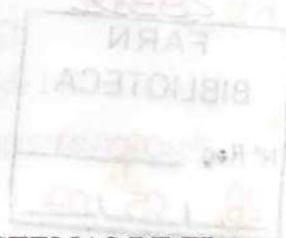


**LIGA DE ENSINO DO RIO GRANDE DO NORTE.
FACULDADE NATALENSE PARA O DESENVOLVIMENTO DO RIO GRANDE DO
NORTE.**

THALES ATHALIMAR FERREIRA DA SILVA

**UMA ABORDAGEM PARA AVALIAÇÃO DA SEGURANÇA EM SISTEMAS DE TI:
UM ESTUDO DE CASO NO RIFOLES PRAIA HOTEL & RESORT**

THALES ATHALIMAR FERREIRA DA SILVA



**UMA ABORDAGEM PARA AVALIAÇÃO DA SEGURANÇA EM SISTEMAS DE TI:
UM ESTUDO DE CASO NO RIFOLES PRAIA HOTEL**

Monografia apresentada ao Curso de Bacharelado em Sistemas de Informação da Faculdade Natalense para o Desenvolvimento do Rio Grande do Norte, como requisito obrigatório à obtenção do grau de Bacharel em Sistemas de Informação.

Orientador: Ytalo Rosendo do Amaral, M. Sc.

NATAL/RN

2006

THALES ATHALIMAR FERREIRA DA SILVA



004:658
5578a
2006
ex 01

Catálogo na Publicação – Biblioteca da FARN
Setor de Processos Técnicos

Silva, Thales Athalimar Ferreira da

Uma abordagem para avaliação da segurança em sistemas de TI: um estudo de caso no Rifolet Praia Hotel / Thales Athalimar Ferreira da Silva. – Natal: FARN, 2006.

62f.

Orientador: Ytalo Rosendo do Amaral (M.Sc.)

Monografia (Bacharelado em Sistemas de Informação) – Faculdade Natalense para o Desenvolvimento do Rio Grande do Norte.

1. Segurança em Tecnologia da Informação – Monografia. 2. Sistemas de Informação – Monografia. I. Título.

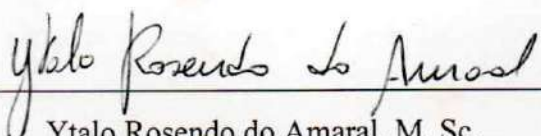
RN/FARN/BC

CDU 004:658

**UMA ABORDAGEM PARA AVALIAÇÃO DA SEGURANÇA EM SISTEMAS DE TI:
UM ESTUDO DE CASO NO RIFOLES PRAIA HOTEL**

Projeto de Monografia apresentado ao Curso de Bacharelado em Sistemas de Informação da
Faculdade Natalense para o Desenvolvimento do Rio Grande do Norte e aprovada em__de
_____de_____.

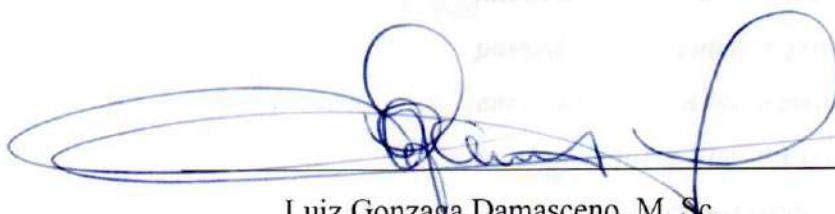
Pela banca examinadora composta pelos seguintes membros.


Ytalo Rosendo do Amaral, M. Sc.

Orientador

Luiz Augusto M. Machado Filho, M. Sc.

Membro Examinador (a)


Luiz Gonzaga Damasceno, M. Sc.

Membro Examinador (a)

Aos meus pais, que batalharam a vida toda para me concederem um estudo digno e assim uma vida melhor, dedico com amor e carinho esse trabalho, fruto de muito esforço, dedicação e estudo. Não posso deixar de dedicá-lo também a minha amada esposa, que por ter passado recentemente por um processo igual, em muito me ajudou nessa batalha. Dedico-lhe também àquele que em todos os momentos me deu força, luz e inspiração: Deus.

AGRADECIMENTOS

Agradeço a todos aqueles que intencionalmente ou não, me ajudaram diretamente ou indiretamente a conseguir desenvolver uma obra desse cunho, pois jamais havia desenvolvido um trabalho parecido e devido a minha ocupação na empresa onde trabalho ficou muito difícil.

Faço um agradecimento em especial ao professor Ytalo Rosendo, que, primeiramente aceitou orientar um aluno que já tinha sido rejeitado por sete outros orientadores, o que nitidamente denotava algo diferente nesse aluno. Segundo por ter me entendido nas ocasiões que por diversas vezes não pude comparecer nas orientações devido ao meu trabalho, e em terceiro lugar por ter dedicado um pouco do seu tempo a me ajudar a desenvolver esse trabalho.

Agradeço também a minha amada esposa, que muito me ajudou e por diversas vezes foi minha co-orientadora, pois havia acabado de fazer uma monografia, que devido a seu excelente desempenho ficou com nota máxima e dessa forma conseguiu passar-me muito para me ajudar a desenvolver esse trabalho.

Não posso deixar de agradecer aos meus queridos e estimados pais, que me deram forças e ajudaram-me de todas as formas não só a concluir esse trabalho, mas a conseguir chegar até essa etapa da minha vida.

Tive uma ajuda especial de uma pessoa que fez-me, mesmo sem intenção, relaxar-me e conseguir esquecer dos problemas da vida e assim esfriar a cabeça para desenvolver essa monografia. Ele, não apenas desviou meu pensamento para o lado positivo como também serviu como fonte inspiradora para que num futuro eu tivesse orgulho de mostrar-lhe essa obra. A meu filho Lucas Henrique muito obrigado.

Existem muitos amigos, que aqui na faculdade fiz, dos quais não posso deixar de agradecer pelo "empurrãozinho" das horas difíceis. Sem estes, não conseguiria fazer esse trabalho.

Ao senhor meu Deus, falta-me palavras para expressar minha gratidão e agradecimento de tudo o que ele me faz. Resumo-lhe em palavras o que meu coração expressa em sentimento: Muito obrigado e que a humanidade siga vossos ensinamentos, assim como eu tenho seguido.

RESUMO

A monografia aqui apresentada tem com finalidade realizar uma análise nos sistemas de informação do Rifóles Praia Hotel & Resort, do ponto de vista de segurança da informação, e expor ao findo da mesma, sugestões sobre como tornar seus sistemas de informação mais seguros. Para isso, foi realizada uma pesquisa aplicada, tendo os dados coletados através de questionário, composto de perguntas objetivas. Em média 63% dos colaboradores que utilizam seus sistemas de informação responderam. Os dados coletados foram receberam tratamento estatístico, o que permitiu a elaboração de tabelas com percentuais e gráficos explicativos. Levando em consideração os conceitos e teorias da segurança da informação abordados nessa monografia e através desta pesquisa, foi observado que a empresa encontra-se com vários tipos de vulnerabilidades de segurança da informação. Dentre as principais vulnerabilidades está o despreparo dos seus colaboradores e a falta de normas que regulamentem a segurança da informação.

Palavras-Chaves: Sistemas de Informação, Tecnologia da Informação, Segurança da informação.

ABSTRACT

The monograph presented here has with purpose to carry through an analysis in the systems of information of the Rifóles Beach Hotel & Resort, of the point of view of security of the information, and to display to findo of the same one, suggestions on as to become its safer systems of information. For this, an applied research was carried through, having the data collected through questionnaire, made up of objective questions. On average 63% of the collaborators whom they use its systems of information had answered. The collected data had been had received treatment statistical, what it allowed to the table elaboration with percentages and clarifying graphs. Taking in consideration the concepts and theories of the boarded security of the information in this monograph and through this research, it was observed that the company meets with some types of security vulnerabilities of the information. Amongst the main vulnerabilities it is the unpreparedness of its collaborators and the lack of one politics of internal security.

Key-words: Information Systems, Information Technology, Information Security.

LISTA DE SIGLAS

SI – Sistemas de Informação.	23
TI – Tecnologia da Informação.	23
ABNT – Associação Brasileira de Normas Técnicas.	23
ISO – International Standartization Organization (Organização de Padrões Internacionais).	23
IEC – International Engineering Consortium (Consórcio de Engenharia Internacional).	23
ABEP – Associação Brasileira de Empresas Estaduais de Processamento de Dados.	23
CPD – Centro de Processamento de Dados.	27
DNS – Domain Name Server (Servidor de Nomes de Domínio).	27
A&B – Alimentos e Bebidas.	27
NDA - Non Disclosure Agreement (Acordo de Não Revelação).	28
ROI – Retorno sobre investimento.	28
DTI – Departamento de Comércio e Indústria do Reino Unido.	27
CCSC – Comercial Computer Security Center (Centro Computacional de Segurança Comercial).	27
BS – British Standart (Pradrão Britânico).	27
NBR – Norma Brasileira.	27
RH – Recursos Humanos.	27
CDR – Compact Disk Read (Disco Compacto de Leitura).	27
CDRW – Compact Disk Read and Write (Disco Compacto de Leitura e Escrita).	27

LISTA DE GRÁFICOS

TABELA 1: Faixa etária dos funcionários.....	25
TABELA 2 – Sexo dos funcionários.....	25
TABELA 3 – Funções Operacionais X Gerencial.....	25
TABELA 4 – Tempo de serviço.....	26
TABELA 5 – Outras ocupações.....	26
TABELA 6 – Compartilhamento de senhas.....	26
TABELA 7 – Senhas de terceiros.....	27
TABELA 8 – Exposição de senhas.....	27
TABELA 9 – Senhas cedidas.....	27
TABELA 10 – Alteração de senhas.....	28
TABELA 11 – Fornecimento de informações.....	28
TABELA 12 – Informações confidenciais.....	29
TABELA 13 – Bloqueio de estação.....	29
TABELA 14 – Reconhecimento de informação.....	29
TABELA 15 – Importância da informação.....	30
TABELA 16 – Credibilidade na segurança em TI.....	30
TABELA 17 – Acesso à informações.....	30

SUMÁRIO

1. INTRODUÇÃO	1
1.1 Problema de Pesquisa	1
2. OBJETIVOS	3
2.1 Objetivo Geral	3
2.2 Objetivos Específicos	3
3. JUSTIFICATIVA	4
4. CARACTERIZAÇÃO DA EMPRESA	5
5. REFERENCIAL TEÓRICO	8
5.1 Informação	8
5.2 Tecnologia da Informação	8
5.3 Sistemas de Informação	8
5.4 Segurança da Informação	8
5.4.1 Descrição de Segurança da Informação	9
5.4.2 A importância da Segurança da Informação	9
5.4.3 Responsabilidade pela segurança da informação	9
5.5 Segurança dos Sistemas de Informação	10
5.6 Segurança Física em TI	11
5.7 Segurança Lógica	13
5.8 Segurança da Informação X Agregação de Valores a Empresa	13
5.9 Vulnerabilidade e Abuso em Sistemas	15
5.10 Atributos da Informação	16
5.11 Auditoria da Segurança da Informação	16
5.11.1 Dificuldades encontradas pela Auditoria de Sistemas na Empresa	17
5.11.2 Papel do auditor de sistemas	17
5.11.3 Importância da auditoria de sistemas	17
5.11.4 Etapas da atuação do auditor de sistemas	18
5.11.5 Perfil do Auditor de Sistemas	18
5.11.6 Necessidades na área de auditoria de sistemas	18
5.11.7 Conceituação de Auditoria de Sistemas	18
5.11.8 Tendências da Auditoria de Sistemas na Organização	19
5.12 ISO 17799	19
5.12.1 O surgimento da Norma Nacional de Segurança de Informação	19
5.12.3 Objetivos da Norma	20

5.12.4 Divisão da Norma Nacional de Segurança de Informação.....	20
6. METODOLOGIA.....	23
6.1 Tipo de Pesquisa.....	23
6.2 População e Amostra.....	23
6.3 Plano de Coleta de Dados.....	23
5.4 Análise dos Dados.....	24
7. RESULTADOS.....	25
8. CONCLUSÃO.....	31
REFERÊNCIAS.....	32
APÊNDICE A – Questionário aplicado aos usuários.....	34
APÊNDICE B - Política de Segurança.....	36

1. INTRODUÇÃO

Segundo Loureiro (1999, p. 22), cada vez mais é aceita a idéia de que o verdadeiro patrimônio de uma entidade é sua tecnologia, que compõe seus sistemas, processos e informações, fundamental para o seu funcionamento, garantindo a competitividade no mercado. Assim sendo, é perceptível que as empresas devem ter suas informações protegidas de acessos indevidos e de uma possível perda destas.

Contudo, para protegê-las se faz necessário um tratamento não só dos profissionais da área de TI, mas de todo o pessoal envolvido com processos que se utilizem de tecnologia dentro da empresa, e é aí onde está um ponto fraco a ser avaliado, pois de acordo com Costa (2004), a segurança da informação gera sempre muitas dúvidas nas pessoas que de uma forma ou de outra devem utilizá-la.

Essas dúvidas vão desde as mais básicas, como anotar sua senha de acesso em um lugar de fácil visualização, usar ou não o internet banking por se tratar de uma transação bancária realizada diretamente pela Internet, até as mais complexas, relacionadas a fraudes eletrônicas, como os e-mails falsos enviados em nome dos bancos aos correntistas, de empresas de créditos aos clientes, de órgãos governamentais aos cidadãos, clonagem de cartões de crédito e até o chamado redirecionamento de DNS, quando um computador finge se passar por outro para roubar informações.

Além de todas essas questões ainda existe a questão natural de falha de equipamentos, que numa determinada situação podem danificar dados e desta forma até parar o funcionamento da empresa. É nesse momento que se deve ter em mãos os backup's dos dados importantes à empresa e ao seu funcionamento devido.

Nem sempre as empresas estão preparadas para lidarem com os riscos trazidos com a informatização da informação. Por isso, trabalhos como este, que objetiva verificar e propor soluções para sanar esse tipo de situação estão cada vez mais sendo aplicado no mundo corporativo.

1.1 Problema de Pesquisa

No Rifóles Praia Hotel & Resort, após ser instalado seus sistemas de informação (SI), foi observado que estes ajudam muito no desenvolvimento das rotinas de trabalho, bem como no desenvolvimento da empresa como um todo. Contudo, passado os tempos atentou-se que todas as informações pertinentes à empresa circulavam dentro de um canal tecnológico (seu

sistema de informação) e que estas podem, intencionalmente ou não, cair em mãos de pessoas que não devam ter acesso àquelas informações. Surgiu-se então a preocupação de garantir a segurança dos SI e com ela veio à problemática: **Como proteger todo o sistema de TI de forma que fique seguro?**

2. OBJETIVOS

2.1 Objetivo Geral

Realizar uma análise nos sistemas de informação e toda área de TI do Rifoles Praia Hotel & Resort a fim de apresentar críticas sobre a segurança da informação nesses sistemas.

2.2 Objetivos Específicos

- Analisar qual o nível de entendimento sobre segurança da informação os colaboradores da empresa têm e como estes tratam esse assunto.
- Realizar uma análise na rede, utilizando softwares específicos, para examinar possíveis falhas nesta.
- Aplicar um check-list para verificar falhas de segurança em softwares e sistemas operacionais;

3. JUSTIFICATIVA

A informação de uma empresa é o seu principal patrimônio, fundamental para o seu funcionamento, garantindo a competitividade no mercado. Por isso, devemos protegê-las de acessos indevidos, pois estes podem vir a cair em mãos de concorrentes e afetar a estratégia, metas e planejamento da empresa. Além disso, devemos protegê-las, a fim de garantir a continuidade do negócio através da confidencialidade, integridade e disponibilidade da informação. Com base nisso, propõem-se ao Rifóles Praia Hotel & Resort a realização de uma análise de segurança a fim de encontrar vulnerabilidades, e caso haja, e apresentar-lhes um relatório conclusivo apontando-as e sugerindo soluções.

Conforme citado anteriormente é de suma importância para a empresa manter seus dados íntegros e confidentes, pois deles dependem diretamente os resultados financeiros que a empresa almeja. Esse trabalho dará ao Rifóles a oportunidade de ingressar no mundo das empresas que têm suas informações protegidas de ameaças que possam vir a desviar o crescimento e a prosperidade da empresa.

4. CARACTERIZAÇÃO DA EMPRESA

O projeto de erguer em algum lugar no Brasil um Hotel temático iniciou-se em meados de 1997, quando foi realizado um estudo de viabilidade econômica em várias capitais do país tendo Natal como a opção escolhida para a construção. A praia de Ponta Negra foi o local escolhido e as obras iniciaram em 2000, tendo sua finalização em setembro de 2001 com sua inauguração.

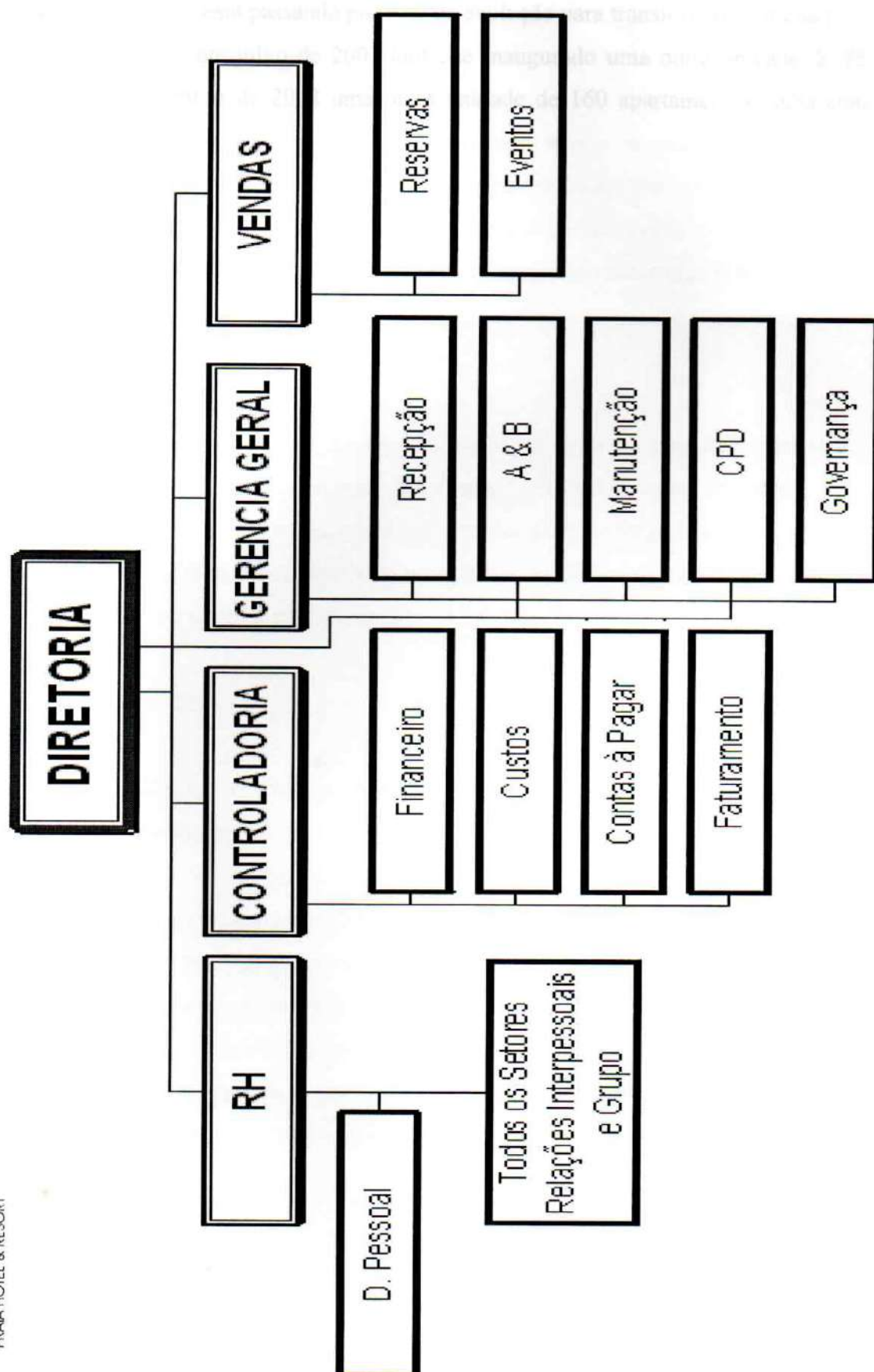
Com características de um navio pirata, o Hotel foi batizado por Rifóles Praia Hotel. O nome Rifóles vem de um corsário francês de nome Jaques Rifoult, que costumava atracar sua nau nas calmas águas do rio potengi e negociar com os nativos, que, por desconhecerem da língua francesa o chamavam de Rifóles.

O hotel foi inaugurado com 110 apartamentos, todos com vista para o mar, dois restaurantes, salão de eventos para 150 pessoas, um parque aquático com quatro piscinas e uma quadra poli esportiva, mirante, estacionamento, garagem, bar na piscina, bar molhado, serviços de lavanderia, autolocadora, room service 24 horas, massagem, recreação e telefonistas bilíngüe.

Em 2004 passou por uma reforma onde foi-lhe acrescidos mais 94 apartamentos, passando a ter 204 uh's (unidade habitacional), três restaurantes, seis piscinas, kids club, salão de beleza, spa com ofurô, fitness center, busines center, salão de eventos para até 600 pessoas e uma área verde de mais de 11km², que o deu a classificação de Resort, passando a ser chamado por Rifóles Praia Hotel & Resort.

O seu quadro funcional é composto por cento e noventa funcionários divididos nos setores de Recepção, Telefonia, A&B, Governança, Segurança e Administração. Abaixo, segue o organograma da empresa:





Em suma, esses são os departamentos hoje existentes no hotel.

Atualmente, o hotel está passando por fase de evolução para transformar-se numa rede de hotéis. Estimasse que até julho de 2007 tenha-se inaugurado uma outra unidade de 75 apartamentos e até dezembro de 2008 uma outra unidade de 160 apartamentos tenha sido construída também.

5. REFERENCIAL TEÓRICO

5.1 Informação

Segundo Ferreira (2004), informação é um dado acerca de alguém ou algo; o conhecimento. Segundo Silva (1997), informação são os resultados das análises dos dados que propiciarão ao executivo ou quem quer que seja o maior conhecimento para a tomada de decisão (escolha entre vários caminhos alternativos que levam a um determinado resultado).

5.2 Tecnologia da Informação

De acordo com Pinheiro (2006), a tecnologia da informação pode ser definida como a combinação de recursos de processamento (hardware, software, bancos de dados, etc), comunicações, pessoas e procedimentos, todos organizados de maneira a obter como produto final uma informação que atenda aos objetivos da organização. Esses recursos são destinados ao armazenamento, processamento e comunicação de informação.

5.3 Sistemas de Informação

Para Pinheiro (2004), um Sistema de Informação (ou, simplesmente SI) é um conjunto de componentes inter-relacionados que coletam, manipulam e disseminam dados e informação, proporcionando um mecanismo de realimentação (feedback) para atender a um objetivo determinado. Esse feedback representa a saída que será utilizada para promover eventuais mudanças na entrada ou nas atividades de processamento.

Os sistemas de informação estão difundidos por todas as funções organizacionais. Eles são usados por áreas como contabilidade, finanças, vendas, produção, controle e assim por diante. Conseqüentemente, esse uso generalizado aumenta a necessidade por novos sistemas cada vez mais complexos e por profissionais com conhecimento no seu desenvolvimento e gerenciamento.

5.4 Segurança da Informação

Este capítulo aborda alguns termos relacionados à estruturação da análise em segurança da informação no âmbito de TI, que são utilizados no decorrer desse trabalho.

Dessa forma são apresentados alguns aspectos importantes para o bom entendimento do estudo e seu contexto assim como explicações gerais acerca de segurança da informação como um todo.

5.4.1 Descrição de Segurança da Informação

Segundo a norma ISO/IEC (17799:2000),

A Segurança da informação pode ser definida como a proteção contra um grande número de ameaças às informações, de forma a assegurar a continuidade do negócio, minimizando danos comerciais e maximizando o retorno de possibilidades e investimentos. Machado (2004).

No entendimento de Machado (2004), segurança da informação trata-se de uma conjugação de estratégias e ferramentas específicas que atendam as necessidades corporativas para a manutenção de um ambiente saudável. Considerada um item vivo, a política de segurança nunca está terminada e deve ser desenvolvida e atualizada durante toda a vida da empresa.

5.4.2 A importância da Segurança da Informação

Segundo Uemura (2000), diretor da Abep (Associação Brasileira de Empresas Estaduais de Processamento de Dados), a Segurança da Informação está atrelada à Tecnologia da Informação quando vemos que se torna premissa a continuidade dos negócios, considerando seus investimentos e sobrevivência de uma corporação. É indispensável que uma organização mantenha algumas políticas de Segurança da informação como: backups de seus dados, planos de contingência, possibilidade confiável de recuperação de dados em caso de perda destes, gerenciamentos de segurança nas redes e internet, projeto de segurança lógica e de segurança física. Essas políticas não devem visar apenas o sucesso da organização, mas também garantir a confiabilidade e alta disponibilidade da informação.

5.4.3 Responsabilidade pela segurança da informação

De acordo com Ângelo (2005), a segurança da informação não cabe apenas aos profissionais de TI. Envolve a combinação de uma série de coisas. Não adianta empregar todos os recursos em firewall, antivírus e outras ferramentas do gênero e deixar a gestão da

segurança de lado. É preciso olhar para a tecnologia mais simples capaz de atender às necessidades da organização e gastar energia no gerenciamento de tudo. A área de TI deve conversar com os departamentos de recursos humanos e jurídico para, por exemplo, criar documentos capazes de proteger a empresa de seus próprios funcionários. Fazer o contratado assinar documentos como o de NDA (non disclosure agreement - Acordo de Não Revelação) é uma boa alternativa para assegurar que documentos confidenciais e essenciais para o negócio da empresa não deixarão as suas dependências. De nada adianta investir em tecnologia para gerar segurança, e deixar pontos primordiais, como o fator humano, de lado.

5.5 Segurança dos Sistemas de Informação

Para Batista (2004), a importância da segurança dos dados é uma característica especial para os sistemas de informação, entretanto, muitas empresas só dão a devida importância a esse fator quando sofrem o primeiro acidente que resulta em um considerável prejuízo.

Batista (2004) afirma que o imenso conjunto de vantagens trazidas pelos sistemas de informação pode ser facilmente descartado quando a organização despreza as características básicas de segurança de dados. Independentemente de ter ou não acesso a uma rede externa (internet por exemplo), a segurança é necessária ao computador. Só ela possibilita a minimização dos prejuízos por paralisações não esperadas, e garante a qualidade dos dados inseridos, das informações neles geradas, e assegura que estes não sejam roubados ou alterados sem autorização.

A segurança da informação, de acordo com Batista (2004) passou a ser um assunto estratégico dentro da empresa, pois ele pode interferir no seu processo de fazer negócios e no valor de seu produto ou serviços. Dentre as principais ameaças para os sistemas de informação destacam-se:

- Incêndio: Os computadores, arquivos e registros manuais podem ser destruídos.
- Falha elétrica: Todo o processamento é suspenso, o equipamento pode ser danificado e podem ocorrer acidentes de dados ou interrupções dos serviços de telecomunicações.
- Mau funcionamento do hardware: Os dados são processados sem precisão ou de modo incompleto.

- Erros de Software: Os programas dos computadores processam os dados sem precisão, de modo incompleto ou sem atender às necessidades do usuário.
- Erros dos usuários: Erros gerados pelos usuários durante transmissão, entrada, validação, processamento da informação, destruição acidental ou não podem prejudicar o processamento ou gerar informações que não representam a realidade ou não são confiáveis.
- Crime por computador: O uso ilegal de hardware, softwares ou dados resulta no roubo de dinheiro ou na destruição de dados ou serviços valiosos.
- Mau uso do computador: Os sistemas de computador são usados com propósitos antiéticos.

Dentre as ameaças citadas, Batista (2004) destaca que uma das que mais se prolifera é a invasão, e segundo ele, os invasores que definem a necessidade de segurança nos sistemas de informações podem ser internos ou externos, e são classificados como:

- Hackers (internos e externos): podem ser profissionais com o objetivo de espionagem empresarial, furtando informações ou ativos, ou podem ser amadores tentando a invasão como forma de diversão ou hobby;
- Funcionários descontentes: desejam se vingar da organização causando algum tipo de dano nos dados ou informações de responsabilidade;
- Usuários mal treinados: danificam dados em operações equivocadas;
- Vírus de computador: entram no sistema por intermédio de disquetes, cd's, mídias removíveis ou mensagens eletrônicas e causam algum tipo de prejuízo digital que resulta em prejuízo real;

Batista (2004) afirma que de todos, os hackers são os mais perigosos, pois possuem conhecimentos suficiente nas áreas de programação, hardware e telecomunicações para causar sérios prejuízos a organização.

5.6 Segurança Física em TI

Conforme Barbosa (2001), a segurança em tecnologia da informação pode ser compreendida por três pilares principais: segurança lógica, segurança física e segurança técnica.

A segurança física desempenha, segundo Barbosa (2001), um papel tão importante quanto à segurança lógica e técnica. Isto porque é a base para a proteção de qualquer

investimento feito por uma empresa. Investir entre os diferentes aspectos de segurança sem observar suas devidas prioridades, pode ocasionar uma perda de todos os recursos investidos em virtude de uma falha nos sistemas mais vulneráveis.

Na concepção de Fontes (1991), a segurança física tem como principais objetivos garantir a continuidade das rotinas, assegurar a integridade dos ativos e manter a integridade e confidencialidade das informações.

Para investir em segurança física, Fontes (1991) descreve que deve-se primeiramente realizar uma análise dos riscos e vulnerabilidades físicas que a empresa possa estar exposta. Esta análise deve ser feita preferencialmente por especialistas no assunto e, se possível, externos à organização, para que não haja conflito ou compromisso com relação a projetos passados realizados com ou sem sucesso.

Existem, ainda segundo Fontes (2001), diversas ferramentas para auxiliar a análise dos impactos nos negócios, em virtude de eventos ou sinistros aos quais a empresa possa estar exposta.

Para Barbosa (2001), a análise de riscos deverá retratar a real situação da empresa quanto aos aspectos de segurança física. Os resultados devem ser encarados como uma ferramenta para auxiliar a empresa a melhorar ou manter seu nível de segurança física e não como uma crítica ao que foi ou deixou de ser feito no passado quanto ao assunto.

Barbosa (2001), afirma que devido a constantes mudanças Tecnológicas, a segurança física, precisa ser flexível e capaz de absorver as diferentes tecnologias que surgem ao longo do tempo. Empresas precisam estar constantemente revisando e reorganizando seus componentes e processos de segurança física.

Além da análise de riscos físicos, Barbosa (2001) relata que deve ser realizado o levantamento de necessidades de componentes e processos de segurança física. Nesta etapa deve ser envolvido um comitê responsável pela continuidade dos negócios da empresa e/ou uma empresa contratada para a elaboração do plano, em razão de envolver assuntos correlacionados de segurança lógica e técnica. Nesta fase, decide-se sobre todos os recursos a serem disponibilizados como equipamentos de monitoração, energia, climatização, ambientes de segurança para os equipamentos críticos, política de segurança de acesso físico às informações e ambientes distintos da organização, dentre os diversos componentes e processos que devem ser envolvidos num projeto de segurança física.

De acordo com Barbosa (2001), para concretizar a segurança física, deve-se também implantar um plano de segurança física, que faz parte de um projeto maior de continuidade de negócios. Após realizar os investimentos e implementar o plano, a empresa deverá estar

constantemente revendo o plano e modificando o que for necessário, o que demonstra ser um processo contínuo e inacabável.

5.7 Segurança Lógica

A segurança lógica é definida por Fontes (1991), como sendo um conjunto de métodos e procedimentos automatizados e manuais destinados a proteger os recursos computacionais contra a sua utilização indevida ou desautorizada, intencional ou não. Compreende o controle de consultas, alterações, inserções e exclusões de dados e o controle do uso de programas e outros recursos.

Para Fontes (1991), sua função primordial é proteger os dados importantes dos arquivos ou componentes dos programas. Essa proteção deve incluir controles ao acesso lógico, estabelecendo a obrigatoriedade da identificação do usuário, senhas e confirmações. Estabelece também, níveis de autorização, restringindo o alcance de cada usuários para ler, gravar, alterar ou atualizar arquivos.

De acordo com Fontes (1991), a grande utilização do processamento eletrônico de dados resulta no aumento de sua vulnerabilidade em ritmo cada vez maior, exigindo meios de segurança mais eficientes para proteção dos dados manuseados. A criação, por exemplo, de redes abertas mostra a necessidade desses controles, chamados de segurança lógica.

Fontes (1991) afirma que o estabelecimento de controles para segurança lógica dos dados deve ser avaliado pelo aspecto custo/benefício, pois que reduz os riscos às informações, aumentando a confiabilidade dos dados, mas também aumenta a sobrecarga dos computadores, alongando os tempos de respostas e fazendo crescer os custos.

Ainda segundo Fontes (1991), as empresas da área financeiras são as que mais investem em providências para proteger suas informações. Essa segurança é gerada com o apoio da alta administração da empresa, através da edição de normas e o estabelecimento de rotinas.

5.8 Segurança da Informação X Agregação de Valores a Empresa

De acordo com Carissimi (2001), a racionalização dos investimentos numa empresa é fundamental. É preciso focar a utilização dos recursos naquilo que mais agrega valor ao negócio. É preciso priorizar. Como se sabe, as empresas estão constantemente expostas à ameaças. Diversos tipos de incidentes podem ocorrer a qualquer momento.

Independentemente de qual seja o tipo, podemos agrupá-los de acordo com a propriedade da informação que eles atingem: confidencialidade (sigilo da informação), integridade (informações íntegras - corretas), disponibilidade (informação disponível quando você precisar dela - por exemplo, o site deve estar no ar).

Problemas de quebra de confidencialidade (causados, por exemplo, por vazamento ou roubo de informações sigilosas), conforme entendimento de Carissimi (2001), podem expor para o mercado ou para a concorrência as estratégias ou tecnologias da empresa. Talvez se tenha estratégias ou tecnologias como diferencial competitivo. Nesse caso, se deixarem de ser segredo de negócio, vão comprometer a vantagem competitiva da empresa perante mercado. O market share será ameaçado. Há o grande risco de a concorrência passar para o campo dos preços.

Em última análise, Carissimi (2001) afirma que a margem de lucro será comprometida, e os acionistas perderão dinheiro. Problemas de disponibilidade (exemplo: um ataque ao site, em que ele fique fora do ar por algum tempo), pode causar impacto direto no faturamento, caso se faça algum tipo de venda on-line. Isso é muito claro.

Mas segundo Carissimi (2001) isso não é tudo, podem ocorrer inúmeros outros problemas dependendo da função do site para empresa, o que novamente ocasionará perda de lucratividade para esta. Problemas de integridade causados, por exemplo, por uma invasão ou problema técnico que altere o valor de dados importantes, sem que se perceba, trazem impactos. Os dados armazenados, em algum momento, são usados para tomadas de decisões. Um dado errado leva a decisões erradas.

Para Carissimi (2001), decisões erradas fatalmente reduzirão o faturamento ou aumentarão custos. Um ataque ao site, com modificação de conteúdo, tornará visível ao mercado que a empresa negligenciou aspectos de Segurança da Informação e isso fará com que os investidores pensem duas vezes antes de investir na empresa, afinal de contas, de uma forma ou de outra a referida empresa acabou por não cuidando de forma devida dos seus Sistemas de Informação.

Carissimi (2001) conclui que elementos fundamentais para a sobrevivência das empresas - como a busca contínua do aumento do faturamento e da redução de custos e a avaliação que o mercado faz dos papéis - estão relacionados com Segurança da Informação.

De acordo com Carissimi (2001), o valor dos papéis da companhia no mercado está associado com a confiança que investidores e agências de classificação de risco depositam nela. Sendo assim, a segurança da informação, permeada por toda a organização, contribui grandemente para sua lucratividade e avaliação da empresa. Em outras palavras, e

respondendo a pergunta feita logo no início: sim, Segurança da Informação agrega valor ao negócio e garante o retorno sobre o investimento (ROI) que os acionistas tanto almejam.

5.9 Vulnerabilidade e Abuso em Sistemas

Para Laudon e Laudon (2001, p338), antes da automação dos computadores, as informações eram mantidas em papéis seguros pelas organizações. Os sistemas de informação trouxeram, dentre outras, a facilidade de acesso aos dados e informações mesmo de fora das organizações, e com ela veio também os riscos de destruição de dados, fraude, erro e uso indevido.

De acordo com Laudon e Laudon (2001, p338), quando os sistemas de computadores não conseguem rodar ou trabalhar como necessário, as empresas que dependem fortemente de computadores passam por uma séria perda da função empresarial, tendo prejuízos na ordem de US\$ 6 milhões por hora em firmas de corretagem. Em empresas que dependem de computadores, os prejuízos aumentam ao passo que seus sistemas ficam fora do ar, e naquelas que têm servidores rodando todo o sistema operacional da empresa, há uma perda total da função empresarial.

Laudon e Laudon (2001, p338) afirma que quando grandes quantidades de dados são armazenadas na forma eletrônica, eles ficam vulneráveis a muito mais tipos de ameaças do que quando existem na forma manual.

Os sistemas computadorizados, segundo Laudon e Laudon (2001, p338), são especialmente vulneráveis a tais ameaças pelas seguintes razões:

- Um sistema de informação complexo não pode ser copiado manualmente.
- Procedimentos computadorizados aparentam ser invisíveis e não são facilmente entendidos ou auditados.
- Embora as chances de desastre nos sistemas automatizados não sejam maiores do que nos sistemas manuais, o efeito de um desastre pode ser muito mais extenso. Em alguns casos, todos os registros de um sistema podem ser destruídos e perdidos para sempre.
- Os sistemas de informação on-line são diretamente acessíveis por muitos indivíduos. Usuários legitimados podem conseguir acesso fácil aos dados de computador que eles não estão autorizados a ver. Indivíduos não autorizados também podem ganhar acesso a tais sistemas.

Para Laudon e Laudon (2001, p338), os avanços nas telecomunicações e softwares ampliaram essas vulnerabilidades, uma vez que através das redes de telecomunicações os sistemas de informação se interconectam com localidades diferentes, e além disso, os arranjos mais complexos e diverso hardware, software, organizacionais e pessoais são necessário para as redes de telecomunicações, criando novas áreas e oportunidades para penetração e manipulação.

De acordo com Laudon e Laudon (2001, p338), as redes sem fios são as mais vulneráveis, pois utilizam frequências de rádio, que é mais fácil de ser interceptada. Já a internet, estabelece problemas especiais porque foi projetada explicitamente para ser acessada com facilidade por pessoas em diferentes sistemas de computadores.

5.10 Atributos da Informação

Segundo Loureiro (1999), a segurança da informação consiste de várias variáveis e pode ser caracterizada pela preservação de três fatores:

- **Confidencialidade:** Garantia de que a informação é acessível somente por pessoas autorizadas a terem acesso;
- **Integridade:** Exatidão, completeza da informação e dos métodos de processamento;
- **Disponibilidade:** Garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

Para Puttini (2000), além das três variáveis de caracterização de segurança da informação citada por Loureiro, existe ainda mais uma, chamada autenticidade. Esta é descrita por ele como:

- **Autenticidade:** Está associado com identificação correta de um usuário ou computador. O serviço de autenticação em um sistema deve assegurar ao receptor que a mensagem é realmente procedente da origem informada em seu conteúdo.

5.11 Auditoria da Segurança da Informação

Para Loureiro (1999), a auditoria da Segurança da Informação consiste na validação e avaliação do controle interno de sistemas de informação. Abaixo segue um organograma da auditoria nas organizações:

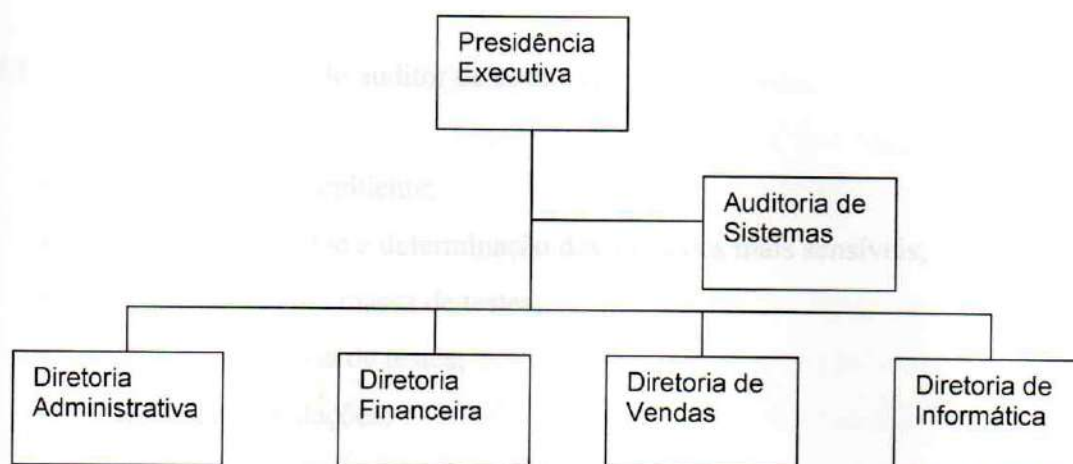


Figura 1 – Ambiente empresarial e situação da área de Informática e da área de Auditoria de Sistemas
Fonte: LOUREIRO (1999)

Ainda segundo Loureiro (1999), a auditoria da Segurança da Informação depende da análise de vários fatores abrangentes.

5.11.1 Dificuldades encontradas pela Auditoria de Sistemas na Empresa

- Defasagem tecnológica;
- Falta de bons profissionais;
- Falta de cultura da empresa;
- Tecnologia variada e abrangente;

5.11.2 Papel do auditor de sistemas

- Validação do fluxo administrativo (planejamento, execução e controle);
- Ênfase nos processos computacionais;
- Comprovação da efetividade dos sistemas computadorizados;
- Garantia da segurança lógica e física e da confidencialidade dos sistemas;

5.11.3 Importância da auditoria de sistemas

- Altos investimentos das organizações em sistemas computadorizados;
- Necessidade de garantir a segurança dos computadores e seus sistemas;
- Garantia do alcance da qualidade dos sistemas computadorizados;
- Auxiliar a organização a avaliar e validar o ciclo administrativo;

5.11.4 Etapas da atuação do auditor de sistemas

- Compreensão do ambiente;
- Análise do ambiente e determinação das situações mais sensíveis;
- Elaboração de uma massa de testes;
- Aplicação da massa de testes;
- Análise das simulações;
- Emissão da opinião quanto ao ambiente auditado;
- Debate com os profissionais da área auditada para discussão das alternativas recomendadas;
- Acompanhamento da implantação da solução proposta;
- Auditoria da solução implantada;
- Novas auditorias no ambiente;

5.11.5 Perfil do Auditor de Sistemas

- Ser independente às áreas a serem auditadas;
- Ter formação em auditoria de computação, conhecendo o ambiente a ser auditado;

5.11.6 Necessidades na área de auditoria de sistemas

- Fortalecimento das técnicas de auditoria de sistemas para atuação em ambientes computacionais complexos;
- Criação de metodologias de auditoria de sistemas;
- Estudo do custo / benefício;
- Ampliação do campo de atuação da auditoria de sistemas;
- Treinamento do auditor de sistemas;

5.11.7 Conceituação de Auditoria de Sistemas

- Controle Interno;
- Momentos de atuação do Auditor de Sistemas;
- Produtos finais da Auditoria de Sistemas;

- Mecânica de implantação das recomendações da auditoria;
- Postura do auditado durante a atuação da Auditoria de Sistemas.

5.11.8 Tendências da Auditoria de Sistemas na Organização

- Criação de um profissional responsável pela segurança da informação;
- Preocupação com a qualidade dos processos computadorizados – criação do Analista de Segurança da Informação e do Analista de Qualidade da Informação.

5.12 ISO 17799

5.12.1 O surgimento da Norma Nacional de Segurança de Informação

De acordo com Rocha (2002), em 1987 o departamento de comércio e indústria do Reino Unido (DTI) criou um centro de segurança de informações, o CCSC (Commercial Computer Security Center - Centro Computacional de Segurança Comercial) que dentre suas atribuições tinha a tarefa de criar uma norma de segurança das informações para o Reino Unido.

Desde 1989 vários documentos preliminares foram publicados por esse centro, até que, em 1995, surgiu a BS 7799 (British Standard 7799). Esse documento foi disponibilizado em duas partes para consulta pública, a primeira em 1995 e a segunda em 1998. Em 1º de dezembro de 2000, após incorporar diversas sugestões e alterações, a BS7799 ganhou status internacional com sua publicação na forma da ISO/IEC 17799:2000. Por fim, em setembro de 2001, a ABNT homologou a versão brasileira da norma, denominada NBR ISO/IEC 17799.

A ISO 17799 cobre os mais diversos tópicos da área de segurança, possuindo um grande número de controles e requerimentos que devem ser atendidos para garantir a segurança das informações de uma empresa, de forma que a obtenção da certificação pode ser um processo demorado e muito trabalhoso.

Em contrapartida, a certificação é uma forma bastante clara de mostrar à sociedade que a empresa dá à segurança de suas informações e de seus clientes a importância que merecem, de tal forma que se prevê que em poucos anos todas as grandes empresas terão aderido a norma e obtido suas certificações.

5.12.3 Objetivos da Norma

De acordo com a Sisnema (2006), a NBR ISO/IEC17799:2001 tem como objetivo fornecer recomendações sobre gestão de segurança da informação para os responsáveis pela introdução, implementação ou manutenção de segurança em suas empresas. Também permite a continuidade dos negócios de uma organização, por meio de implantação de controles que reduzem a perda de informações essenciais.

O uso desta norma de segurança apresenta características como definir quem terá acesso aos dados do sistema, qual será o nível deste acesso e gerenciamento restrito de usuários através de senhas de entrada ao sistema.

5.12.4 Divisão da Norma Nacional de Segurança de Informação

A norma nacional de segurança de informação é dividida nos 10 macros controles:

- Política de Segurança;
- Segurança Organizacional;
- Classificação e Controle dos Ativos da Informação;
- Segurança em Pessoas;
- Segurança Física e do Ambiente;
- Gerenciamento de Operações e Comunicações;
- Controle de Acesso;
- Desenvolvimento da Segurança de Sistemas;
- Gestão da Continuidade do Negócio;
- Conformidade.

Cada um destes controles é subdividido em vários outros controles, a NBR possui um total de 137 controles de segurança, todos voltados para manutenção dos três fatores primordiais: a Confidencialidade, a Integridade e a Disponibilidade das Informações Críticas.

A Confiabilidade é definida pela NBR como sendo: a garantia de que a informação só pode ser acessada e manipulada por pessoas autorizadas, ou seja, ela é restrita a um conjunto de entidades, que podem ser seres humanos ou podem ser um sistema eletrônico.

A Integridade, segundo a NBR, implica que toda vez que uma informação é manipulada ela está consistente, ou seja, que não foi alterada ou adulterada por um acesso legal ou ilegal e a Disponibilidade é a garantia de que uma informação sempre poderá ser

acessada, pelas pessoas e processos autorizados, independentemente do momento em que ela é requisitada e do local no qual está armazenada.

Afirmar que um ambiente é aderente à Norma de Segurança da Informação significa dizer que o mesmo utiliza os recursos adequados para garantir a Disponibilidade, Confidencialidade e a Integridade de suas informações. Mas para isto devem ser aplicados ao ambiente alguns ou todos os controles existentes na norma de segurança. Contudo, a lista dos controles que devem ser aplicados depende de características do próprio ambiente, como por exemplo: forma e local de armazenamento das informações, valor das informações armazenadas, quem pode acessá-las, quais servidores estão instalados, que tipo de serviços são disponibilizados aos usuários da rede interna e da rede externa e etc.

Para entendermos melhor os termos técnicos da norma, descrevemos abaixo alguns desses termos segundo a própria norma ISO 17799.

A Análise de Risco de um ambiente baseia-se na avaliação do impacto de uma falha de segurança nas atividades da organização, bem como na sua probabilidade de ocorrência. O resultado desta análise apontará os principais pontos a serem trabalhados e a prioridade das informações a serem protegidas. Sendo o resultado da Análise de Risco dependente das características atuais do ambiente e como o mesmo não é estático, este resultado representa as melhores ações a serem aplicadas em um determinado momento no ambiente. Conseqüentemente, análises de risco periódicas devem ser realizadas, mesmo quando um ambiente não tenha se modificado. Neste caso, a nova análise é justificada pelo fato de que novas vulnerabilidade e ameaças surgem diariamente. Contudo, independente do ambiente, dos riscos e das ameaças que foram indicadas pelo resultado da Análise de Risco, existe um conjunto mínimo de controles, que segundo a NBR, sempre devem ser implementados. Este conjunto segundo a NBR engloba:

Política de segurança da informação: este é um documento que descreve quais atividades os usuários estão autorizados a realizar, como e quando podem ser realizadas. É de vital importância que a alta administração apóie o uso da Política e demonstre o seu comprometimento com a aplicação de suas penalidades cabíveis.

Definição das responsabilidades de segurança: este controle visa esclarecer a quem "pertence" cada ativo da organização, bem como quem deve ser contactado em caso de problemas de segurança relacionados a ativos em questão.

Processo de treinamento: a melhor forma de evitar mal uso das informações é educar seus usuários, assim é de vital importância que todo e qualquer usuário passe por um treinamento antes de ter acesso as informações contidas no ambiente.

Relatórios dos incidentes: estes documentos permitem a criação de uma "base de conhecimento" que poderá ser utilizado para identificar e evitar futuros incidentes de segurança.

Gestão da continuidade das atividades do ambiente: este controle diz respeito ao processo de se manter a informações, integras sempre acessíveis mesmo em caso de parte do ambiente esteja comprometido.

Como vemos a Norma de Segurança é bastante extensa e complexa, gerando um grande esforço e trabalho para ser implantada. Contudo, ver-se também, que se implantada devidamente, o ambiente ficará muito menos vulnerável e bem mais seguro.

6. METODOLOGIA

6.1 Tipo de Pesquisa

Para entender melhor como a empresa trata atualmente o aspecto segurança em TI, e assim poder avaliar e desenvolver um planejamento para implantação de segurança em sistemas de TI, foi desenvolvido uma pesquisa descritivo-exploratória, com questões relativas à Segurança da Informação. A idéia central desta pesquisa consiste em identificar como o ambiente estudado trata suas informações e qual o nível de conscientização de seus colaboradores quanto a confidencialidade, integridade e disponibilidade da informação. Foi exposto um resultado quantitativo para melhor demonstrar o resultado dessa pesquisa e para melhor entendimento do leitor, foi desenvolvida também uma pesquisa bibliográfica sobre segurança da informação e assuntos que circundam esta.

6.2 População e Amostra

Para alcançar um resultado de pesquisa satisfatório no que diz respeito a evidenciar o real cenário em que se encontra a empresa no que se refere a segurança em TI, a pesquisa buscou atingir ao maior número de colaboradores possível. O Rifóles Praia Hotel & Resort tem 190 colaboradores, dos quais aproximadamente 80 têm acessos aos sistemas de TI. Desses, 50 responderam ao questionário proposto por esta pesquisa. Esse número equivale a um total de 63% dos colaboradores que utilizam algum sistema de informação. Estes colaboradores trabalham nas mais variadas área da empresa.

6.3 Plano de Coleta de Dados

Buscando realizar uma pesquisa aplicada que demonstrasse o mais próximo da realidade possível a situação da empresa em relação a segurança em TI, foi elaborado 01 (um) instrumento de pesquisa (vide anexo I), direcionado a todos os colaboradores do escopo com acesso a algum SI, abrangendo todos os cargos, buscando avaliar como estes profissionais vêem e tratam o quesito segurança da informação.

No questionário foram abordadas questões direcionadas a senhas, tipos de informações que circulam pela empresa, conhecimento de informações sigilosas, divulgação

de informação, dentre outras questões relevantes para identificação dos pontos mais críticos que refletem o nível de conscientização dos usuários, quanto à Segurança da Informação.

Esta pesquisa tem o intuito de levantar se os usuários têm consciência do valor da informação, se eles sabem quais podem ser disseminadas e quais não podem ser discutidas fora do ambiente "seguro", que é o seu grupo de trabalho, se existe uma cultura de divulgação de ações de segurança como política de utilização de senhas, de e-mails, termos de confidencialidade e responsabilidade, dentre outros.

6.4 Análise dos Dados

Os dados coletados na pesquisa foram trabalhados através do software Excel e analisados quantitativamente e/ou percentualmente, a partir de ferramentas estatísticas. Sendo os dados reunidos em conjuntos para análises e conclusão do relatório final.

7. RESULTADOS

Nesse capítulo serão expostos os resultados obtidos na pesquisa através do questionário aplicado aos colaboradores do Rifóles Praia Hotel & Resort.

TABELA 1 – Faixa etária dos funcionários.

Faixa Etária	Frequência	Percentual
Até 20 anos	41	21%
De 21 a 30 anos	49	25%
De 31 a 40 anos	69	36%
Acima de 40	31	18%

Relação entre faixa etária e usuário de sistemas de informação no Rifóles.

A tabela 1, demonstra a relação entre idade e profissionais que utilizam sistemas de informação na referida empresa. Percebemos que a maioria dos colaboradores que utilizam sistemas de informação na empresa têm entre 31 e 40 anos de idade.

TABELA 2 – Sexo dos funcionários.

Sexo	Frequência	Percentual
Masculino	102	54%
Feminino	88	46%

Relação entre sexo dos usuário de sistemas de informação no Rifóles.

Na tabela 2, percebemos que no Rifóles a diferença de utilização dos sistemas de informação computadorizados entre mulheres e homens é relativamente pequena.

TABELA 3 – Funções Operacionais X Gerencial.

Função	Frequência	Percentual
Gerencial	14	28%
Operacional	36	72%

Proporcionalidade entre gerentes de funcionários na utilização dos sistemas de informação.

Como é de se esperar em qualquer empresa, a quantidade de funcionários operacionais é bem maior que a de nível gerencial. Isso pode ser visto na tabela 3, descrita acima.

TABELA 4 – Tempo de serviço.

Tempo de Serviço	Frequência	Percentual
Menos de 1 ano	19	10%
De 1 a 5 anos	158	83%
Acima de 5 anos	13	7%

Tempo de serviço dos usuários do Rifóles Praia Hotel & Resort.

A tabela 4 mostra que a maioria dos funcionários do Rifóles trabalham nesta empresa entre 1 e 5 anos. O número dos que trabalham a mais de 5 quase que se equipara com os que trabalham a menos de 1 anos.

TABELA 5 – Outras ocupações.

Possui outro emprego	Frequência	Percentual
Sim, na mesma área	0	0%
Sim, em outra área	1	2%
Não	49	98%

Usuários com outras ocupações em outras empresas

Uma questão que em determinadas situações pode ser muito perigoso para a empresa, é o fato de funcionários que trabalham em outras empresas e são muitas vezes um perigo em potencial quando se trata do ponto de vista de segurança da informação, pois muitas vezes disponibilizam informações (as vezes até sigilosas) para as outras empresas que trabalham, que muitas vezes é na mesma área. No caso do Rifóles, vemos que apenas 2% dos colaboradores que responderam a este questionário trabalham em outra empresa. O fato de essa outra ocupação não ser na mesma área que o hotel, faz com que diminua as possibilidade de um prejuízo para o Rifóles.

TABELA 6 – Compartilhamento de senhas.

Confidencialidade de senha	Frequência	Percentual
Compartilha sua senha	22	44%
Não Compartilha sua senha	28	56%

Relação de usuários que compartilham suas senhas com outros usuários.

A tabela 6 apresenta a preocupação, ou não, dos usuários em compartilharem sua senha pessoal com outros usuários. Vemos aqui um dado preocupante para o Rifóles Praia

Hotel, pois 44% de seus usuários compartilham suas senhas, o que pode vir a causar sérios problemas a empresa e repercutir diretamente nos usuários.

TABELA 7 – Senhas de terceiros.

Utilização de senhas de terceiros	Frequência	Percentual
Utiliza senha de terceiro	22	44%
Não utiliza senha de terceiro	28	56%

Relação de usuários que utilizam senhas de terceiros.

Uma relação interessante é a demonstrada na tabela 7, tendo em vista o exposto na tabela 6, pois verificamos que a quantidade de usuários que utilizam a senha do companheiro de trabalho é maior do que a quantidade que compartilha, evidenciando que um grupo de usuários apesar de usar a senha do colega, não divulga a sua própria.

TABELA 8 – Exposição de senhas.

Expõe senha	Frequência	Percentual
Sim	43	86%
Não	7	14%

Percentual de usuários que expõe suas senhas em agenda, computador ou local similar.

Um fato bastante preocupante encontrado no Rifóles, se dá pela exposição de senhas anotadas em agendas, papéis soltos na mesa, nas próprias mesa de trabalho ou locais similares. A tabela 8 mostra um número assustador de 86% dos usuários praticando tal fato.

TABELA 9 – Senhas cedidas.

Acesso rápido	Frequência	Percentual
Sim	43	86%
Não	7	14%

Proporção de usuários que cedem suas senhas para acessos rápidos pelos colegas.

No que se refere à senhas, os usuários do Rifóles estão se expondo bastante. É o que também mostra a tabela 9, demonstrando que 86% dos usuários cedem sua senha a terceiros para que estes façam um acesso rápido aos sistemas.

TABELA 10 – Alteração de senhas.

Alteração de senha	Frequência	Percentual
Mensalmente	3	6%
Trimestralmente	2	4%
Semestralmente	6	12%
Somente quando o sistema solicita alteração	39	78%

Prática de alteração de senha por parte dos usuários.

Como podemos comprovar através da tabela 10, a senha pessoal é o fator mais preocupante dentro do Rifóles no que se refere a segurança, pois em várias perguntas a grande maioria dos usuários demonstram claramente não se preocuparem muito com o aspecto segurança.

TABELA 11 – Fornecimento de informações.

Fornecimento de Informação	Frequência	Percentual
Forneço a informação, pois não há nada confidencial em minha área	25	50%
Forneço a informação após identificar o solicitante	23	46%
Solicito autorização a meu superior para liberar a informação	2	4%

Demonstrativo sobre como o usuários procede para fornecer informações que têm acesso.

Na tabela 11, vemos que apenas à pequena minoria se preocupa em checar com o superior se realmente pode passar a informação para um terceiro.

TABELA 12 – Informações confidenciais.

Informações Confidenciais	Frequência	Percentual
Reconheço as informações vitais	23	46%
Não reconheço as informações vitais	27	54%

Proporção de usuários que realmente sabem quais informações são vitais ao negócio.

A tabela 12 mostra que em média, a metade dos usuários sabem quais informações são vitais para o negócios e a outra metade não. Quando relacionamos esse resultado com o exposto na tabela 10 percebemos que o fato de 46% reconhecerem as informações vitais à empresa não evita que estes repassem estas a terceiros.

TABELA 13 – Bloqueio de estação.

Bloqueio de Estação	Frequência	Percentual
Bloqueio ao sair	8	16%
Não bloqueio ao sair	42	84%

Usuários que bloqueiam suas estações ao se ausentar da frente do computador.

Outro fato que não estamos acostumado a verificar do dia a dia, são os usuários preocupados no que pode ser feito em sua estação de trabalho durante sua ausência. Esse fato é evidenciado no Rifóles através da tabela 13, onde 84% dos usuários não bloqueiam suas estações de trabalho ao se ausentarem.

TABELA 14 – Reconhecimento de informação.

Informação Confidencial	Frequência	Percentual
Meu setor possui	21	42%
Meu setor não possui	29	58%

usuários que reconhecem que seu setor têm informação confidencial

É de fácil percepção que os colaboradores do Rifóles não tratam a confidencialidade da informação através do exposto na tabela 14, pois sabemos que todos os setores de uma empresa de uma forma ou de outra possui algum tipo de informação confidencial.

TABELA 15 – Importância da informação.

Importância da Informação	Frequência	Percentual
Conhece a importância	20	40%
Não Conhece	30	60%

Relação dos usuários que sabem a importância da informação para a empresa

Esse dado é muito importante para segurança da informação, pois não se protege aquilo que não se julga ser importante. No Rifóles, vemos pela tabela 15 que 60% dos usuários não conhecem a importância da informação para a empresa.

TABELA 16 – Credibilidade na segurança em TI.

Credibilidade na segurança em TI	Frequência	Percentual
Acesso fácil	12	24%
Acesso não fácil	38	76%

Relação dos usuários que acreditam na segurança da informação do Rifóles.

A tabela 16 demonstra que 76% dos usuários, acreditam que o acesso a informações importantes à empresa por uma pessoa externa não é fácil.

TABELA 17 – Acesso à informações

Acesso à informações	Frequência	Percentual
Informações operacionais	50	100%
Informações gerenciais	20	40%
Informações confidenciais	15	30%
Informações imprescindíveis à continuidade do negócio	13	26%
Não tenho acesso a nenhuma informação importante	0	0%

Tabela 16: Tipo de informação que os usuários têm acesso.

Na tabela 17, é exposto a qual tipo de informação os usuários têm acesso dentro da empresa.

8. CONCLUSÃO

Ao término desse estudo de caso, chegou-se a conclusão que o Rifóles Praia Hotel & Resort se encontra em uma situação passiva a ocorrer problemas gerados por falta de segurança em seus sistemas de TI. Foi observado que existem diversas vulnerabilidades nos mais diversos setores da empresa. Abaixo segue as principais.

- Procedimentos impróprios para garantia da segurança da informação por parte dos usuários, faltando a estes normas a seguirem.
- Falta de diretrizes sobre como os funcionários devem lidar diante de algum incidente de segurança.
- Inexistência de uma rotina de auditoria nos sistemas utilizados pelos usuários.

Conforme objetivo proposto por essa monografia, é apresentado no APÊNDICE B, sugestão em segurança de TI ao Rifóles Praia Hotel & Resort. Baseado na análise dos resultados da pesquisa aplicada aos usuários, análise da rede local e resultados do check-list de segurança foi elaborado uma Política de Segurança contextualizando e criando solução para todos os pontos vulneráveis encontradas nesse estudo de caso. A aplicação dessa Política de Segurança, gera uma solução imediata aos problemas ora encontrados e dessa maneira garante que o ambiente de TI se torne seguro.

REFERÊNCIAS

ALBERTO, Bastos. **Computer World** - 01 Mar 1998.

ÂNGELO, Fernanda K. **O básico é básico**. ComputerWorld, 08/06/2005. Disponível em <http://old.computerworld.com.br/AdPortalv5/adCmsDocumentShow.aspx?GUID=11659A93-17C9-438A-89D0-B19D090D09EB&ChannelID=38>. Acesso em 03 maio 2006.

BARBOSA, Mauricio Alves. **Segurança Física em TI** – Confira as melhores práticas antes de investir. Módulo Security Magazine, 10/01/2001. Disponível em http://www.modulo.com.br/pt/page_i.jsp?page=3&catid=2&objid=90&pagenumber=0&idiom=0. Acesso em 10 maio 2006.

BATISTA, Emerson de Oliveira. **Sistemas de Informação – O Uso Consciente da Tecnologia para o Gerenciamento**. São Paulo: Editora Saraiva – 2004.

CARISSIMI, Leonardo. **Segurança da Informação Agrega Valor?** Descubra porque a resposta é sim. Módulo Security Magazine, 23/08/2001. Disponível em <<http://www.modulo.com.br/index.jsp>>. Acesso em 05 maio 2006.

COSTA, Carlos Alberto. **Como proteger as informações nas empresas**. Info Guerra, 13/7/2004. Disponível em <http://www.infoguerra.com.br/infonews/viewnews.cgi?newsid1089705099,58559>. Acessado em 22 de julho de 2006.

FERREIRA, Aurélio Buarque de Holanda. **Aurélio - O Dicionário da Língua Portuguesa** – São Paulo: Editora Positivo – 2004

FONTES, Joaquim Rubens. **Manual de Auditoria de Sistemas** – Rio de Janeiro: Editora Ciência Moderna Ltda. – 1991

GONÇALVES, Luís Rodrigo de Oliveira. **O surgimento da Norma Nacional de Segurança de Informação [NBR ISO/IEC-1779:2001]**. Lokabit, 19/03/2004. Disponível em <http://www.lockabit.coppe.ufrj.br/rlab/rlab_textos.php?id=85> Acesso em 24 maio 2006.

LAUDON, Kenneth C.; LAUDON, Jane Price. **Gerenciamento de Sistemas de Informação** – Rio de Janeiro: Editora Livros Técnicos e Científicos S.A. - 2001

LOUREIRO, Gil Antônio de. **Auditoria em Computadores**. Maio de 2000.

MACHADO, Cesar de Souza. **51 questões mais frequentemente formuladas sobre a BS7799 e ISO17799**. Cdigital, 03/03/2004. Disponível em <http://www.cdigital.com.br/iso/faq.htm>. Acesso em 24 maio 2006.

PINHEIRO, José Mauricio Santos. **Por que estudar sistemas de informação?** Projeto de Redes, 28/09/2004. Disponível em http://www.projetoederedes.com.br/artigos/artigo_porque_estudar_sistemas_de_informacao.php. Acessado em 19 de agosto de 2006.

PINHEIRO, José Mauricio Santos. **A Importância da Tecnologia da Informação e das Telecomunicações nos Sistemas de Informação**. Projeto de Redes, 28/09/2004. Disponível em http://www.projetoderedes.com.br/artigos/artigo_importancia_da_tecnologia.php Acessado em 19 de agosto de 2006.

PUTTINI, Ricardo S. **Segurança e Criptografia**. Segurança de Redes – UNB. Disponível em <http://webserver.redes.unb.br/security/introducao/introducao.htm> Acessado em 07 de novembro de 2006.

ROCHA, Cláudio. **Como tudo começou**. Segurança Security, 12/11/2002. Disponível através de <http://www.informabr.com.br/nbr.htm> Acessado em 26 de agosto de 2006.

SILVA, Diller Grisson. **Manual de Informática**. São Paulo: Editora D' Livros. - 1997.

SISNEMA. **Conheça a norma de segurança NBR ISO/IEC17799**. Sisnema Informática, 10/02/2006. Disponível em <http://sisnema.com.br/Materias/idmat016399.htm> Acessado em 26 de agosto de 2006.

UEMURA, Cláudio Norikazu. **A importância da Segurança da Informação**. Módulo Security, 28/03/2005. Disponível através de <http://www.modulo.com.br/index.jsp>. Acesso em 26 maio 2006.

APÊNDICE A – QUESTIONÁRIO APLICADO AOS USUÁRIOS
PESQUISA SOBRE A SEGURANÇA DA INFORMAÇÃO

NATAL, ____ / ____ DE 2006

SOBRE O FUNCIONÁRIO

1.Faixa etária

- a) ☐ Até 20 anos
- b) ☐ De 21 a 30 anos
- c) ☐ De 31 a 40 anos
- d) ☐ Acima de 40

2.Sexo

- a) ☐ Masculino
- b) ☐ Feminino

3.Função

- a) ☐ Gerencial (Chefe de divisão, Chefe de Gabinete, Diretoria, etc...)
- b) ☐ Operacional (Agente administrativo, Oficial administrativo, Auxiliar de Gabinete, etc...)

4.Trabalha na EMPRESA a

- a) ☐ Menos de 1 ano
- b) ☐ De 1 a 5 anos
- c) ☐ Acima de 5 anos

5.Possui outro emprego?

- a) ☐ Sim, na mesma área em que trabalho na EMPRESA
- b) ☐ Sim, em outra área
- c) ☐ Não

SOBRE SENHAS

6.Alguém, além de você, sabe a(s) sua(s) senha(s) utilizada(s) para acessar informações da EMPRESA? ☐ Sim ☐ Não

7.Você utiliza a senha de algum outro funcionário para acesso à informações da EMPRESA? ☐ Sim ☐ Não

8.Você anota as suas senhas em algum local próximo ao computador, na agenda, ou local similar? ☐ Sim ☐ Não

9.Você deixa outras pessoas utilizarem sua senha para algum trabalho rápido?

☐ Sim ☐ Não

10.Com que frequência você altera (s) sua(s) senha(s):

- a) ☐ Mensalmente

- b) ☐ Trimestralmente
- c) ☐ Semestralmente
- d) ☐ Somente quando o sistema solicita alteração

SOBRE DIVULGAÇÃO DE INFORMAÇÕES

11. Como você procede para fornecer informações, que você tem acesso, solicitadas por telefone ou e-mail?

- a) ☐ Forneço a informação, pois não há nada confidencial em minha área.
- b) ☐ Forneço a informação após identificar o solicitante
- c) ☐ Solicito autorização a meu superior para liberar a informação;
- d) ☐ Outros:

12. Você sabe quais as informações são vitais para o negócio da EMPRESA?

☐ Sim ☐ Não

SOBRE ACESSO À INFORMAÇÃO

13. Ao sair você costuma deixar seu computador bloqueado ou efetuar o LogOff?

☐ Sim ☐ Não

14. O seu setor possui informações consideradas confidenciais? ☐ Sim ☐ Não

15. Na sua opinião, todos os funcionários do seu setor sabem a importância das informações da EMPRESA? ☐ Sim ☐ Não

16. Na sua opinião, seria difícil pessoas externas conseguirem informações importantes na EMPRESA? ☐ Sim ☐ Não

17. Quais os tipos de informações que você tem acesso?

- a) ☐ Informações operacionais
- b) ☐ Informações gerenciais
- c) ☐ Informações confidenciais
- d) ☐ Informações imprescindíveis à continuidade do negócio
- e) ☐ Não tenho acesso a nenhuma informação importante

OBSERVAÇÕES

Qualquer observação sobre alguma resposta, favor informar o nº da questão e a Observação:

APÊNDICE B - Política de Segurança

Introdução

A cada dia novas ameaças à segurança das redes computacionais aparecem, colocando em risco os negócios das Organizações. Portanto, o desenvolvimento, a freqüente atualização e a eficaz aplicação de normas e regras que permitem lidar com tais ameaças são de fundamental importância nos dias de hoje. Existem diversos tipos de ameaças de uma variedade de fontes tais como, fraudes eletrônicas, sabotagem, vandalismo, fogo, etc. Os problemas proporcionados por vírus, hackers, ataques de DoS (deny of service) levam à alteração ilegal dos sistemas, à perda de informações e à interrupção do funcionamento normal dos sistemas. Estes têm se tornado cada vez mais comuns, mais ambiciosos e mais sofisticados.

A dependência nos serviços, a interconexão de redes públicas e privadas e o compartilhamento das informações colocam as Organizações vulneráveis as ameaças de segurança. Isto tudo serve de motivação para a implantação de uma norma de segurança.

1. Objetivo

Essa política de segurança têm o objetivo de fornecer um conjunto de Regras e Recomendações aos administradores de rede e usuários, visando a proteção e segurança dos equipamentos, dados, pessoas e instalações da empresa, a saber:

- Estabelecer procedimentos para a instalação e manutenção de ferramentas, hardware e software, visando a segurança dos sistemas computacionais e de comunicação do Rífoles Praia Hotel & Resort.
- Orientar, por meio de suas diretrizes, todas as ações de segurança de todos os setores para minimizar os riscos de segurança e garantir autenticidade, confidencialidade, integridade e disponibilidade da informação.
- Estabelecer procedimentos visando prevenir e responder a incidentes de segurança.

2. Abrangência

Esta política de segurança tem abrangência para toda a Empresa, em relação às instalações, equipamentos, informação e pessoal relacionado a esta e abrange os seguintes aspectos:

- Segurança física dos dispositivos de rede e da infra-estrutura;
- Segurança lógica dos equipamentos de rede;
- Segurança da Informação;

3. Segurança Física das Instalações de Processamento

A Segurança Física tem como objetivos específicos:

- Proteger edificações e equipamentos;
- Prevenir perda, dano ou comprometimento dos ativos;
- Manter a continuidade das atividades dos negócios;
- Reduzir as ameaças que coloquem em risco o bom funcionamento dos sistemas.

3.1 Sistema de Proteção contra Descargas Atmosféricas (SPDA) e Aterramento

Recomenda-se que as edificações onde encontram-se instalações de processamento, estejam protegidas por um sistema contra descargas atmosféricas (para-raios) e possuam sistema de aterramento eficiente, observando-se o seguinte:

- Todo sistema de proteção deve receber manutenção preventiva e inspeção anualmente.
- O projeto, instalação e manutenção do sistema deve estar em conformidade com a norma NBR-5419-2000.
- A função do para-raio é proteger edificações e pessoas, não abrangendo necessariamente equipamentos eletro-eletrônicos.
- Recomenda-se a utilização de protetores para os equipamentos considerados essenciais, tais como centelhadores a gás, varistores ou similares, adequados para cada tipo de equipamento.
- Em relação à rede elétrica, aconselha-se o uso dos para-raios de baixa tensão, do tipo pastilhas de Óxido de Zinco, nos quadros elétricos de entrada do edifício.
- A inspeção e medição do sistema de aterramento também devem ser anual, conforme a norma vigente.

3.2 Fornecimento de energia

Os equipamentos devem estar protegidos contra falhas de alimentação elétrica, observando-se as especificações do fabricante do equipamento quanto ao fornecimento de energia:

- É altamente recomendado o uso de no-break em equipamentos que suportam atividades críticas e para todos os componentes do backbone do Hotel.
- O uso de grupo-gerador em instalações estratégicas e áreas do núcleo de TI é fortemente recomendado.
- Para o caso dos ativos classificados com criticidade máxima (servidores e central telefônica) uso de no-breaks que tenham autonomia de no mínimo uma hora é obrigatório.
- Para outros equipamentos em áreas sujeitas a corte do fornecimento de energia freqüentemente, o seu uso deve ser estudado, sendo uma boa alternativa a aquisição de no-break com maior autonomia.
- Tanto para o no-break como para o grupo-gerador, convém que seja firmado um contrato de manutenção para que as peças e componentes do sistema estejam sempre em perfeito estado e de acordo com as recomendações do fabricante.
- Equipamento de rede classificado com criticidade máxima deverá dispor de $N+1$ fontes de alimentação, onde N é igual ao número mínimo de fontes para suportar a carga imposta pela configuração do equipamento. A fonte redundante deverá estar operacional, no modo load sharing, de modo que o failover de uma das fontes seja imperceptível.
- A equipamento com mais de uma fonte de alimentação recomenda-se alimentação múltipla de circuitos elétricos, de modo a evitar um único ponto de falha, correspondendo um circuito para cada fonte.
- É importante que as salas de equipamentos do backbone do Rifolet recebam alimentação de circuitos totalmente independentes, ou seja, diferentes dos circuitos que alimentam os prédios vizinhos. Esses circuitos devem estar interligados diretamente à rede elétrica primária da empresa.
- Convém ainda que as salas contendo os equipamentos possuam iluminação de emergência e interruptores elétricos de emergência que permitam o desligamento em caso de necessidade.

- A instalação elétrica deve seguir a norma NBR-5410 "Instalações Elétricas de Baixa Tensão".

3.3 Segurança do cabeamento

A segurança do cabeamento é tão importante quanto a segurança dos equipamentos de rede. Assim, é importante observar o seguinte:

- O cabeamento de fibra óptica deve ser preferencialmente subterrâneo e, neste caso, o encaminhamento do mesmo deve ser através do sistema de dutos de uso exclusivo da empresa, evitando passar outros cabos dentro desse tubulação.
- A instalação de cabeamento de fibra óptica com gel em seu núcleo deve seguir as recomendações das normas vigentes.
- O cabeamento de fibra óptica do núcleo do backbone deve possuir proteção anti-roedor, sendo que a norma NBR 14773 pode ser consultada.
- As rotas do cabeamento de fibra óptica devem receber sinalização específica para evitar acidentes e/ou danos de terceiros. Cabe ao Centro de Processamento de Dados local manter a relação e identificação das rotas dos cabos ópticos do backbone.
- As caixas de passagem devem ser mantidas adequadas ao uso e possuir tampas de ferro com identificação do logotipo do Rifóles.
- A instalação de cabeamento, tanto em cobre quanto em fibra óptica, deve seguir as recomendações da norma CCE/USP UN 2.0, NBR 14565 e TIA/EIA 568-B.2-1.

4. Segurança Ambiental

A Segurança Ambiental tem por objetivo adotar medidas que evitem risco às instalações e equipamentos por ocorrência dos seguintes fatores:

- Incêndio;
- Fumaça;
- Poeira;
- Vibração;
- Umidade;
- Água.

Recomenda-se que:

- Sensores de controle destes fatores estejam integrados a um sistema que permita a monitoração remota, assim como o disparo de alarmes.
- Sejam adotados, ainda, procedimentos restringindo comida, bebida e fumo dentro das Instalações de Processamento.

5. Segurança do acesso às instalações

A Segurança das instalações com relação ao acesso físico tem como objetivos específicos:

- Prevenir e controlar o acesso não autorizado a informações e instalações físicas da Unidade/Departamento;
- Prevenir perda, dano ou comprometimento dos ativos;
- Evitar a exposição ou roubo de informação.

5.1 Controle de Acesso

As instalações de processamento ou outras áreas de segurança devem ser equipadas com controles de entrada apropriados, de forma que somente pessoal autorizado tenha acesso liberado.

O controle de acesso depende dos requisitos de segurança próprios da área considerada e pode se dar através de:

- Controle de entrada (métodos de acesso físico);
- Crachás de identificação e procedimentos pelos quais o acesso é concedido, modificado ou negado;
- Chaves e/ou cartão inteligente;
- Restrições de acesso baseadas no status do funcionário e horas de operação;
- Pontos de contato para acesso;
- Fechaduras eletrônicas;
- Combinação dos itens anteriores;

5.2 Segurança do acesso à instalação:

Convém que cada Unidade crie normas ou procedimentos que complementem os sistemas de segurança adotados e sugeridos:

- Recomenda-se que o Controle de Acesso utilize como validação um sistema de cartão com PIN (personal identification number). Eventualmente, em locais mais críticos, pode-se optar também pela validação biométrica (impressão digital, por exemplo);
- O fornecimento dos cartões de acesso deve ser através do gerente responsável pela segurança;
- O extravio ou roubo de cartões de acesso deve ser informado imediatamente à segurança;
- Os cartões de acesso devem ser mantidos pelos seus respectivos proprietários todo o tempo, e nunca devem ser emprestados para qualquer pessoa ou deixados desprotegidos;
- Mesmo durante o horário comercial o acesso com cartão deverá ser necessário para os funcionários;
- Todas as portas externas são bloqueadas fora do horário comercial normal;
- Qualquer pessoa dentro de uma área de segurança deverá dispor de identificação de acordo com a função por ela exercida;
- Os funcionários não podem permitir a estranhos o acesso aos recursos de rede.
- Os visitantes ou funcionários sem permissão deverão ganhar autorização e identificação especial para ter acesso e permanecer nos locais de segurança, devendo estar explícito qual o propósito de adentrar ao local, quais as atividades que serão desenvolvidas e a quais recursos estas pessoas terão acesso;
- Serviços de terceiros em Instalações de Processamento devem ser agendados previamente, deve ser fornecido o nome das pessoas que executarão o serviço, assim como o detalhamento da atividade a ser desenvolvida;
- Tanto para o caso de terceiros quanto para visitantes, uma pessoa da Unidade/Depto deve sempre acompanhar o trabalho, de forma que um estranho nunca fique sozinho nas instalações;

Adicionalmente, convém que o Controle de Acesso utilize sistemas eletrônicos complementares:

- Circuito Fechado de TV nas áreas consideradas estratégicas, havendo registro da imagem local por meio de câmeras de vídeo, que deverão estar sendo armazenadas em

alguma mídia, de forma a poderem ser resgatadas em caso de alguma ocorrência ou auditoria;

- Alarme que envie alguma mensagem a uma estação de gerenciamento remota ou a algum dispositivo móvel que ande sempre com o gerente da Unidade/Depto caso ocorra algum acesso não autorizado;

5.3 Segurança para o Sistema de Telefonia

Semelhante às Instalações de Processamento, o sistema de telefonia requer cuidados e procedimentos que visem a segurança:

- O acesso físico ao hardware do sistema de telefonia e aos terminais de configuração de sistema é restritivo aos administradores do sistema de telefonia e ao pessoal da companhia provedora do serviço;
- O sistema de telefonia deve estar em uma área segura que necessite de métodos de acesso especializados via chaves ou cartões eletrônicos;
- A instalação de novos modems deve ser coordenada pelo grupo responsável, a fim de fornecer a segurança necessária e infra-estrutura de rede para manter a segurança.
- Todos os quadros telefônicos existentes no prédio devem está devidamente fechados por meio de trava mecânica e/ou eletrônica, chave ou outro dispositivo que permita barrar o acesso de pessoas não autorizadas
- A fim de dificultar a sabotagem, clonagem ou similares nos telefones da empresa, os esquemas de numeração dos ramais telefônicos e seus circuitos não deve ser afixados nos quadros telefônicos ou em lugares de fácil acesso.

6. Segurança dos equipamentos

A segurança dos equipamentos está diretamente relacionada aos procedimentos de instalação e proteção, atentando-se ao seguinte:

- A instalação de equipamentos deve seguir o procedimento recomendado pelo fabricante e/ou normas específicas existentes, na falta destes, deverá ser consultado o setor responsável pela instalação elétrica da Unidade;
- Os equipamentos devem ser instalados de modo a permitir fácil acesso à equipe de manutenção de rede;
- A instalação deve garantir boa ventilação a seus componentes;

- Terminais públicos devem estar presos via dispositivos de alarme antifurto e cabos com travas;
- Equipamento instalado fora das áreas de segurança deverá dispor de proteção física, como armário, gaiola, ou equivalente, com trava mecânica e/ou eletrônica, chave ou outro dispositivo que permita barrar o acesso de pessoas não autorizadas;
- A instalação, manutenção e atualização de equipamentos no backbone da empresa é de responsabilidade única e exclusiva dos Centros de Processamento de Dados.

6.1 Segurança de equipamentos instalados fora do Rifoles

Os equipamentos instalados fora dos limites do Hotel e interligados a ele, devem ter autorização expressa do responsável pela administração do backbone do Hotel para poder manter a conexão.

6.2 Manutenção de equipamentos

Em relação à manutenção dos equipamentos, deve-se observar o seguinte:

- A manutenção de equipamentos deve ser de acordo com intervalos e especificações do fabricante. Se essas recomendações não forem conhecidas, procedimentos de manutenção devem ser elaborados e aplicados;
- Apenas profissionais autorizados podem fazer manutenção nos equipamentos, ou seja, o próprio fabricante, empresas autorizadas por ele e equipes de manutenção de redes dos Centros de Processamento de Dados.
- Devem ser mantidos registros de todas as falhas suspeitas ou ocorridas em toda manutenção preventiva e corretiva. É recomendado o uso de um sistema computacional com um banco de dados para estas informações, preferencialmente com acesso via web.
- Equipamentos enviados para manutenção de terceiros e que possuem meios de armazenamento (disco rígido, fitas, etc) devem ter seus itens checados para assegurar que toda informação sensível, sigilosa e software licenciado foi removido ou sobreposto antes da alienação do equipamento.
- Um hardware sobressalente deve estar disponível caso a criticidade do equipamento seja alta;

- Dispositivos de armazenamento danificados, assim como equipamentos, devem sofrer uma avaliação de riscos para verificar se eles devem ser destruídos, reparados ou descartados. Recomenda-se que cada ativo ou parte dele seja avaliado por uma Comissão constituída pelo Diretor da Unidade, à qual caberá dar o devido destino.

7. Segurança lógica ou Segurança da informação

Tão importante quanto a segurança física é a segurança da informação.

Recomenda-se a adoção das seguintes medidas que visem proteger a integridade das informações do Hotel:

- Sugere-se a utilização de cofres especiais para a guarda das mídias contendo as cópias de segurança (back-up). Estes cofres especiais são resistentes a incêndio, umidade, interferências eletromagnéticas, poeira, fumaça e vandalismo;
- O acesso às mídias de back-up deve ser restrito ao pessoal autorizado;
- O acesso ao aplicativo de back-up deve ser restrito ao pessoal autorizado;
- Equipamentos, informações ou software não devem ser retirados da organização sem autorização;
- Toda informação, quer em mídia eletro-eletrônica ou papel, deve ficar sempre guardada em locais apropriados e de acesso restrito, especialmente fora dos horários de trabalho normal;
- É recomendado que uma outra cópia seja guardada fora do site, semanalmente, por meio do gerente ou um funcionário autorizado;
- Aconselha-se que seja feita uma vez por semana o back-up completo dos sistemas e, diariamente, de preferência à noite ou madrugada, a cópia incremental, ou seja, o que foi modificado;
- A restauração deve ocorrer da última cópia completa até as cópias com as alterações incrementais (layered over), até o momento do evento.

7.1 Contas de Acesso aos Sistemas

Sobre o acesso aos sistemas, segue:

- Cada usuário deve possuir uma conta individual. Não deve haver contas corporativas ou contas compartilhadas por mais de um usuário, a não ser em situações específicas e prazos determinados;
- O Centro de Processamento de Dados manterá um sistema unificado de contas dos usuários dos Sistemas do Rifóles, sejam Corporativos, sejam de Internet;
- Cada novo funcionário da empresa receberá uma conta única para acessar os sistemas, incluindo o acesso remoto, necessário à execução de suas funções;
- A solicitação de abertura de contas em quaisquer dos sistemas se dará pelo preenchimento de um Termo de Identificação e Compromissos (vide Anexo V);
- Após receber uma conta, cujas identificações foram criadas pelos administradores dos sistemas ou de redes, o proprietário da conta deverá alterar sua senha após realizar o seu primeiro login.
- A autorização e o nível da conta será concedido pelo proprietário e/ou administrador do sistema, ou se for o caso, pelo administrador de rede;
- Contas de usuários que venham a se desligar da empresa, serão canceladas no ato de sua demissão, salvo casos excepcionais que serão analisados pelo Centro de Processamento de Dados;
- O Setor de Pessoal deve comunicar o responsável pelo Centro de Processamento de Dados sobre o desligamento dos funcionários imediatamente tenha sido tomada a decisão.

7.2 Segurança para rede de dados

A segurança para a rede sob o aspecto da segurança lógica deve considerar filtros e protocolos habilitados nos ativos.

- Cabe ao CPD (Centro de Processamento de Dados) implantar regras de proteção nos seus roteadores e/ou firewall para proteger as redes de uma forma restritiva (método de exceção);
- Para os roteadores do backbone, os filtros e regras deverão ser obrigatórios e estudados para cada caso;
- O acesso lógico aos equipamentos de rede (roteadores, switches, modems, servidores, ou outros) deve sempre ser protegido por senhas não-padrão (default ou inicial), quer para suporte, configuração ou gerenciamento e, preferencialmente, a partir de um número restrito de equipamentos;

- As senhas de acesso lógico aos equipamentos devem ser trocadas periodicamente, a cada 90 dias no máximo, ou quando o administrador ou funcionário que as detenha venha a se desligar da empresa ou da função;
- Os responsáveis devem manter um registro (log) para as alterações de configuração dos equipamentos de rede;
- É recomendado o uso de aplicativos de gerenciamento para os equipamentos de rede e servidores, que notifiquem o administrador em casos de anomalias;
- Para o caso do gerenciamento SNMP, não deve estar habilitado se não estiver em uso, do contrário, garantir acesso estritamente aos administradores responsáveis;
- Também é recomendada a utilização de antivírus que monitorem as mensagens de correio eletrônico;
- As informações de configuração dos equipamentos devem estar armazenadas em servidores administrativos, nunca em servidores públicos ou de produção;
- Sempre que possível, os equipamentos de rede devem fazer back-up de sua configuração em servidores administrativos, buscando aumentar a segurança e confiabilidade;
- Os equipamentos devem ter habilitados somente os protocolos necessários;

7.3 Segurança de acesso remoto

- Somente o CPD podem fornecer acesso remoto as máquinas do Rifóles, sendo estes os responsáveis pela configuração do hardware;
- A autenticação deve ser necessariamente através de senhas, podendo estar combinada com recurso de identificação de chamada;
- Não deverá ser permitido múltiplo acesso simultâneo para o mesmo usuário, a menos em casos analisados e autorizados pelos gerentes responsáveis.
- Modems discados utilizados para administração do sistema de telefonia devem ser protegidos por senhas;
- A autenticação e o log de acesso de rede através de modems discados devem ser feitos via um sistema de relatório e autenticação centralizado;
- A utilização de modems em computadores instalados na empresa deve ser autorizada pelo Centro de Processamento de Dados.

7.4 Segurança para terminais públicos

- Todos os sistemas para utilização pública devem estar em uma rede de acesso restrito, configurados com um conjunto mínimo de utilitários;
- Os visitantes devem se dirigir à recepção, ou outro setor responsável, a fim de receber uma conta de convidado (guest);
- Contas de convidados (guest) são capazes apenas de acessar a Internet, aplicativos do Office, softwares de comunicação on-line (MSN, ICQ, etc) e jogos, nenhum outro recurso ou sistema interno;
- As contas de convidados (guest) são automaticamente desativadas por inatividade após 10 minutos;
- Contas de convidados devem ser configuradas com data de expiração com base nos requisitos dos mesmos;
- Os funcionários devem sempre encerrar a sessão (efetuar o logout), ou bloquear sua máquina antes de se ausentar do terminal;

7.5 Segurança para servidores

Além das recomendações, um plano de contingência deve ser criado para a recuperação de desastres.

- Os servidores devem ser configurados para suportar apenas os serviços necessários;
- Os servidores devem ser fisicamente seguros, permitindo acesso restrito;
- Os administradores dos servidores devem estar atentos a atualizações e correções de vulnerabilidades dos sistemas operacionais e software;

7.6 Segurança para notebooks e PDAs

- Os notebooks devem utilizar senhas de BIOS para evitar acesso não autorizado caso sejam roubados;
- Os usuários jamais devem deixar sessões abertas, efetuando o logout quando ele não estiver em uso;
- Recomenda-se que dados importantes sejam protegidos por senhas e criptografia;
- É fortemente recomendado que o usuário utilize senhas diferentes para os sistemas e equipamentos, defendendo-se em caso de roubo de alguma senha;

- Estes equipamentos portáteis devem estar presos fisicamente através de cabos, correntes ou outro dispositivo de segurança, ou ainda, trancados em gavetas ou armários quando fora de uso;

8. Segurança Administrativa

Cabe ao administrador as seguintes diretivas visando a segurança administrativa:

- É proibido o acesso aos arquivos e informações do usuário, exceto em caso de segurança ou apuração de algum fato envolvendo o próprio usuário, sempre com a ciência do gerente ou responsável pela rede;
- A monitoração de dados e voz que circulam através dos meios só deverá ser praticada visando a detecção de invasão ou outro assunto relacionado à segurança;
- O administrador que incorrer em alguma não-conformidade ou evento que resulte em parada ou prejuízo de serviços deve estar ciente que haverá investigação que poderá resultar em alguma ação contra ele;

Os usuários, por sua vez, devem atender às seguintes diretivas básicas:

- A utilização dos recursos de rede só é concedida mediante a adesão dos usuários às normas e diretivas de segurança vigentes, lendo, entendendo e assinando o termo adequado;
- É responsabilidade do usuário criar e trocar as senhas de acordo com as recomendações da norma, tendo ciência de que as contas são pessoais e intransferíveis;
- Os recursos jamais devem ser utilizados de maneira inadequada, de forma a comprometer os sistemas ou a segurança da rede, ou agindo de forma ofensiva;
- O usuário deve estar ciente de que atos impróprios resultarão em investigação, podendo acarretar punição;
- Os terminais devem ser bloqueados ou ter a sessão finalizada quando fora de uso;
- Notebooks, PDAs ou outros dispositivos portáteis estão sujeitos a inspeção pelo administrador;
- Os usuários concordam em participar de auditorias, em conformidade com as diretivas de segurança;

- Cabe ao usuário notificar à recepção ou responsável pelo local, qualquer observação em relação a defeitos, acesso não autorizado, falhas de segurança ou afins.

9. Diretrizes gerais para lidar com incidentes

Os funcionários devem ler e entender as seguintes diretrizes para lidar com incidentes:

- Todos os incidentes e suas soluções devem ficar registrados, sendo submetidos ao gerente de rede, ou ao administrador de rede ou alguém responsável pela rede e este ao Grupo de Segurança;
- A análise do incidente deverá ser discutida em uma reunião em grupo para identificar os pontos fracos do setor, visando prevenir incidentes futuros, procurando sempre contar com o apoio do CPD.

9.1 Em relação ao acesso físico

- No caso de um visitante não autorizado, o funcionário deve notificar imediatamente o departamento de segurança e solicitar auxílio para remoção do mesmo;
- Caso o visitante seja pego cometendo furto, ataque ou destruição da propriedade, deve-se notificar o departamento de segurança para que ele entre em contato com as autoridades competentes;
- Todas as testemunhas devem fornecer aos responsáveis pela segurança um depoimento detalhado do incidente que indique a presença de um visitante não autorizado e devem estar disponíveis para interrogatório posterior pela segurança e pelas autoridades competentes;
- Todas as portas, fechaduras e métodos de acesso que não estejam funcionando devem ser informados ao departamento de segurança. A segurança coordenará com o departamento de manutenção a correção do equipamento defeituoso;
- Os gerentes devem ser notificados quando um funcionário estiver envolvido em uma brecha de segurança;
- Os funcionários não devem tratar destas situações sozinhos, mas devem notificar a segurança e permitir que o pessoal da segurança controle a situação.

9.2 Em relação aos ativos de rede

- Sempre tentar identificar a causa do incidente;
- Se uma invasão causar parada ou ruptura de serviços, a prioridade é restabelecer os serviços, porém sempre que possível, os administradores devem tentar identificar a origem do problema, preservando as evidências;
- No caso de uma invasão é aconselhável rever as regras dos filtros dos roteadores, modificando-as para controlar os efeitos;
- Em caso de incidente que resulte em perda de dados, o funcionário deve notificar ao responsável pela rede imediatamente;
- Em caso de incidentes como falha de hardware, comprometimento do sistema ou invasões de um servidor ou outro ativo, deve-se removê-lo da rede e deixá-lo em seu estado atual a fim de permitir um trabalho de investigação eficiente;

10. Auditoria

É importante que o setor adote um esquema de Auditorias. Neste caso, os funcionários devem ler e entender e cooperar com os procedimentos e diretivas adotadas.

- As auditorias serão realizadas principalmente em servidores e equipamentos de rede para assegurar a configuração e atualização adequadas;
- Os auditores podem ser funcionários internos ou de órgãos externos, com ou sem o conhecimento dos administradores;
- Auditorias nas linhas telefônicas devem ocorrer regularmente para verificar a funcionalidade dos modems existentes e para identificar os não autorizados;
- As auditorias em sistemas de usuários seguirão as diretivas adotadas;
- As auditorias podem ser notificadas ou não.

10.1 Auditorias notificadas

São anunciadas previamente aos funcionários, de modo que tenham tempo para preparar o ambiente e rever suas práticas. Seus propósitos são:

- Analisar os sistemas em relação aos componentes de segurança;
- Verificar se as práticas dos usuários não são impróprias ou desafiam a segurança;
- Assegurar que as informações são apropriadas e cumprem aos objetivos.

10.2 Auditorias não anunciadas

São aleatórias, buscando a identificação de vulnerabilidades e a constante conscientização com a segurança.

Podem ser implementadas na forma de ataques simulados, desde que permaneçam no escopo da rede local.