2**	15%
Híbrido.	**6**	46%

A diretoria demonstra interesse pelos temas de segurança da informação?



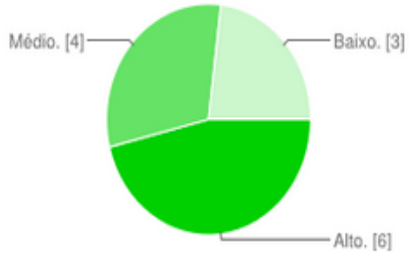
Sim. Muito.	**4**	31%
Sim. Razoavelmente.	**4**	31%
Sim. Pouco.	**2**	15%
Não.	**3**	23%

O tema "segurança da informação" faz parte da pauta/ata nas reuniões de diretoria?



Sim. Em todas as reuniões.	**0**	0%
Sim. Em algumas reuniões.	**4**	31%
Sim. Apenas quando necessário trata sobre o assunto	**4**	31%
Sim. Raramente	**0**	0%
Não.	**5**	38%

Qual o nível de conscientização da diretoria quanto à segurança da informação?



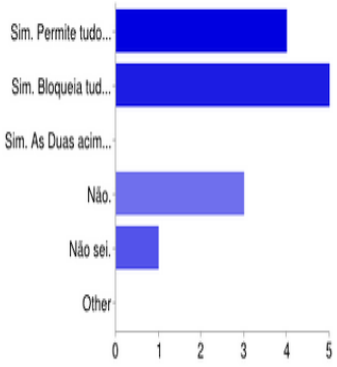
Alto.	6	46%
Médio.	4	31%
Baixo.	3	23%

Política e Auditoria de TI

Há uma política de segurança da informação?

Sim. Possui uma política assinada por todos os funcionários.	2	15%
Sim. Mas apenas alguns funcionários a assinou.	1	8%
Sim. Mas não há nenhum documento com as assinaturas dos funcionários.	2	15%
Sim. Mas os funcionários foram comunicados somente de forma verbal.	1	8%
Sim. Os funcionários foram comunicados através de e-mail e/ou outras formas.	2	15%
Não.	5	38%

Há uma ACL (lista de controle de acessos) que controle o tráfego da rede, permitindo aos funcionários acessarem apenas conteúdos seguros e/ou úteis para a empresa ou para os mesmos?

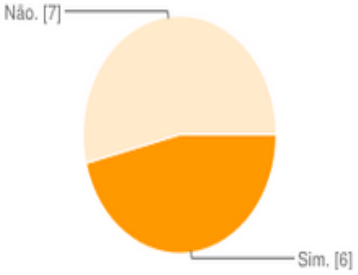


Sim. Permite tudo. Deixa o acesso livre para todos e vai bloqueando conteúdo impróprios ou desnecessários a medida que for necessário	4	31%
Sim. Bloqueia tudo. Deixa o acesso bloqueado e vai liberando de acordo com a necessidade da empresa ou dos funcionários	5	38%
Sim. As Duas acima cita. Dando acesso total ao trafego interno da rede e bloqueando todos os acesso a internet.	0	0%
Não.	3	23%
Não sei.	1	8%
Other	0	0%

Como é feita a proteção física dos equipamentos de TI pertencentes a empresa? (Exemplo: câmeras de vigilância, servidores, computadores, etc)

Câmeras de vigilância e chaveamento de salas posteriores o horário de expediente, a sala não é segura pois não fica dentro do setor de TI da empresa. Os servidores do departamento de TI se encontram no mesmo local que as pessoas trabalham sendo vigiado por câmeras e portas trancadas quando não minguem, o do financeiro fica em uma sala separada com refrigeração própria, e trancado. Somente chave geral da porta de entrada Não é feita. A segurança é feita por acesso restrito ao local onde os mesmo se encontram e toda a movimentação é monitorada por cameras. Alguns servidores têm redundância e os me ...

Possui uma política voltada para o uso de terceiros (pessoas que não trabalham na empresa), da rede (sem fio ou cabeada) e/ou do sistema da empresa?

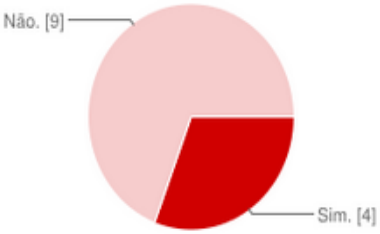


Sim.	6	46%
Não.	7	54%

Descreva sobre esta política.

E bem simples se não trabalha ou pertence a organização não tem acesso. Existe uma rede sem fio específica para acesso de visitantes, mas separada da rede da empresa, dando acesso apenas para um link de internet exclusivo para esse fim. Terceiros não acessam os dados da empresa. So pode ser utilizado por prestadoras de serviço de internet, sendo monitorado existem maquinas para o uso de cliente e fornecedores para serviços não pode usar

Possui uma política de uso de mídias de armazenamento (pen-drives, cdrom, etc.) em equipamentos da empresa para mídias pessoais, ou seja, de propriedade de funcionários ou mesmo terceiros?

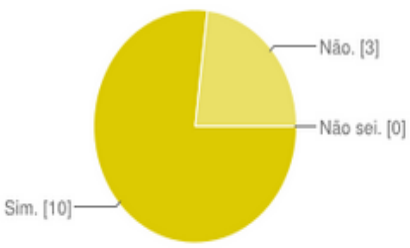


Sim.	4	31%
Não.	9	69%

Descreva sobre esta política.

A maioria Máquinas estão travadas para pen drive Mas alguns micros são desabilitados as portas USB e CDROM. não é autorizado o uso de midias que não são de propriedade da empresa monitorado e restrito a funcionários apenas funcionarios

Há um registro de histórico das operações realizadas por cada login (usuário)?



Sim.	10	77%
Não.	3	23%
Não sei.	0	0%

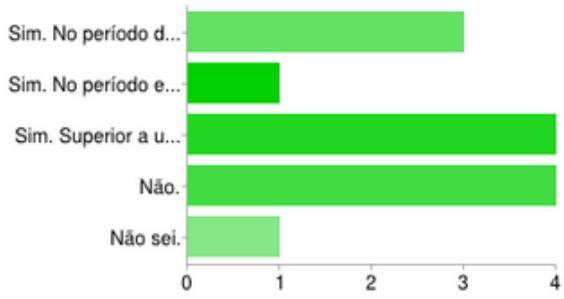
Qual é o procedimento realizado com relação ao(s) login(s) de sistema de um ex-funcionário?

O usuário tem sua senha bloqueada, não é excluída pois qualquer movimento feito dentro do sistema ele poderá ser identificado por quem foi feito, assim um funcionário que saiu da empresa pode ser identificado como o responsável por alguma coisa ilícita, Existem histórico de navegação na web, e os sistemas desenvolvidos existem login para todos os usuários que o utilizam, mais registros no login do servidores. suspender sua conta Login exlcuido. Assim que o funcionário é desligado da empresa e a baixa é feita no sistema, um email é disparado de forma automática para pessoas chaves que providencia ...

Qual é o procedimento com relação a desastres (incêndio, ataques de intrusos, queda momentânea de energia, enchentes, etc.) na rede?

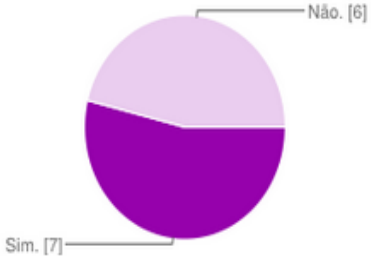
Primeiramente o conferimento do servidor, se ele está ok ou não, segundo são as baterias do nobreak estão carregas, quanto a ataques de intrusos há um certo retrucamento pois a única pessoa que pode mexer no servidor não é o funcionário de ti da empresa, causando assim um pouco de transtorno. Após isso é verificado máquina por máquina o seu funcionamento. Contra Inocêncio não existem uma media, mais para ataques de intrusos sim para todos os serviços retira da rede, ver se realmente e um ataque caso seja reconfigura tudo novamente com antes do ataque, quanto a queda de energia existe nobreak ...

Há uma análise dos riscos que podem ameaçar o ativo e a informação que a empresa deseja proteger, como ataques, vulnerabilidades e vírus, para auxílio na melhoria da política de informação?



Sim. No período de no máximo uma semana.	3	23%
Sim. No período entre uma quinzena e um mês.	1	8%
Sim. Superior a um mês.	4	31%
Não.	4	31%
Não sei.	1	8%

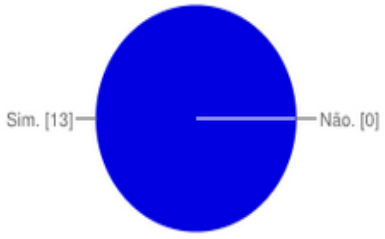
Esta análise auxílio na melhoria da política de informação existente na empresa?



Sim.	7	54%
Não.	6	46%

Configuração e Funcionamento dos Recursos de TI

A empresa sempre mantem seus softwares atualizados?



Sim.	13	100%
Não.	0	0%

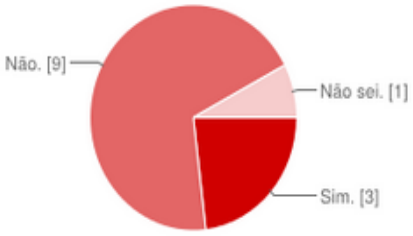
Há uma hierarquia no acesso dos usuários ao sistema nas quais cada um tem permissão de acessar apenas a parte que o auxilia em suas obrigações?

Sim.	**13**	100%
Não.	**0**	0%
Não sei.	**0**	0%

Observações sobre a questão acima.

Sim porém todos os usuários do escritório tem permissão livre para alterar qualquer coisa, porém não de dados de uma outra filial, apenas da filial onde trabalha. | O acesso pode ser concedido por grupo de usuários ou acesso diferente para usuários individuais. | Em alguns lugares sim. Outros não é necessário. | cada setor possui sua premissão | Sim existe grupos de funcionarios que apenas podem ver uma informações mais nunca altera-la.

A empresa possui algum sistema de detecção e/ou prevenção de intrusos?

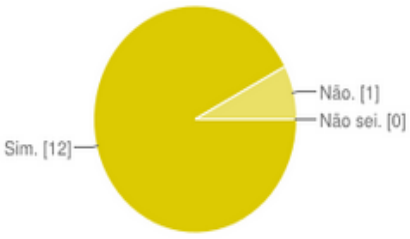


Sim.	**3**	23%
Não.	**9**	69%
Não sei.	**1**	8%

Qual sistema de detecção e/ou prevenção de intrusos?

Apenas anomalias grotescas, como lentidão do servidor, erros em banco de dados e etc. | não sei | nenhum | Nao existe. | Monitoramento constante ao trabalho do firewall. | VPN protegida | não tem. | não possui | não sei | nao possui | não possui | segurança na rede para não permitir que intrusos entrem | Nenhum.

A empresa possui algum sistema de antivírus?

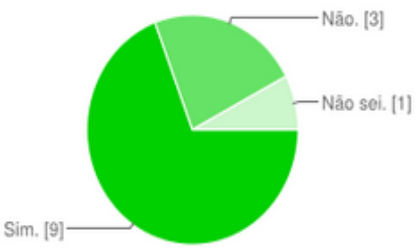


Sim.	**12**	92%
Não.	**1**	8%
Não sei.	**0**	0%

Qual sistema de antivírus?

Verificação periódica do técnico resposável de TI. | kaspersky | nenhum | Qualquer sistema free. | panda | Avast | Avast, Symantec, AVG. | Avast | Avast | Avira e Avast | Panda Adminsecure | Avast | Ambos as máquinas utilizando Eset Smart Security 5

Possui algum firewall (sistema que controla o tráfego de entrada e saída da rede ou de uma determinada maquina)?



Sim.	9	69%
Não.	3	23%
Não sei.	1	8%

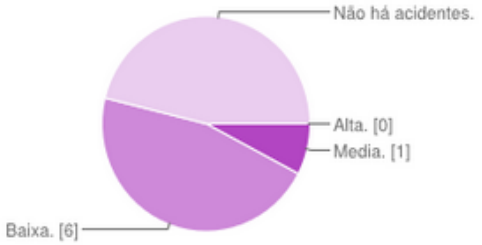
Possui algum firewall (sistema que controla o tráfego de entrada e saída da rede ou de uma determinada maquina)? Caso não, por quê?

Como especificado em alguma questão anterior, o servidor e a rede do sistema é fechada, sendo linux, porém não implementada mudanças de portas de serviços como ssh e implementações do iptable. | não sei | possui iptables | Sim. | sim | sim | possui | sim | sim | sim | Suse linux | não, porque não houve necessidade ainda | Não sei.

Houve alguma dificuldade na configuração do firewall? Caso sim, qual dificuldade?

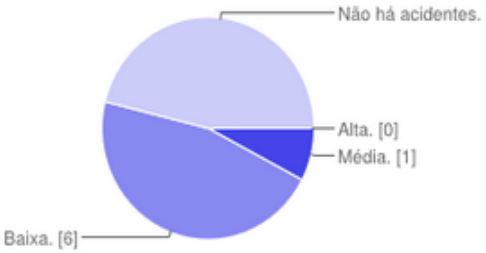
Não tem firewall. | não sei | não | Nao. | Não. | naão | Não, o mesmo foi feito terceirizado. | não | não sei | não | sim, pouco conhecimento em software livre | não | Não sei.

Qual é a taxa de acidentes em TI (desastres naturais, invasões, roubos de equipamentos, perda de informações, etc)?



Alta.	0	0%
Media.	1	8%
Baixa.	6	46%
Não há acidentes.	6	46%

Qual a gravidade destes acidentes?

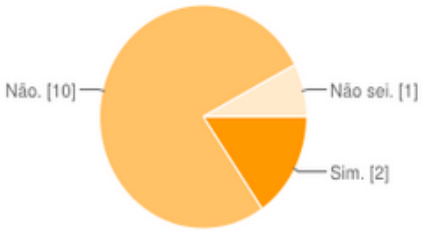


Alta.	0	0%
Média.	1	8%
Baixa.	6	46%
Não há acidentes.	6	46%

Possui algum sistema responsável pelo backup (cópia rotineira da informação da empresa)? Caso sim, qual?

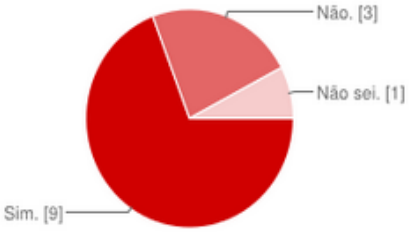
Sim. Em formas de mídias de dvd diárias feitas pelo funcionário de TI e no hd espelhado do servidor reserva e no hd2 do servidor principal. | Manual | sim. scripts em bash | Não. | Possui. Sistema desenvolvimento por equipe DBA (equipe terceirizada) para backup de banco de dados. Para outros arquivos backup feito por sistema criado pela própria DPC. os backups são feitos em servidores, fita e dvd. | sim | sim, cobian. | sim, espelhamento dos servidores backup em hd externo | sim, não sei qual é o sistema | sim. Server 2008 | sim, Cobyan Backup | sim, um software que vem juntamente com um armazenador de dados | Não.

O backup é criptografado para proporcionar sua melhor proteção?



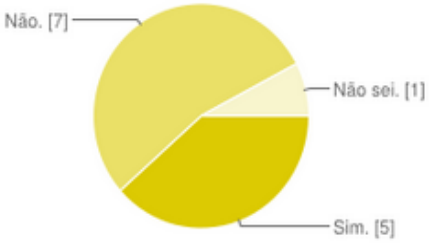
Sim.	2	15%
Não.	10	77%
Não sei.	1	8%

Há uma preocupação sobre o local onde é armazenado a mídia do backup?



Sim.	9	69%
Não.	3	23%
Não sei.	1	8%

A empresa se preocupa em investir em mídias de backup mais eficientes (com maior durabilidade)?



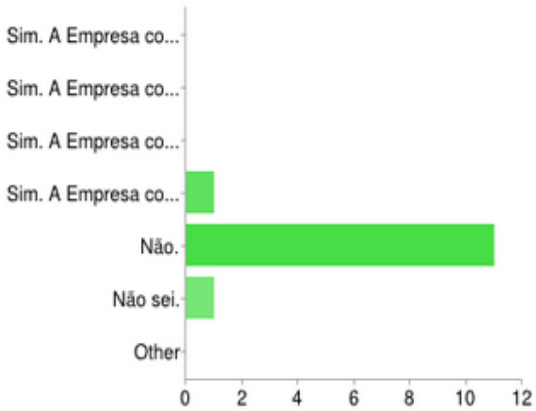
Sim.	5	38%
Não.	7	54%
Não sei.	1	8%

Quanto tempo que os backups são mantidos antes de sua remoção?

30 dias | 15 dias | 6 meses | Nao sei. | 1 mês | por meses | uma semana | 3 meses | não sei | 24hrs | 6 meses | 7 dias | Não

Normas de Segurança da Informação

A empresa baseia-se em alguma norma de segurança para formular a sua política interna? Qual?

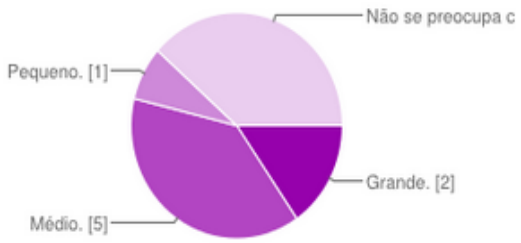


Sim. A Empresa conhece a norma RFC 2196.	0	0%
Sim. A Empresa conhece a norma RFC 17099.	0	0%
Sim. A Empresa conhece a norma BS 7799.	0	0%
Sim. A Empresa conhece a norma ISO/IEC 27000.	1	8%
Não.	11	85%
Não sei.	1	8%
Other	0	0%

Os funcionários que trabalham no setor de segurança possuem alguma certificação em alguma norma de segurança? Caso sim, qual(s)?

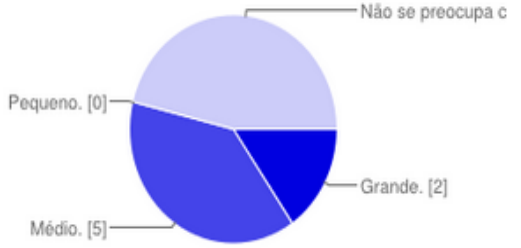
Não. dois em graduação. não Nao. não não não sei não sim, não sei não não não Não possui um setor responsável pela segurança.

Qual o nível de investimento ou incentivo da sua empresa na preparação (cursos, treinamentos, palestras, etc.) de seus funcionários de TI?



Grande.	2	15%
Médio.	5	38%
Pequeno.	1	8%
Não se preocupa com isso.	5	38%

Qual o nível de investimento ou incentivo da sua empresa na preparação (cursos, treinamentos, palestras, etc.) de seus funcionários de Segurança da Informação?



Grande.	2	15%
Médio.	5	38%
Pequeno.	0	0%
Não se preocupa com isso.	6	46%

OBSERVAÇÃO / COMENTÁRIOS

Infelizmente, em cidades pequenas como Caratinga, não existe gestor e sim empresário, a causa disso é ineficiência de investimentos em todas as áreas dentro da empresa, principalmente a de TI, onde o empresário apenas pensa no lucro e não no gasto. sem comentários É de interesse da empresa investir em um sistema de prevenção de queda de internet, onde, o serviço de internet seria prestado por vários provedores e no caso de queda de um, o outro funcionaria. Há uma preocupação na área de segurança pois o sistema é integrado com o sistema da CEMIG e pela a visão que esta tem os nossos dados pode ...