FACULDADE DE ADMINISTRAÇÃO E NEGÓCIOS DE SERGIPE
FANESE
ESPECIALIZAÇÃO EM GESTÃO DE REDES E SEGURANÇA DA INFORMAÇÃO

GEAN CARLOS SILVA GERMANO

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO
ESTUDO DE CASO:
GW COSTRUÇÕES S/A.

Aracaju - SE
2015

GEAN CARLOS SILVA GERMANO

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO
ESTUDO DE CASO:
GW COSTRUÇÕES S/A.

Trabalho de Conclusão de Curso apresentado ao núcleo de Pós-Graduação e Extensão da FANESE, como requisito para obtenção do título de Especialista em Gestão de Redes e Segurança da Informação.

Coordenador: Prof. Esp. Luciano Cerqueira Passos

Aracaju - SE
2015

RESUMO

Este trabalho tem como objetivo apresentar um estudo de caso sobre política de segurança da informação em uma organização privada, onde foram analisados todos os objetivos de controle e os controles relacionados à segurança da informação implementados nesta organização. Serão mostrados os principais problemas, e também as ações utilizadas até então neste processo. São feitas avaliações quanto à conformidade da gestão de segurança da informação desta organização em relação às normas da família ISO 27000, sobretudo em relação à norma NBR ISSO/IEC 17799 - Código de Conduta de Gestão de Segurança da Informação e à norma ABNT NBR ISO/IEC 27001 - Sistemas de Gestão de Segurança da Informação - Requisitos. Serão avaliados também fatores críticos de sucesso à gestão de segurança da informação em organizações como, por exemplo, o apoio da alta administração, a participação de todas as áreas e a conscientização e capacitação em segurança da informação.

Além de todos estes resultados, é abordado também a importância e pertinência da técnica de estudo de caso em pesquisas de gerenciamento de segurança da informação em ambientes organizacionais.

Palavras-chave: segurança da informação, normas, política da segurança da informação, processos, controles.

SUMÁRIO

1. INTRODUÇÃO

A segurança da informação é de extrema importância, e fundamental para garantir o bom funcionamento, de todos os sistemas e evitar que pessoas mal intencionadas capturem informações essenciais da empresa.

Atualmente a informação tornou-se um ativo mais valioso para as grandes empresas, no mesmo tempo, que passou a exigir uma segurança mais adequada. A tecnologias de informação e comunicação está crescendo de forma rápida, fazendo com que a maioria das empresas tenham maior eficiência e rapidez nas tomadas de decisão, por isso a empresa WG Construções S/A, da extrema importância a segurança da informação, que é essencial para a sobrevivência e competitividade da instituição.

Inicialmente será apresentando uma visão geral sobre Segurança da Informação, e os princípios básicos, a segurança da informação visa ajudar grandes números de ameaças para assegurar a continuidade do negócio. Esta segurança é obtida a partir da implementação de uma série de controles, que podem ser políticas, práticas e procedimentos, os quais precisam ser estabelecidos para garantir que os objetivos de segurança específicos da empresa sejam atendidos.

A política de segurança pode trazer ao ambiente da empresa, regras e procedimentos que devem ser seguidos por todos, para a garantia da segurança da informação. É importante que a política de segurança seja divulgada para todos os colaboradores, e que eles estejam cientes da importância do seguimento desta política.

2. *SEGURANÇA DA INFORMAÇÃO*

Para Marcos Sêmola (2014, p. 41) podemos definir segurança da informação como uma área do conhecimento dedicada ã proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sal indisponibilidade. De forma mais ampla, podemos também considera-lo como a prática de gestão de riscos incidentes que impliquem o comprometimento, dos três principais conceitos da segurança: confidencialidade, integridade e disponibilidade da informação. Dessa forma, estaríamos falando da definição de regras que incidiriam sobre todos os momentos do ciclo de vida da informação: manuseio, armazenamento, transporte e descarte, viabilizando a identificação e o controle de ameaças e vulnerabilidades.

3. *PRINCÍPIOS BÁSICOS*

Para Adriana Beal (2008, p. 1) segurança da informação pode ser entendida como o processo de proteger informações das ameaças para a sua integridade, disponibilidade e confidencialidade.

A segurança da informação visa, assim, a preservar ativos de informação, levando em conta três objetivos fundamentais:

- Confidencialidade:

Garantia de que o acesso à informação é restrito aos seus usuários legítimos.

- Integridade:

Garantia da criação legítima e da consistência da informação ao longo do seu ciclo de vida: em especial, prevenção contra criação, alteração ou destruição não autorizada de dados e informações. O objetivo de autenticidade da informação é englobado pelo de integridade, quando se assume que este visa a garantir não só que as informações permaneçam completas e precisas, mas também que a informação capturada do ambiente externo tenha sua fidedignidade verificada e que a criada internamente seja produzida apenas por pessoas autorizadas e atribuída unicamente ao seu autor legítimo.

- Disponibilidade:

Garantia de que a informação e os ativos associados estejam disponíveis para os

usuários legítimos de forma oportuna.

Alguns autores acrescentam a esses três objetivos o de legalidade (garantia de que a informação foi produzida em conformidade com a lei), ou ainda o de uso legítimo (garantia de que os recursos de informação não são usados por pessoas não autorizadas ou de maneira não autorizada). Essas preocupações, no entanto, são melhor classificadas como objetivos organizacionais, dois quais derivariam os requisitos de segurança necessários para proteger as informações sob os pontos de vista da confidencialidade, integridade e disponibilidade. Por exemplo, o objetivo de legalidade decorre da necessidade de a organização zelar para que as informações por ela ofertadas – em especial aquelas entregues a terceiros por determinação legal – sejam fidedignas e produzidas de acordo com as normas vigentes. Esse objetivo gera, no campo da segurança da informação, exigências no tocante à confidencialidade, integridade e disponibilidade de dados e informações (tais como requisitos de proteção do sigilo de informações pessoais, da consistência dos demonstrativos financeiros divulgados, da disponibilidade de serviços de informação e comunicação contratados pro clientes).

4. MECANISMOS DE SEGURANÇA

Um meio de se aplicar e suportar os princípios básicos de segurança da informação é a utilização de mecanismos e controles (físicos e lógicos), que podem ser encontrados em:

- Controle de Acesso Físico

Segundo Adriana Beal (2008, p. 81), um grupo específico de medidas preventivas é chamado barreiras de segurança. Uma barreira corresponde a qualquer obstáculo colocado para prevenir um ataque, podendo ser física (cerca elétrica, parede), lógica (processo de logon para acesso a uma rede) ou uma combinação de ambas (autenticação de indivíduos por dispositivo biométrico para concessão de acesso, catraca eletrônica, porta aberta por cartão magnético). A ISSO 17799 (item 7.1.1) utiliza a expressão perímetro de segurança, definindo-a como “quaisquer elementos que estabeleçam uma barreira ao acesso indevido”. Uma melhor definição para perímetro de segurança seria o contorno ou linha delimitadora de uma área ou região separada de outros espaços físicos ou lógicos por um conjunto qualquer de barreiras.

Exemplos de barreiras que podem ajudar a formar um perímetro de segurança incluem salas-cofre, roletas de controle de acesso físico e uso de token ou dispositivo

biométrico para autenticação de pessoas antes da liberação da passagem. Medidas detectivas de invasão de um perímetro de segurança podem incluir circuitos internos de TV, alarmes e sirenes e detectores de incêndio; entre outras medidas preventivas ou redutoras do impacto disponíveis estão os climatizadores de ambiente, detectores de fumaça e acionadores de água para combate a incêndio.

A ISSO 17799 recomenda para a segurança física a consideração das seguintes diretrizes e controles de segurança (item 7.1.1):

- Perímetro de segurança claramente definido.
- Perímetro de prédios ou locais que contenham recursos de processamento de dados fisicamente consistente (sem brechas que facilitem a invasão).
- Implantação de área de recepção ou outro meio de acesso físico ao local ou prédio e restrição do acesso apenas a pessoas autorizadas.
- Barreiras físicas estendidas da laje do piso até a laje superior, quando necessário para prevenir acessos não autorizados ou contaminação ambiental causada por fogo, inundação, fumaça etc.
- Portas de incêndio no perímetro de segurança com sensores de alarme e mola para fechamento automático.

4.2 Controle de Acesso Lógico

O controle de acesso lógico é um conjunto de medidas e procedimentos com o objetivo de proteger os dados, os programas e sistemas contra possíveis tentativas de acesso não autorizadas.

Ainda segundo Adriana Beal (2008, p. 92), com relação ao ambiente de usuário final, exemplos de controles lógicos adicionais aplicáveis são a ativação de função de time out (desativação automática de uma sessão de usuário após determinado tempo de inatividade na estação de trabalho, exigindo novo fornecimento de ID e senha para reativá-la), proteção de tela com senha, desconexão de terminal conectado a computador de grande porte quando a sessão é finalizada e limitação automática do acesso a horários de uso autorizado.

A melhor forma de se compreender o problema da segurança lógica e identificar as medidas de proteção mais adequadas é segmentar o problema em área: segurança de redes, segurança de aplicativos, segurança de sistema e segurança do ambiente de usuário final.

- Segurança de redes:

As redes ampliam enormemente os riscos para a segurança de dados, informações e serviços de informação. Atualmente, as redes já se confundem com o próprio negócio: pressionadas pela necessidade de comunicação, organizações públicas e privadas acabam desenvolvendo redes de informação complexas e sofisticadas, que incorporam tecnologias cada vez mias diversificadas, como técnicas de criptografia, voz sobre IP (VoIP), acesso remoto e sem fio, serviços Web, sistemas de armazenamento distribuído de dados etc. Essas redes se tornam cada vez mais permeáveis, à medida que parceiros de negócio passam a ter acesso a serviços via extranets, clientes interagem com a rede usando transações de comércio eletrônico ou processos de CRM (customer relationship management, ou gestão de relacionamento com clientes) e funcionários se conectam aos sistemas corporativos usando redes privadas virtuais (VPNs).

Toda essa complexidade torna as redes mais e mais vulneráveis a ameaças provenientes de hackers, criminosos agindo via Internet, funcionários descontentes, concorrentes desleais e outros agentes interessados em cometer abusos. Com o aumento das vulnerabilidades e do interesse de pessoas mal-intencionadas em obter vantagens, não é de se estranhar que as pesquisas sobre segurança indiquem um crescimento acentuado dos ataques às rede a cada ano.

Garfinkel e Spafford (1996, p. 809-810) descrevem alguns casos de quebra de segurança de rede com consequências graves para as organizações envolvidas, como o do hacker Kevin Mitnik, que na década de 90 supostamente invadiu a rede da Netcom Communications, empresa prestadora de serviços de comunicação, e obteve uma cópia completa da base de dados de sua clientela, incluindo o número de cartão de crédito de mais de 30.000 clientes. Obviamente, havia falhas graves de segurança na organização, que mantinha informações confidenciais dessa natureza num sistema que podia ser acessado via Internet.

- Segurança de software:

A segurança de software diz respeito ao uso de controles embutidos nos próprios programas, que operam independentemente das medidas de proteção a que estão submetidas as redes, complementando-as (no caso do comércio eletrônico, por exemplo, as complexidades dos requisitos de segurança acabam levando à necessidade de implementação de controles nos próprios aplicativos para assegurar a confidencialidade de dados, uma vez

que não existem garantias suficientes de que as redes ofereçam o alto nível de proteção exigido para esse tipo de transação).

- Segurança de sistemas aplicativos:

A segurança de sistemas aplicativos pode demandar diversos tipos de controle, de acordo com os requisitos de segurança existentes:

- Validação de entrada de dados (verificações de duplicidade de registros, valores fora dos limites aceitáveis, caracteres inválidos, dados ausentes, incompletos ou excessivos, não autorizados ou inconsistentes).
- Controle do processamento interno (restrições usadas para minimizar o risco de falhas causadas por erro de processamento ou ações intencionais que possam levar à perda de integridade dos dados).
- Validação da saída (verificações da plausibilidade dos dados de saída, conciliação de valores e outros testes para garantir que os relatórios e os dados de consulta produzidos sejam válidos e completos).
- Controle da transmissão de mensagens (verificações para detectar modificações não autorizadas ou corrupção no conteúdo de mensagens transmitidas eletronicamente e para proteger esse conteúdo da divulgação indevida).

- Segurança de software utilitários:

Por oferecer oportunidades para que usuários mal-intencionados se desviem dos controles de acesso existentes na rede, os programas utilitários oferecem uma preocupação específica no âmbito da segurança de software. No item 9.5.5 da ISO 17799 são indicados alguns controles especialmente aplicáveis no caso dos softwares utilitários: remoção do ambiente de SI/TI de todos os utilitários que não estejam em uso, segregação entre área de utilitários e área de aplicativos, restrição do acesso a um número mínimo de usuários formalmente autorizados e limitação da disponibilidade dos utilitários ao período em que são necessários para a realização de atividades planejadas.

- Segurança do ambiente de usuário final:

Proteger o ambiente de usuário final pode exigir, além das medidas de proteção aplicadas às redes, softwares e comunicações, controles relativos a aspectos como compartilhamento de recursos e áreas de armazenamento de informações e uso de computação móvel. Medidas de proteção aplicáveis ao ambiente de usuário final incluem:

- Controles adequados à proteção de informações críticas que precisem ser compartilhadas (por exemplo, em projetos ou planos de natureza confidencial), para restringir o acesso aos membros da equipe ou grupo encarregada do seu desenvolvimento (essa proteção pode exigir o uso de software para encriptação de informações sigilosas).
- Controles adequados para a atualização permanente de antivírus e softwares de verificação da segurança.
- Uso de firewall pessoal para proteção da estação de trabalho.
- Procedimento de logon (entrada no sistema) que limitem o tempo máximo para sua conclusão e o número máximo de tentativas de entrada.
- Políticas e controles relacionados ao uso de equipamentos portáteis, como laptops, hand-helds etc.

5. POLÍTICA DE USO

Tem como objetivo, apresentar a forma, de como os recursos de informática serão utilizados por todos os funcionários da empresa. Para manter os recursos de informática em bom funcionamento, as seguintes orientações devem ser respeitadas, caso não, penalidades serão aplicadas, segue:

- Não é permitido o acesso à Internet para uso de bate-papo, chats e afins ;
- Não é permitida a navegação nos sites com conteúdo, pornográfico e de caráter sexual, pornografia infantil (pedofilia), apologia ao terrorismo e às drogas, violência e agressividade (racismo, preconceito, etc.), e conteúdo impróprio, ofensivo, ilegal, discriminatório, e similares;
- Programas de computador: permitido a utilização apenas os programas instalados e homologados pela equipe de TIC – Tecnologia da Informação e

Comunicação: Fica terminantemente proibido:

- Instalação de qualquer tipo de jogos;
- Instalação de qualquer tipo de programa sem o conhecimento e autorização da equipe de TIC – Tecnologia da Informação e Comunicação;

- Não revelar minha senha de acesso a rede corporativa, computadores, Internet e/ou de minha caixa postal (e-mail) coorporativo a ninguém e tomar o máximo de cuidado para que ela permaneça somente de meu conhecimento;
- Não é permitida a troca de arquivos de vídeo ou música;
- Caso observe algum problema no equipamento que você está utilizando, não tente resolver sozinho, chame a equipe de TIC – Tecnologia da Informação e Comunicação;
- Não me ausentar da estação de trabalho sem encerrar a sessão de uso do navegador (browser), sem bloquear estação de trabalho, bem como encerrar a seção do email corporativo, garantindo assim a impossibilidade de acesso indevido por terceiros;

O usuário assumirá a responsabilidade por dano causado por algum procedimento de iniciativa própria de tentativa de modificação da configuração, física ou lógica, do computador e/ou rede sem a autorização expressa equipe de TIC – Tecnologia da Informação e Comunicação;

6. ESTUDO DE CASO

A empresa analisada WG Construções S/A, tem 2 unidades em Sergipe. Sendo o Setor de Tecnologia da Informação no escritório central em Estância/SE. Possui um único link dedicado via par metálico (OI/Telemar). O negócio da empresa é baseado no Sistema da Totvs. O Sistema da Totvs abrange todas as áreas da empresa. Cada usuário tem seu nível de visão, baseado na função exercida na Empresa. Portanto o Sistema da Totvs, é um possível alvo para invasões e posteriormente roubo de informações valiosas ou alterações. Causando enormes perdas financeiras para a empresa. A Empresa WG Construções S/A, trabalha no ramo de Fabricação de estruturas pré-moldadas de concreto armado, em série e sob encomenda, constrói linhas e redes elétricas para todo o sul do Estado de Sergipe fazendo inclusive eletrificação rural.

A empresa WG Construções S/A, não possui hoje Política de Segurança e nenhum Plano de Continuidade de Negócios. Atualmente tem cerca de 90 colaboradores, em sua sede possuí 30 Computadores entre os setores: RH, Financeiro, contábil, e a alta direção. Possuí três servidores onde estão instalados e configurados todos os sistemas e arquivos que a empresa precisa para está funcionando, como servidor de Banco de Dados, File Server, Firewall, etc. Todos os departamentos possuem acesso à rede mundial de computadores à Internet via Proxy, os computadores tem acesso à internet por um firewall que atualmente está descontinuado. A situação atual é preocupante, precisando realizar várias melhorias para garantir que a informação esteja segura.

6.1 Teste de Conformidade – Atual

De acordo com a Norma NBR ISSO/IEC 17799 (Código de Conduta de Gestão de Segurança da Informação) na avaliação atual a empresa possui:

1. POLÍTICA DE SEGURANÇA	**Sim**	**Sim, porém desatualizada**	**Não**
Política de segurança?			X
Algum responsável pela gestão da política de segurança?			X

2. SEGURANÇA ORGANIZACIONAL	**Sim**	**Sim, porém desatualizada**	**Não**
Infraestrutura de segurança da informação para gerenciar as ações corporativas?			X
Fórum de segurança formado pelo corpo diretor, a fim de gerir mudanças estratégicas?			X
Definição clara das atribuições de responsabilidade associadas à segurança da informação?			X
Identificação dos riscos no acesso de prestadores de serviço?			X
Controle de acesso específico para os prestadores de serviço?	X		
Requisitos de segurança dos contratos de terceirização?			X

3. CLASSIFICAÇÃO E CONTROLE DOS ATIVOS DE INFORMAÇÃO	**Sim**	**Sim, porém desatualizada**	**Não**
Inventário dos ativos físicos, tecnológicos e humanos?		X	
Critérios de classificação da informação?			X
4. SEGURANÇA EM PESSOAS	**Sim**	**Sim, porém desatualizada**	**Não**
Critérios de seleção e política de pessoal?			X
Acordo de confidencialidade, termos e condições de trabalho?			X
Processos para capacitação e treinamento de usuários?	X		
Estrutura para notificar e responder aos incidentes e falhas de segurança?			X

5. SEGURANÇA FÍSICA E DE AMBIENTE	Sim	Sim, porém desatualizada	Não
Definição de perímetros e controle de acesso físico aos ambientes?		X	
Recursos para segurança e manutenção dos equipamentos?			X
Estrutura para fornecimento adequado de energia?	X		
Segurança de cabeamento?	X		

6. GERENCIAMENTO DAS OPERAÇÕES E COMUNICAÇÕES	Sim	Sim, porém desatualizada	Não
Procedimentos e responsabilidades operacionais?			X
Controle de mudanças operacionais?			X
Segregação de funções e ambientes?	X		
Planejamento e aceitação de sistemas?		X	
Procedimentos para cópias de segurança?		X	
Controles e gerenciamento de Rede?			X
Mecanismos de segurança e tratamentos de mídias?			X
Procedimentos para documentação de sistemas?			X
Mecanismos de segurança do correio eletrônico?			X

7. CONTROLE DE ACESSO	Sim	Sim, porém desatualizada	Não
Requisitos do negócio para controle de acesso?			X
Gerenciamento de acessos do usuário?	X		
Controle de acesso à rede?	X		
Controle de acesso ao sistema operacional?	X		
Controle de acesso às aplicações?	X		
Monitoração do uso e acesso ao sistema?			X
Critérios para computação móvel e trabalho remoto?			X

8. DESENVOLVIMENTO E MANUTENÇÃO DE SISTEMAS	Sim	Sim, porém desatualizada	Não
Requisitos de segurança de sistemas?			X
Controles de criptografia?			X
Mecanismos de segurança nos processo de desenvolvimento e suporte?			X

9. GESTÃO DA CONTINUIDADE DO NEGÓCIO	Sim	Sim, porém desatualizada	Não
Requisitos de segurança de sistemas?			X

10. CONFORMIDADE	Sim	Sim, porém desatualizada	Não
Gestão de conformidades técnicas e legais?			X
Recursos e critérios para auditoria de sistemas?			X

Segundo Sêmola, de acordo com a Norma NBR ISSO/IEC 17799 (Código de Conduta de Gestão de Segurança da Informação), a avaliação atual teve um resultado de 22

pontos, conforme descriminado logo abaixo, a situação está em fase de muita atenção:

"Resultado entre 26-0

Cuidado! A situação não é confortável para a empresa. A segurança da informação não está sendo tratada como prioridade e a pontuação indica a ausência ou ineficácia de muitos dos controles recomendados pela norma. As causas podem ser o desconhecimento dos riscos e a falta de sensibilização dos executivos e da alta administração. Arrisco dizer que seu segmento de mercado não vive um momento muito competitivo ou que a segurança não seja vista por seus clientes como um fator crítico de sucesso por conta da natureza de sua atividade. Outra hipótese é que devem estar ocorrendo ações isoladas - de um departamento ou de outro - que apesar de louváveis, não distribuem uniformemente a segurança e acabam por minimizar o aumento do nível de segurança do negócio".

6.2 Plano de implantação da segurança

O plano de implantação da segurança vem apresentar a solução para que todos os objetivos sejam alcançados.

- Atualização tecnológica da infraestrutura de servidores e demais ativos de rede;
- Migração dos servidores atuais para nova tecnologia de virtualização;
- Garantir alta disponibilidade e a segurança da informação.

Inicialmente propomos realizar a aquisição de Hardware e Software para uma nova reestruturação da infraestrutura de rede para apoiar o negócio da empresa. Colocamos o servidor de Banco de dados em Cluster como os demais serviços: File Server, AD e o ERP em Cluster NLB, usando recurso de virtualização. Colocamos também servidor de backup e antivírus, WSUS em cluster. Propomos implantar dois firewalls ASA como firewall de borda e dois UTMs como firewall interno, aumentando assim a segurança da organização. Sugerimos implantar dois links redundantes de internet de operadora diferentes, com o intuito de minimizar a falta de conexão com o provedor de correio eletrônico. Para aumento da segurança foi criado também, uma rede segmentada com VLANS departamentais, restringindo assim o acesso entre as mesmas. E por fim contratar uma empresa especializada para fazer uma análise da Segurança da Informação e propor uma política que venha atender as necessidades da empresa, segundo as normas para atingir a segurança é de extrema importância.

6.3 Projetos a serem aprovados

Para que possamos alcançar todos os resultados diante do que foi analisado no cenário atual, seguem os projetos por ordem de prioridade a serem aprovados.

Projetos	Prioridade
Solução de Hardware e Software de Backup	0
Cluster para banco de dados e aplicações	0
Storage SAS para aplicações críticas	0
Virtualização	0
Firewalls em Back-to-Back	0
Política de segurança	1
Segmentação da rede	1
Monitoramento de rede	2
Rede sem fio	2
Contrato E-mail 365(Nuvem)	3
Link internet redundante	3

6.4 Retornos do investimento

Com a implantação dos projetos, a empresa contará com os seguintes benefícios:

- Aumento expressivo da velocidade de acesso aos dados;
- Com a solução de virtualização, a empresa irá trabalhar de forma redundante, onde caso uma máquina falhar a outra assume suas funções automaticamente garantindo a disponibilidade do ambiente;
- Ter uma organização de TI adequada às necessidades do negócio e capaz de agregar mais valor à organização.
- Com a contratação de empresa especializada em segurança da informação, irá oferecer, além da economia eventual de seus recursos humanos, melhorias no uso dos investimentos efetuados em ferramentas, redução de ocorrências que demandam ações de reparação de outras áreas, tempo de resposta melhor para continuidade dos negócios, em contrapartida a compromissos e responsabilidades.

6.5 Complexidade

Segue tabela mostrando os Projetos x Complexidade por fase.

Primeira Fase: Prioridade 0	**Complexidade**
Solução de Hardware e Software de Backup	Alta
Cluster para banco de dados e aplicações	Alta
Storage SAS para aplicações críticas	Alta
Virtualização	Alta
Firewalls em Back-to-Back	Alta
Primeira Fase: Prioridade 1	**Complexidade**
Política de segurança	Média
Segmentação da rede	Baixa
Primeira Fase: Prioridade 2	**Complexidade**
Monitoramento de rede	Baixa
Rede sem fio	Média
Primeira Fase: Prioridade 3	**Complexidade**
Contrato E-mail 365(Nuvem)	Média
Link internet redundante	Média

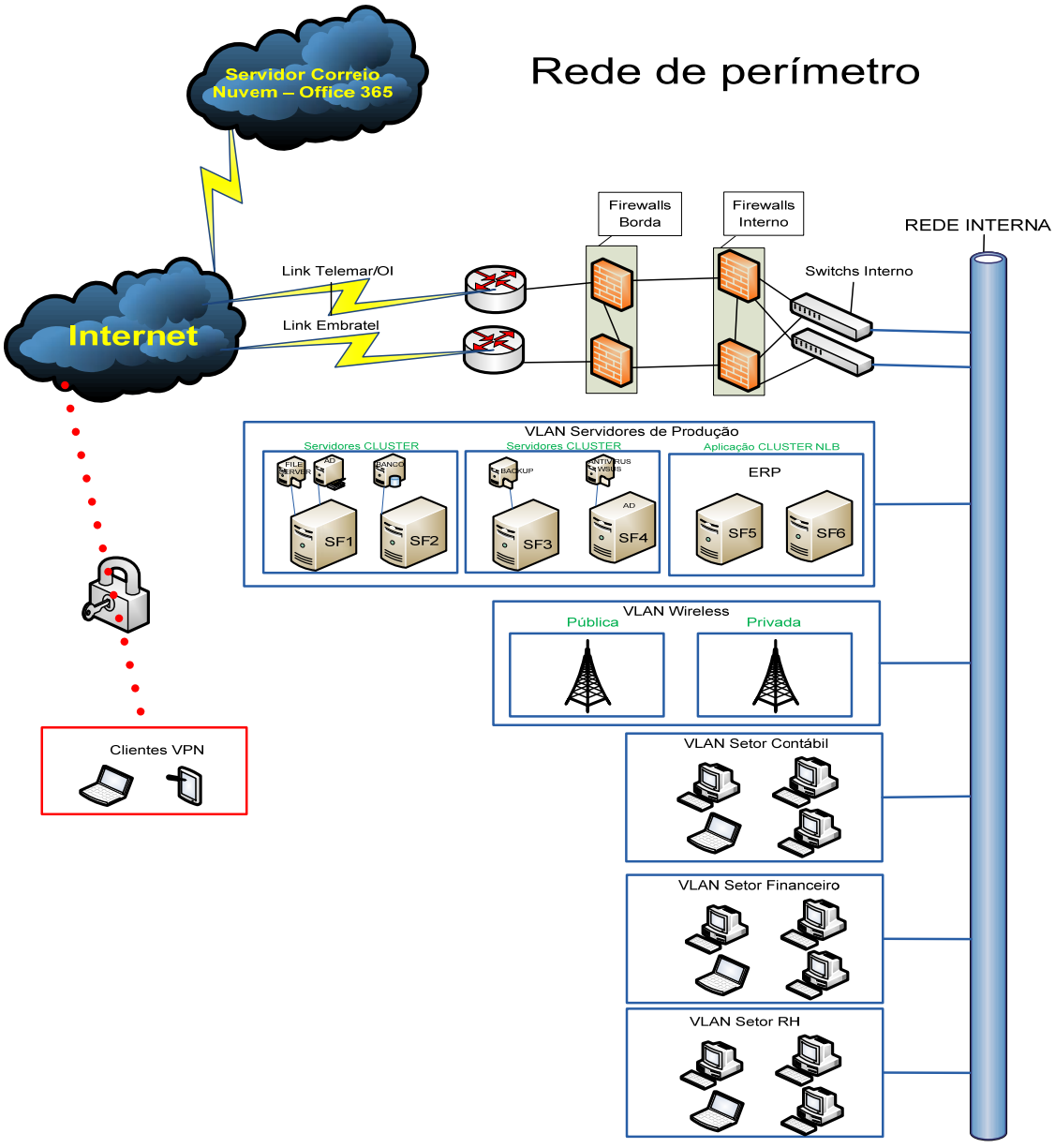
6.6 Custo

De acordo com a prioridade na execução dos projetos, os investimentos a serem aprovados estão divididos em quatro fases:

Primeira Fase: Prioridade 0	**Valor**
Solução de Hardware e Software de Backup	R$ 254.000,00
Cluster para banco de dados e aplicações	
Storage SAS para aplicações críticas	
Virtualização	
Firewalls em Back-to-Back	
Primeira Fase: Prioridade 1	**Valor**
Política de segurança	R$ 15.000,00
Segmentação da rede	

Primeira Fase: Prioridade 2	Valor	
Monitoramento de rede	R$	8.000,00
Rede sem fio		
Primeira Fase: Prioridade 3	**Valor**	
Contrato E-mail 365(Nuvem)	R$	12.600,00
Link internet redundante		
Total Geral	R$	289.600,00

6.7 Diagrama de rede - proposto



6.8 Teste de Conformidade – Proposto

Segundo NBR ISO/IEC 17799, tem como principal característica descrever controles preventivos, em sua grande maioria, evitando a ocorrência de incidentes envolvendo as informações corporativas, visando reduzir o tempo de exposição ao risco, que permitem detectar, de maneira mais rápida e efetiva, eventuais violações às regras do Sistema.

1. POLÍTICA DE SEGURANÇA	**Sim**	**Sim, porém desatualizada**	**Não**
Política de segurança?	X		
Algum responsável pela gestão da política de segurança?	X		

2. SEGURANÇA ORGANIZACIONAL	**Sim**	**Sim, porém desatualizada**	**Não**
Infraestrutura de segurança da informação para gerenciar as ações corporativas?	X		
Fórum de segurança formado pelo corpo diretor, a fim de gerir mudanças estratégicas?	X		
Definição clara das atribuições de responsabilidade associadas à segurança da informação?	X		
Identificação dos riscos no acesso de prestadores de serviço?	X		
Controle de acesso específico para os prestadores de serviço?	X		
Requisitos de segurança dos contratos de terceirização?	X		

3. CLASSIFICAÇÃO E CONTROLE DOS ATIVOS DE INFORMAÇÃO	**Sim**	**Sim, porém desatualizada**	**Não**
Inventário dos ativos físicos, tecnológicos e humanos?	X		
Critérios de classificação da informação?	X		
4. SEGURANÇA EM PESSOAS	**Sim**	**Sim, porém desatualizada**	**Não**
Critérios de seleção e política de pessoal?	X		
Acordo de confidencialidade, termos e condições de trabalho?	X		
Processos para capacitação e treinamento de usuários?	X		
Estrutura para notificar e responder aos incidentes e falhas de segurança?	X		

5. SEGURANÇA FÍSICA E DE AMBIENTE	**Sim**	**Sim, porém desatualizada**	**Não**
Definição de perímetros e controle de acesso físico aos ambientes?	X		
Recursos para segurança e manutenção dos equipamentos?	X		
Estrutura para fornecimento adequado de energia?	X		
Segurança de cabeamento?	X		

6. GERENCIAMENTO DAS OPERAÇÕES E	**Sim**	**Sim, porém**	**Não**

COMUNICAÇÕES		desatualizada	
Procedimentos e responsabilidades operacionais?	X		
Controle de mudanças operacionais?	X		
Segregação de funções e ambientes?	X		
Planejamento e aceitação de sistemas?	X		
Procedimentos para cópias de segurança?	X		
Controles e gerenciamento de Rede?	X		
Mecanismos de segurança e tratamentos de mídias?	X		
Procedimentos para documentação de sistemas?	X		
Mecanismos de segurança do correio eletrônico?	X		

7. CONTROLE DE ACESSO	Sim	Sim, porém desatualizada	Não
Requisitos do negócio para controle de acesso?	X		
Gerenciamento de acessos do usuário?	X		
Controle de acesso à rede?	X		
Controle de acesso ao sistema operacional?	X		
Controle de acesso às aplicações?	X		
Monitoração do uso e acesso ao sistema?	X		
Critérios para computação móvel e trabalho remoto?	X		

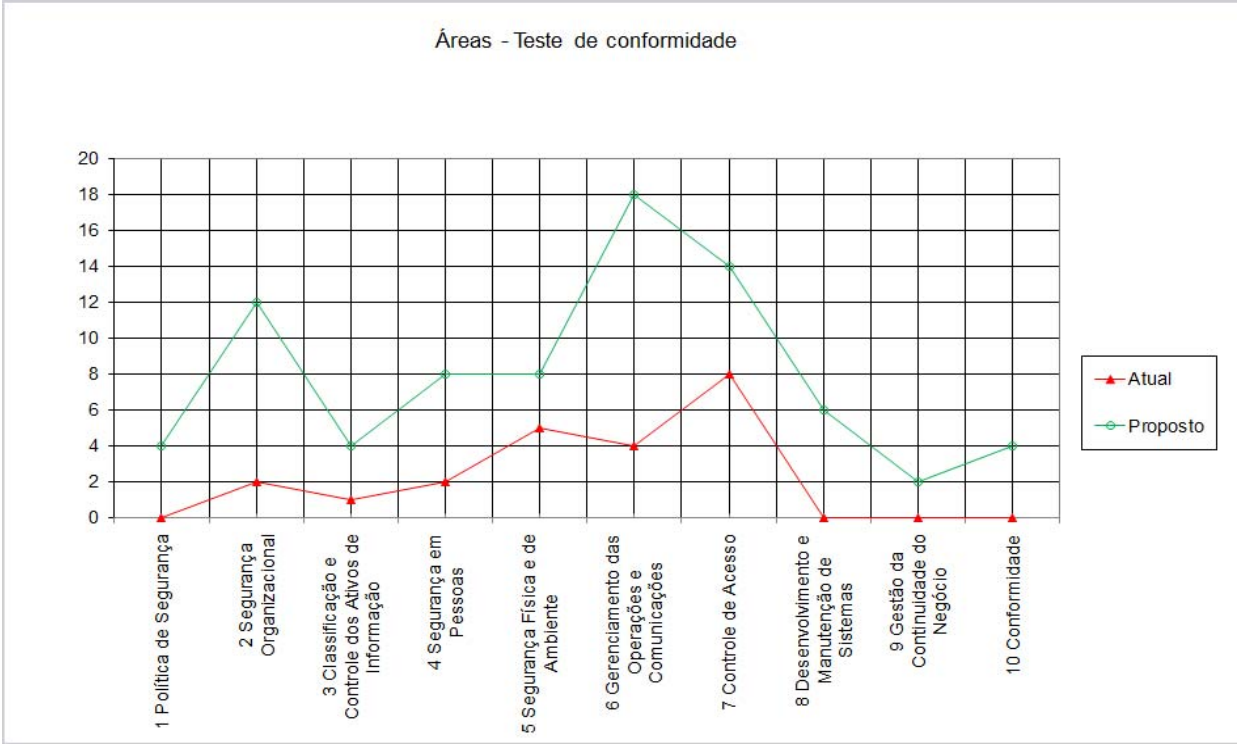
8. DESENVOLVIMENTO E MANUTENÇÃO DE SISTEMAS	Sim	Sim, porém desatualizada	Não
Requisitos de segurança de sistemas?	X		
Controles de criptografia?	X		
Mecanismos de segurança nos processo de desenvolvimento e suporte?	X		

9. GESTÃO DA CONTINUIDADE DO NEGÓCIO	Sim	Sim, porém desatualizada	Não
Requisitos de segurança de sistemas?	X		

10. CONFORMIDADE	Sim	Sim, porém desatualizada	Não
Gestão de conformidades técnicas e legais?	X		
Recursos e critérios para auditoria de sistemas?	X		

Após a implantação de novos recursos tecnológicos a nova avaliação teve como resultado 80 pontos, atingindo o nível mais alto segundo os critérios da norma Norma NBR ISSO/IEC 17799 (Código de Conduta de Gestão de Segurança da Informação).

6.9 Gráfico - teste de conformidade



7. CONSIDERAÇÕES FINAIS

Esse artigo se propôs como objetivo geral, mostrar que, a segurança de Informação é o elemento chave dentro da organização: envolvendo aspectos técnicos, humanos, etc, sendo de extrema importância a definição e existência de uma Política para efetiva proteção das informações. O objetivo da segurança da informação é proteger a organização contra riscos, apoiada em uma Política de Segurança e uma estrutura de Segurança, onde se podem identificar as vulnerabilidades e os controles para a proteção das informações.

Percebe-se que, a tarefa de implementação das principais práticas de segurança da informação na organização (NBR ISO/IEC 17799), não é tarefa fácil. Portanto, o ato de uma conscientização ampla da necessidade da adoção das práticas de segurança constitui-se em um grande passo tomado pela direção. Sempre lembrando que o melhor caminho não é a implantação compulsória, e sim a disseminação da cultura entre cada um dos ambientes da empresa. Uma vez que, nem todos os colaboradores entendem a necessidade de mecanismos de controle e de gerenciamento da segurança da informação.

Esse foi o objetivo principal deste trabalho, foi demonstrar a aplicação da norma NBR ISO/IEC 17799 dentro do âmbito de uma empresa, indicando controles necessários para garantirmos um nível maior de Segurança da Informação. Visto que, todo este trabalho deve ser em prol da defesa e segurança da informação, um dos bens mais valiosos de qualquer empresa.

.

REFERÊNCIAS

Sêmola, Marcos, **GESTÃO DA SEGURANÇA DA INFORMAÇÃO Uma Visão Executiva, 2ed.** Rio de Janeiro: Elsevier, 2014.

Beal, Adriana, **SEGURANÇA DA INFORMAÇÃO Princípios e Melhores Práticas para a Proteção dos Ativos de Informação nas Organizações,** São Paulo: Atlas, 2008.

Santos, Alfredo Luiz dos, **SEGURANÇA DA INFORMAÇÃO Gerenciamento de Identidades.** Rio de Janeiro: Brasport, 2007.

Fontes, Edison Luiz Gonçalves, **SEGURANÇA DA INFORMAÇÃO O Usuário faz a diferença.** São Paulo: Saraiva, 2006.

NORMA BRASILEIRA ABNT NBR ISO/IEC 17799. http://www.ciencianasnuvens.com.br/site/wp-content/uploads/2014/09/215545813-ABNT-NBR-177991.pdf. Acessado em 28 de Abril de 2015.

Dutra, Diana. **Norma iso - 17799 - Segurança da Informação**. http://www.ebah.com.br/content/ABAAAfdgcAK/norma-iso-17799-seguranca-informacao. Acessado em 28 de Abril de 2015.

Garcia, Paulo Sergio Rangel. **Analise Comentada da NBR ISO/IEC 17799: Uma contribuição para a gestão da segurança da informação**. http://www.feg.unesp.br/ceie/Monografias-Texto/CEIE0402.pdf. Acessado em 29 de Abril de 2015.

Casanas, Alex Delgado Gonçalves. **O Impacto da Implementação da NORMA NBR ISO/IEC 17799 – Código de Práticas para a Gestão da Segurança da Informação - Nas Empresas**. http://www.fatec.br/html/fatecam/images/stories/dspti_ii/asti_ii_material_apoio_3_seguranca_informacao_texto_base1.pdf. Acessado em 29 de Abril de 2015.

Martins, Alaíde Barbosa. **Uma Metodologia para Implementação de um Sistema de Gestão de Segurança da Informação**. http://www.scielo.br/pdf/jistm/v2n2/02.pdf. Acessado em 30 de Abril de 2015.

Baldissera, Thiago André. **Impacto na Implementação da Norma NBR ISO/IEC 17799 Para A Gestão da Segurança da Informação Em Colégios: Um Estudo de Caso**. http://www.abepro.org.br/biblioteca/enegep2007_tr640475_9300.pdf. Acessado em 30 de Abril de 2015.