UNIVERSIDADE FEDERAL DE PERNAMBUCO
CENTRO ACADÊMICO DO AGRESTE
NÚCLEO DE GESTÃO
CURSO DE ADMINISTRAÇÃO

CLEYLLTON HUDSON CURSINO DE BRITO JORGE

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO: UMA ANÁLISE DA PERCEPÇÃO DOS ESTUDANTES DE ADMINISTRAÇÃO DA UNIVERSIDADE FEDERAL DE PERNAMBUCO – CAMPUS ACADÊMICO DO AGRESTE

CARUARU
2014

UNIVERSIDADE FEDERAL DE PERNAMBUCO
CENTRO ACADÊMICO DO AGRESTE
NÚCLEO DE GESTÃO
CURSO DE ADMINISTRAÇÃO

CLEYLLTON HUDSON CURSINO DE BRITO JORGE

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO: UMA ANÁLISE DA PERCEPÇÃO DOS ESTUDANTES DE ADMINISTRAÇÃO DA UNIVERSIDADE FEDERAL DE PERNAMBUCO – CAMPUS ACADÊMICO DO AGRESTE

Trabalho de Conclusão de Curso apresentado à Coordenação do Curso de Administração, da Universidade Federal de Pernambuco, Centro Acadêmico do Agreste, como requisito parcial para aprovação na disciplina Trabalho de Conclusão de Curso.

Orientadora: Profª. Drª. Maria das Graças Vieira

CARUARU
2014

Catalogação na fonte:
Bibliotecária Simone Xavier CRB4 - 1242

J82p Jorge, Cleyllton Hudson Cursino de Brito.
Política de segurança da informação: uma análise da percepção dos estudantes de administração da Universidade Federal de Pernambuco – Campus Acadêmico do Agreste. / Cleyllton Hudson Cursino de Brito Jorge. - Caruaru: O Autor, 2014.
62f..; 30 cm.

Orientadora: Maria das Graças Vieira.
Monografia (Trabalho de Conclusão de Curso) – Universidade Federal de Pernambuco, CAA, Administração, 2014.
Inclui referências bibliográficas

1 Segurança da informação. 2. Gestão de informação. 3. Administração. I. Vieira, Maria das Graças. (Orientadora). II. Título.

658 CDD (23. ed.) UFPE (CAA 2014-177)

CLEYLLTON HUDSON CURSINO DE BRITO JORGE

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO: UMA ANÁLISE DA PERCEPÇÃO DOS ESTUDANTES DE ADMINISTRAÇÃO DA UNIVERSIDADE FEDERAL DE PERNAMBUCO – CAMPUS ACADÊMICO DO AGRESTE

Este trabalho foi julgado, adequado e aprovado para a obtenção do título de graduação em Administração da Universidade Federal de Pernambuco - Centro Acadêmico do Agreste.

Caruaru, 30 de julho de 2014.

_____

Profº. Drº. Cláudio José Montenegro de Albuquerque
Coordenador do Curso de Administração

BANCA EXAMINADORA:

_____

Profª. Drª. Maria das Graças Vieira
Universidade Federal de Pernambuco - Centro Acadêmico do Agreste
Orientadora

_____

Prof. Dr. Silvana Medeiros Costa
Universidade Federal de Pernambuco - Centro Acadêmico do Agreste
Banca

_____

Prof.
Universidade Federal de Pernambuco - Centro Acadêmico do Agreste
Banca

Dedico este trabalho a Minha mãe, Maria Cleriane Cursino de Brito, Meu avô (In memoriam) Ademar Bezerra de Brito, e a minha avó (In memoriam) Cleria Cursino de Brito

AGRADECIMENTOS

Agradeço a todos que me acompanharam nestes 4 anos e 6 meses de jornada, a luta de todos os dias minha mãe, a toda minha família, amigos e ao apoio dos professores que sem eles não conseguiria.

[...]E o fim é belo incerto
depende de como você vê, o
novo o credo a fé que você
deposita em você e só[...]

O TEATRO MÁGICO

RESUMO

Com a informação ganhando cada vez mais importância nas organizações, faz se perceber que os gestores cada vez mais devam está preparados para um mercado onde o valor da informação é o ativo mais valioso da organização, e que é necessário a proteção desta, através da classificação da informação e de manter está informação sempre com, confidencialidade, integridade, Autenticidade e Disponibilidade, características essas que normalmente são protegidas com uma boa Política de Segurança da Informação. Este trabalho tem como objetivo a analisar a percepção dos estudantes de administração do campus acadêmico do agreste acerca do tema Políticas de Segurança da Informação, já que os estudantes de administração se preparam para ser os futuros gestores das organizações.

Palavras-chave: Políticas de Segurança da Informação, Administração, Gestão da Informação.

ABSTRACT

With information increasingly gaining more importance in organizations, it is clear that the managers increasingly must is prepared for a market where the value of information is the most valuable asset of the organization, and that this protection is necessary, by classifying information and keep this information always, confidentiality, integrity, authenticity and availability, these characteristics are usually protected with a good information Security Policy. This study aims to examine the students' perceptions of campus academic administration of the rough on the subject of Information Security Policies, as business students preparing to be the future managers of organizations.

Keywords: Information Security Policies, Management, Administration, Information Management.

LISTA DE ABREVIATURAS E SIGLAS

ABNT – Associação Brasileira de Normas e Técnicas

CERT - Centro de Estudos, Respostas e tratamentos de incidentes de Segurança no Brasil

DNS – Servidor de Nomes de Domínio (*Domain Name Service*)

DoS – Negação de Serviço (*Denial of Service*)

IP – Protocolo de Internet (*Internet Protocol*)

ISO/IEC – Organização Internacional de Padronização (*International Organization for Standardizatio)*

NBR – Norma Brasileira

TI - Tecnologia Da Informação

LISTA DE TABELAS

LISTA DE GRÁFICOS

SUMÁRIO

1. INTRODUÇÃO

Segundo Smicaluk et. al. (2007), com a revolução da tecnologia, a informação tornou-se o ativo mais valioso das empresas e a segurança dessa informação virou um fator primordial, com isso, a informação torna-se um fator importante dentro das organizações. Inúmeras empresas sofrem diariamente ataques à sua base de dados e redes de computadores, muitos desses ataques não obtêm sucesso, mas quando algumas dessas ameaças obtêm sucesso no ataque, pode representar um prejuízo altíssimo, levando muitas vezes ao fechamento da organização atacada. Um exemplo disso atualmente é a disseminação de vírus e os ataques de *hackers* pela Internet a várias corporações, o que tem levado as organizações a investir alto em *softwares* como antivírus, *firewall* e filtros de e-mail para conter essas pragas virtuais.

Ainda segundo Smicaluk et. al. (2007), a segurança da informação pode ser ameaçada de várias formas, como acidentes naturais (incêndio, enchentes, furacões, etc.), acidentes estes que podem comprometer a integridade das informações, ou até mesmo causar a perda total destas. A informação também pode ser corrompida através de invasões lógicas a estrutura da organização, por *hackers* e *crackers*, que além de quebrar a privacidade dos sistemas podem contaminar as máquinas com vírus, cavalos de tróia, *spams*, *spywares*, entre outros. Porém o mais comum é que o fator humano seja o calcanhar da Aquiles em qualquer projeto de sistema de informação. A segurança da informação pode ser prejudicada de várias formas através dos erros humanos, como: um mau gerenciamento das permissões de acesso a informação pode prejudicar a disponibilidade e levar a ocorrência de fraudes na informação.

Apesar da conscientização da maioria das organizações quanto à necessidade de criação e cumprimento de uma política de segurança da informação, a implantação sofre muita resistência por mudar a rotina dos funcionários. E por muitas vezes, uma resistência, pelo próprio gestor não ter uma percepção positiva quanto à importância de uma política de segurança da informação.

Esse aumento da utilização da tecnologia da informação aponta para que os gestores de TI devam investir em treinamento e numa implementação de uma política de segurança. Mas quanto aos futuros gestores de organizações, novas gerações destes saem da universidade todo ano para o mercado, qual será a percepção deles acerca do tema “política de segurança da informação”.

1.1 Objetivos

1.1.1 Objetivo geral

O objetivo geral desta pesquisa é investigar a percepção dos estudantes do curso de administração da Universidade Federal de Pernambuco – Campus Acadêmico do Agreste, sobre a importância do que é uma política de segurança da informação.

1.1.2 Objetivos específicos

Os objetivos adjacentes ao objetivo geral trilham o caminho ao alcance da centralização desta pesquisa. São eles:

- Identificar as práticas dos estudantes relativas à política de segurança da informação;
- Identificar soluções para melhor conscientizar acerca do tema; e
- Analisar o preparo dos estudantes na universidade acerca do tema.

1.2 Justificativa

Os sistemas de informação estão cada vez mais presentes na rotina das pessoas, isso reflete uma perspectiva que existe desde uma visão empresarial a uma visão pessoal e a grande presença de sistemas de informação automatizados faz perceber que a questão de segurança não pode ser algo que apenas o gestor de TI deva ter conhecimento, mas deve ser uma

preocupação geral e algo que todos devam ter conhecimento. Segundo Laudon e Laudon (2004), conhecer sistemas de informação é essencial para os administradores, porque a maioria das organizações precisa deles para sobreviver.

Essa pesquisa ajudará a ver como está o aprendizado e a percepção atual dos futuros gestores acerca do tema políticas de segurança da informação.

A pesquisa foi realizada com os estudantes de administração que visa conhecer como é o grau de conscientização e compreensão sobre políticas de segurança com futuros gestores, levando em consideração que a pesquisa é realizada com estudantes do curso superior de Administração de Empresas e estão sendo preparados para gerir empresas. E hoje é necessário que todos dentro de uma empresa, principalmente os gestores tenha uma boa percepção sobre políticas de segurança e que os futuros gestores estejam sendo preparados para lidar com os problemas de segurança da informação.

Dessa forma esta pesquisa se justifica por mostrar um cenário sobre os futuros gestores e como eles estão preparados acerca do tema de política de segurança da informação.

2. REVISÃO DA LITERATURA

Neste capítulo serão introduzidos alguns conceitos importantes para um melhor entendimento do trabalho como os conceitos de ativos, informação, sistemas de informação, segurança da informação, política de segurança da informação e engenharia social.

2.1 ATIVOS

Segundo Modulo (2005, apud Bauer 2006, p.7), "*ativo é todo elemento que compõe os processos, incluindo o próprio processo, que manipulam e processam a informação, a contar a própria informação, o meio em que ela é armazenada, os equipamentos em que ela é manuseada, transportada e descartada.*"

O termo ativo vem da área de operação de valores financeiros onde pode ser considerado em elemento ou bem de valor para a organização, devido a este valor, necessita de proteção. Segundo a norma ISO/IEC 13335: 2004 ativo é definido como qualquer coisa que tenha algum valor para a organização.

De várias maneiras pode se dividir os ativos para um melhor tratamento. Entre as formas de dividir estão: equipamentos, aplicações, usuários, ambientes, informações e processos. Desta forma, segundo Sêmola (2003), é possível identificar melhor as fronteiras de cada grupo, tratando-os com especificidade e aumentando qualitativamente as atividades de segurança.

Para os fins desse trabalho no próximo tópico explanaremos sobre a informação como um ativo para as organizações.

2.1.1 Informação

Segundo Moraes e Laureano (2005), a informação é um ativo que, como qualquer outro ativo importante para os negócios, tem um valor para a organização e, conseqüentemente, necessita ser adequadamente protegido. DIAS (2003), acrescenta que, a informação é o principal patrimônio da empresa.

Segundo a norma ISO/IEC 13335: 2004, ativo de informação pode ser conceituado como qualquer componente que pode ser humano, tecnológico, físico ou lógico que domina ou sustenta um ou mais processos de negócio de determinada área.

> *"*A *informação* é um ativo que, como qualquer outro ativo importante, é essencial para os negócios de uma organização e, consequentemente, necessita ser adequadamente protegida. [...] A informação pode existir em diversas formas. Ela pode ser impressa ou escrita em papel, armazenada eletronicamente, transmitida pelo correio ou por meios eletrônicos, apresentada em filmes ou falada em conversas. Seja qual for a forma de apresentação ou o meio através do qual a informação é compartilhada ou armazenada, é recomendado que ela seja sempre protegida adequadamente." ABNT NBR (ISO/IEC 27002, 2005, p.2)

Segundo Carvalho (2001, Apud Gurgel, 2006), a informação nos últimos tempos se tornou um elemento fundamental para a sobrevivência e existência das organizações. As organizações se alimentam de informações e traça seu rumo com base nelas, de forma que fornece o sentido de uma organização ser. A todo instante, milhares de dados estão sendo processados em informações para uso das organizações, essas informações procedem de fontes internas e externas. Segundo Gurgel (2006), na chamada era da informação, a mesma não deve ser posta em segundo plano ao se falar em estratégia. E não só na estratégia, mas a informação deve estar sempre sendo observada e tratada da melhor forma possível, em prol das vantagens proporcionadas por uma abordagem que trate a informação como um bem valioso.

Esse valor que a informação agrega se dá principalmente por a informação desempenhar papéis importantes tanto na definição quanto na execução de uma estratégia. Ela ajuda na identificação das ameaças e das oportunidades para a empresa e cria o cenário para uma resposta competitiva mais eficaz (REZENDE E ABREU, 2000).

E a valorização da informação fez com que muitas vulnerabilidades e ameaças tivessem como alvo principal as informações. Segundo Bauer (2006), quanto maior for à organização maior será sua dependência da informação.

2.2 SISTEMAS DE INFORMAÇÃO

Para Stair e Reynolds (2002), sistema de informação é um conjunto de elementos ou componentes inter-relacionados que coletam, manipulam e disseminam os dados e as informações e fornecem um mecanismo de feedback[1] para atender um objetivo. Laudon; Laudon (2004) adicionam que as saídas dos sistemas de informação são destinadas à tomada de decisões, à coordenação e ao controle de uma organização. Os sistemas de informação podem ser de forma manual ou computadorizado, sendo que a maioria dos sistemas começam como manuais e se tornam computadorizados.

Ainda segundo Stair e Reynolds (2002), o sistema de informação computadorizado é composto de hardware, software, banco de dados, telecomunicações, pessoas e procedimentos para coletar, manipular, armazenar e processar os dados em informação.

Vulnerabilidades e ameaças tentam roubar os dados e as informações em todos os componentes de um sistema de informação. Segundo Dias (2003) a informação está em constante risco, e foram criados técnicas e documentos para a proteção dos sistemas de informação. Nos próximos tópicos será explanado as vulnerabilidades, ameaças, e os princípios de segurança dos sistemas de informação.

2.3 VULNERABILIDADES E AMEAÇAS.

Segundo Laudon e Laudon (2004) o uso de sistemas de informação automatizado fez com que os dados focem concentrados em arquivos de computador, o que consequentemente gerou uma grande vulnerabilidade pois os dados automatizados são mais suscetíveis a destruição, fraude e uso indevido.

Vulnerabilidade no contexto da tecnologia da informação é definida pela cartilha do CERT (2006), como uma falha no projeto, implementação ou configuração de um *software* ou sistema operacional que, quando explorada por um *hacker*, resulta na violação da segurança de um computador ou rede de computadores, Segundo a norma ISO/IEC 13335: 2004, ameaça é a causa

[1] Feedback Em sistemas de informação, o feedback é a saída utilizada para promover as mudanças na entrada ou nas atividades de processamento.

potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização.

Existem casos onde um *software* ou sistema operacional instalado em um computador pode conter uma vulnerabilidade que permite sua exploração remota, ou seja, através da rede, como os vários problemas do *Internet Explorer,* da Microsoft, publicados na seção informes de segurança em (TECHNET, 2010). De acordo com Bertin (2001 apud Laudon e Laudon, 2004), cita que a amazon.com perdeu 244 mil dólares a cada hora que ficou fora de serviço durante o ataque de um hacker, em fevereiro de 2000.

Portanto, um *hacker* conectado à *Internet*, ao explorar tal vulnerabilidade, pode obter acesso não autorizado ao computador vulnerável. Entretanto, fabricantes em muitos casos não disponibilizam novas versões de seus *softwares* quando é descoberta alguma vulnerabilidade, mas sim correções específicas chamadas *patches*.

Existem vulnerabilidades, porém, que não decorrem propriamente da má configuração dos serviços ou falhas em sistema operacional. De fato, as mais comuns são causadas devido ao uso descuidado ou inadvertido, por parte dos funcionários, de recursos como: o correio eletrônico, a *internet* ou a instalação de *softwar*es não confiáveis.

Segundo Laudon e Laudon (2004), quando grandes quantidades de dados estão em formato eletrônico, esses dados ficam vulneráveis a muito mais tipos de ameaças do que se estivesse em formato manual. Através dos meios eletrônicos, principalmente o uso de redes de computador, se propagam os vírus, *spywar*es, *trojan-horses* entre outros. A Tabela 2.1 apresenta algumas formas de ataque:

Tabela 2.1 – Formas de Ataque.

Ameaça	**Explanação**
Adware	*Software* especificamente projetado para apresentar propagandas, seja através de um *browser*, seja através de algum outro programa instalado em um computador.
Backdoors	Programas que permitem o retorno de um invasor a um computador comprometido, utilizando serviços criados ou modificados para este fim.
Bots	É um programa capaz de se propagar

	automaticamente, explorando vulnerabilidades existentes ou falhas na configuração de *softwares* instalados em um computador. Adicionalmente ao *worm*, dispõe de mecanismos de comunicação com o invasor, permitindo que o *bot* seja controlado remotamente.
Cavalos de Tróia	É um programa, normalmente recebido como um "presente" (por exemplo, cartão virtual, álbum de fotos, protetor de tela, jogo, etc), que além de executar funções para as quais foi aparentemente projetado, também executa outras funções normalmente maliciosas e sem o conhecimento do usuário.
Engenharia Social	Roubo de informações da empresa através de técnicas, contra o próprio pessoal da empresa.
Keylogger	*Keylogger* é um programa capaz de capturar e armazenar as teclas digitadas pelo usuário no teclado de um computador.
Rootkits	Mecanismos para esconder e assegurar a presença, do invasor, no computador comprometido.
Spyware	É o termo utilizado para se referir a uma grande categoria de *software* que tem o objetivo de monitorar atividades de um sistema e enviar as informações coletadas para terceiros.
Virus	Vírus é um programa ou parte de um programa de computador, normalmente malicioso, que se propaga infectando, isto é, inserindo cópias de si mesmo e se tornando parte de outros programas e arquivos de um computador
Worms	*Worm* é um programa capaz de se propagar automaticamente através de redes, enviando cópias de si mesmo de computador para computador.

FONTE: O Autor, baseado na cartilha de segurança para a internet 3.1 CERT.

De acordo com Ulbrich e Valle (2003), existem três tipos de falhas mais comuns que podem ser exploradas pelos *hacker*s, elas são a Perda de Disponibilidade, Perda de Confidencialidade e a Perda de Integridade que serão explanados nos tópicos a seguir:

2.3.1 Perda de Disponibilidade

Segundo Duarte (2012), a disponibilidade é conseguida quando certo serviço como, por exemplo, a energia elétrica, encontra-se protegido de uma interrupção indevida. O serviço tem disponibilidade quando ele sempre está

disponível ao usuário. Uma perda de disponibilidade afeta todos que contam com o serviço e é o que mais irrita o usuário, e pode ser citado vários exemplos onde a disponibilidade é uma preocupação como, por exemplo, a disponibilidade de informações de preços, a disponibilidade dos sistemas, da rede e da internet.

Ainda segundo Duarte (2012), algumas ameaças foram criadas para afetar a disponibilidade dos sistemas o ataque mais conhecido é o ataque de negação de serviço. Ataque de negação de serviços é aquele que consome recursos enviando falsas requisições para um servidor ou uma rede, congestionando o sistema e fazendo com que ele fique indisponível durante o ataque.

> "Perda de Disponibilidade: acontece quando a informação deixa de estar acessível por quem necessita dela. Seria o caso da perda de comunicação com um sistema importante para a empresa, que aconteceu com a queda de um servidor ou de uma aplicação crítica de negócio, que apresentou uma falha devido a um erro causado por motivo interno ou externo ao equipamento ou por ação não autorizada de pessoas com ou sem má intenção." (DUARTE, 2012, p. 9).

2.3.2 Perda de Confidencialidade

Segundo Duarte (2012), a confidencialidade é obtida quando existe a proteção do conteúdo, das mensagens e das estatísticas do tráfego, sem que elas sejam violadas. Apesar de não ser o item de maior importância para o consumidor, ele vem ganhando cada vez mais importância entre as organizações, pois o acesso indevido por pessoas não autorizadas as informações podem causar sérios problemas as estratégia organizacionais. A perda de confidencialidade é o que implica em mais consequências sobre as organizações.

Ainda segundo Duarte (2012), é importante notar que, apesar da perda de confidencialidade ser uma propriedade importante, nem sempre é necessária. Como no caso da confidencialidade dos preços, o qual é público, e dos comandos de controle, o qual não levanta ameaça alguma. A confidencialidade de algum software também não deve ser problema, já que a segurança do mesmo deve estar em chaves criptográficas.

Porém segundo Duarte (2012), caso haja a perda de confidencialidade alguns riscos podem acontecer, por exemplo, devido à quebra de privacidade das informações de consumo, ladrões poderiam usar estes dados sigilosos que foram obtidos para fazer um levantamento dos hábitos de uma determinada vítima e dessa maneira planejar um assalto.

Hackers poderiam obter as informações confidenciais de usuários de uma determinada companhia elétrica e de posse desses dados, poderiam vendê-los para terceiros. Sentindo-se penalizados, os usuários processariam a fornecedora, acarretando em perda de dinheiro e até mesmo mercado pela mesma.

> "Perda de Confidencialidade: seria quando há uma quebra de sigilo de uma determinada informação (ex: a senha de um usuário ou administrador de sistema) permitindo que sejam expostas informações restritas as quais seriam acessíveis apenas por um determinado grupo de usuários." (DUARTE, 2012, p. 7)

2.3.3 Perda de Integridade

Para Duarte (2012), a integridade, resumidamente, pode ser definida como o mantimento de uma informação protegida de mudanças exteriores não autorizadas. Se a integridade for corrompida os danos podem ser gravíssimos, pois é muito difícil detectar a mudança nas informações. A mudança é uma simples linha de código que pode alterar todo o resultado final do sistema. Como por exemplo, um algoritmo que determina que nota menores que 7 os alunos estão reprovados, a troca do sinal de menor para maior irá reprovar todos os alunos que tiraram mais que 7, e por muitas vezes esse erro só será notado depois que os dados já tiver sido lançado.

2.4 SEGURANÇA DE SISTEMAS DE INFORMAÇÃO

Segundo Laudon e Laudon (2004), o termo segurança abarca as politicas, procedimento e medidas técnicas usadas para impedir acesso não autorizado, alteração, roubo ou danos físicos a sistemas de informação. Ela pode se dar

por um conjunto de técnicas e ferramentas, destinadas a salvaguardar hardwares, softwares, redes de comunicação e dados.

O fator fundamental para uma melhor proteção dos ativos contidos nos sistemas de informação da organização é a segurança. Segundo a cartilha da CERT (2006), um computador (sistema computacional) pode ser dito como seguro se atender a 3 requisitos básicos, tabela 2.2, que são: confidencialidade, integridade e disponibilidade.

Tabela 2.2 – Pilares básicos de Segurança

Principio de Segurança	Explanação
Confidencialidade	A informação só está disponível para os usuários devidamente autorizados à acessá-las.
Integridade	A informação está intacta, sem nenhuma alteração não autorizada.
Disponibilidade	A informação está disponível para o usuário que seja autorizado a utilizá-la no momento em que se precisa.

Fonte: Cartilha do CERT(2006)

Enquanto que para Cruz (2010), tabela 3, a segurança tem 4 requisitos básicos que são: confidencialidade, autenticidade, integridade e disponibilidade.

Tabela 2.3 – Princípios de segurança

Princípios de Segurança	Envolve proteção de
Confidencialidade	Privacidade, Secretismo e Anonimato
Autenticidade	Certificação do dono da Informação e seus mandatários
Integridade	Alteração dos dados (incluindo origem) da informação
Disponibilidade	Utilização permanente da Informação

Fonte: Cruz (2010)

Alguns autores, assim como Cruz, utiliza os 4 princípios básicos enquanto que outros, assim como na cartilha do CERT utiliza 3 princípios básicos, incluindo dentro de integridade os conceitos de autenticidade, que alguns autores também chamam de confiabilidade.

Segundo a norma ISO/IEC TR 18044:2004, um evento de segurança da informação é a ocorrência identificada de um sistema, serviço ou rede que indica uma possível violação da política de segurança da informação ou falha de controles, ou uma situação previamente desconhecida, que possa ser relevante para a segurança da informação.

Segundo Bauer (2006), a segurança dos sistemas de informação pode ser dividida, e tratada, em duas grandes camadas: a da segurança física e a da informação, as quais serão tratadas nas próximas seções.

2.4.1 Segurança física

Segundo Bauer (2006), a segurança física visa impedir que pessoas não autorizadas tivessem o acesso às dependências, e proteger os equipamentos que tratam ou armazenam as informações, através de prevenções contra perdas, roubos ou vazamento de informações. Segundo Fontes (2004 apud Bauer, 2006), a segurança física tem como principais objetivos: garantir a continuidade das rotinas; assegurar a integridade dos ativos; manter a integridade e confidencialidade das informações.

Segundo Lemos (2001 apud Bauer, 2006), um ponto que normalmente é negligenciado por quem pensa em segurança é o acesso físico a terminais e outros dispositivos da rede. Obter e guardar cópias de backup seguras contra roubo, furto e danos, assim como os dispositivos (*notebook, palmtop, netbook e outros terminais portáteis*) também representa uma ameaça em caso de roubo ou acesso não autorizado. Deve-se ter cuidado com a segurança em relação aos dados armazenados nos discos rígidos e memórias desses terminais, além desses terminais deve se ter uma boa segurança sobre os armários de distribuição de cabos, servidores, roteadores e servidores de nome (DNS).

Ainda segundo Lemos (2001 apud Bauer, 2006), o acesso remoto, quer seja por um terminal estabelecido pela empresa ou um ponto de rede para conexão de equipamentos portáteis é algo que abre uma grande brecha para ataques, por permitir utilização de IPs falsos, rastreamento de pacotes, entre outras falhas de segurança. Caso seja necessário oferecer este serviço, deve ser algo inteiramente à parte da rede interna da organização. Além disso, deve se observar escritórios vazios e desconectá-los fisicamente do quadro de distribuição de cabos e monitorar todas as tentativas de conexão não autorizada.

A prevenção na segurança de acesso evita problemas de integridade ou até mesmo confidencialidade violada. “Um dos pontos fundamentais da

segurança física é o controle de acesso. Ele está baseado no fato de que nem todas as pessoas devem ou precisam ter acesso a todas as áreas da organização" (LOSS CONTROL, 2003, p.1).

2.4.2 Segurança da informação

O termo segurança da informação tem sido algo amplamente discutido no mundo, no Brasil em 2005 foi criado a ABNT NBR ISO/IEC 17799;2005 que segundo a ABNT é uma família de normas de sistemas de gestão de segurança da informação, e estas normas são equivalentes a ABNT NBR ISO/IEC 17799: 2005 .

Segundo a norma NBR ISO/IEC 17799: 2005, a segurança da informação trata da proteção da informação de vários tipos de ameaça para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio.

Para Silva e Stein (2007), a definição de segurança da informação pode ser sumarizada como a proteção contra o uso ou acesso não autorizado à informação, assim como a proteção contra a negação de serviços a usuários autorizados, enquanto a integridade e confidencialidade dessa informação são preservadas. Na ABNT NBR ISO/IEC 17799: 2005 (p. 1), tem-se que

"segurança da informação é a preservação da confidencialidade, da integridade e da disponibilidade da informação; adicionalmente, outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confiabilidade".

Enquanto a segurança da informação para Beal (2005), é o processo de proteção da informação das ameaças a sua integridade, disponibilidade e confidencialidade.

Sêmola (2003), aponta a segurança da informação como "uma área do conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade".

2.5 GESTÃO DA SEGURANÇA DA INFORMAÇÃO

Segundo Netto e Silveira (2007 apud Holanda, 2006) o comitê que trata da segurança da informação na ISO aprovou a criação de uma família de

normas sobre gestão da segurança da informação, batizada pela série 27000, onde a então ABNT NBR ISO IEC 17799: 2005 foi rebatizada por ABNT NBR ISO IEC 27002:2005.

A norma trás uma definição de 127 controles que compõem o escopo do Sistema de Gestão de Segurança da Informação que são agrupadas em 11 seções de controle: Política de Segurança da Informação; Organização da Segurança da Informação; Gestão de Ativos; Segurança em Recursos Humanos; Segurança Física e do Ambiente; Gestão das Operações e Comunicações; Controle de Acesso; Aquisição, Desenvolvimento e Manutenção dos Sistemas de Informação; Gestão de Incidentes da Segurança da Informação; Gestão da Continuidade do Negócio e Conformidade.

Segundo Borges, Parisi e Gil (2003), o controle e a segurança dos sistemas de informação devem ter o comprometimento de todas as pessoas envolvidas no processamento de dados. Caruso (2006), diz que para manter a proteção dos sistemas é necessário que medidas sejam tomadas, e os procedimentos e normas devem ser utilizados por todos que atuam nas organizações.

Laudon e Laudon (2004, apud Borges, Parisi e Gil, 2003), atribuem ao gerente de TI a adoção de metodologias adequadas à redução das contingências, dos riscos e ameaças às organizações, combinando medidas manuais e automatizadas que, juntas, corresponda ao efetivo controle.

Imoniana (2003), sugere que exista uma relação estreita entre as carreiras de TI e as carreiras de Finanças enquanto que Laudon e Laudon (2004), sugere também, que é necessário que exista uma ligação com o CEO, gerente da organização e o gerente de TI para uma melhor gestão de segurança da informação,

Assim sendo a controladoria, como unidade administrativa responsável pelo controle de sistemas de informações, apóia a gestão da TI na implementação de políticas e técnicas que venham a contribuir com a eficácia do sistema, e para que todos tenham um comprometimento sobre o que é necessário para manter a segurança da informação, sugere-se a criação de um documento de política de segurança da informação, onde segundo a ISO IEC 27002:2005 a política de segurança proverá uma orientação e apoio para a segurança da informação.

Segundo Caruso (2006), se todos na organização estiverem comprometidos com as normas de segurança, o resultado final será o ganho da organização em manter suas atividades e negócios bem sucedidos.

2.6 POLITICA DE SEGURANÇA DA INFORMAÇÃO

Segundo Menezes et. al. (2009 apud Fonseca, 2009), as políticas de segurança são instruções claras que fornecem as orientações de comportamento empregado para guardar as informações e é um elemento fundamental no desenvolvimento de controles efetivos para contra-atacar as possíveis ameaças à segurança.

Segundo o RFC 2196 (1997), uma política de segurança a ser implementada deve consistir num conjunto formal de regras que devem ser seguidas pelos usuários dos recursos da organização a ser implementada.

> "O principal objetivo da política de segurança é informar aos usuários, funcionários e gerentes de seus requisitos obrigatórios para a proteção da tecnologia e ativos de informação. A política deve especificar os mecanismos através dos quais esses requisitos podem ser cumpridos. Outro objetivo é fornecer uma base a partir da qual possam adquirir, configurar e auditar os sistemas e redes para o cumprimento da política. Portanto, uma tentativa de utilizar um conjunto de ferramentas de segurança na ausência de, pelo menos, uma política de segurança implícita não faz sentido." (RFC 2196, 1997, p.7).

As políticas de segurança da informação estão entre as mais significativas quando se diz respeito a evitar e detectar ataques contra a informação da empresa. O controle efetivo de segurança é implementado principalmente por meio de treinamento dos funcionários que vão desde os funcionários do mais baixo escalão até os de alto nível. Quanto maior o grau de importância das informações que o funcionário tem acesso, maior deve ser o investimento e cobrança sobre políticas de segurança para com o funcionário (FONSECA, 2009).

Para uma eficácia na adoção de uma boa política de segurança, a mesma deverá apresentar algumas características, conforme especifica a ABNT NBR ISO/IEC17799: 2005: (i) ser aprovada pela diretoria, divulgada e publicada de

forma ampla para todos os colaboradores; (ii) ser revisada regularmente, com garantia de que, em caso de alteração, ela seja revista; (iii) estar em conformidade com a legislação e cláusulas contratuais; (iv) deve definir as responsabilidades gerais e específicas; e (v) deve dispor as conseqüências das violações.

Para Martins e Santos (2005), além do que é especificado na norma ABNT NBR ISO/IEC17799: 2005 é necessário que a política de segurança abranja os seguintes tópicos:

- Propriedade da Informação – é interessante determinar o responsável pela informação, pessoa esta que poderá definir quem poderá ter acesso às informações e que nível de acesso é permitido, e qual a periodicidade necessária para a realização do backup desta informação;
- Classificação da informação – o gestor deverá classificar a informação quantos aos princípios de disponibilidade, confidencialidade e integridade;
- Controle de acesso – deve atender ao princípio de menor privilégio. Todo pedido de acesso deve ser documentado. Deve-se evitar a segregação de função, por exemplo, um mesmo usuário não deve ter acesso à geração de pagamento e liberação do mesmo. É importante, também, que se mantenham as trilhas de auditoria no sistema;
- Gerência de Usuários e Senhas – As senhas devem ser únicas e individuais, seguindo critérios de qualidade, isto é, senhas fortes com trocas periódicas. A responsabilidade da senha é do usuário proprietário da mesma;
- Segurança Física – Os acessos a áreas de servidores devem ser consentidos mediante autorização. Deve-se ter controle quanto à entrada e saída de equipamentos e pessoas, recomendando-se a criação de normatizações de controles internos referentes à segurança física, os quais deverão ser auditados periodicamente;

- Desenvolvimento de sistemas ou compra de sistemas/software – é importante definir uma sistemática interna com ênfase nos requisitos de segurança; e
- Plano de continuidade de Negócios – é um dos mais importantes tópicos na política de segurança, sendo recomendada a geração de controles e padrões especificando detalhes quanto ao plano de contingência e continuidade dos negócios.

Para Fonseca (2009), é essencial que a gerência de primeiro escalão adote e suporte com firmeza o desenvolvimento de políticas de segurança e de um programa de segurança das informações. Assim como qualquer outro método corporativo, para que um programa de segurança seja bem sucedido, a gerência deve fazer mais do que apenas apoiá-lo, deve demonstrar um comprometimento pessoal. Os empregados precisam ter consciência de que a gerência acredita que a segurança das informações é para a operação da empresa, que a proteção das informações comerciais da empresa é essencial para que ela continue funcionando e de que o trabalho de cada empregado pode depender do sucesso do programa.

3. METODOLOGIA DA PESQUISA

Para cada pesquisa cientifica são utilizados conhecimentos, métodos, técnicas e outros procedimentos científicos com objetivo de encontrar soluções para os problemas propostos. Desta maneira, serão apresentados neste capítulo, os métodos escolhidos para a obtenção das respostas a pergunta problema definida nesta pesquisa.

3.1 NATUREZA DA PESQUISA

A pesquisa pode ser classificada em diferentes aspectos: quanto aos fins, quanto aos meios e quanto à forma de abordagem.

3.1.1 Quanto aos fins

A pesquisa é dita descritiva, pois segundo este tipo de pesquisa é adotado “como objetivo primordial as descrições das características de uma determinada população ou de determinado fenômeno” (GIL, 1999, p.46).

Pode também estabelecer correlações entre variáveis e define sua natureza, não tendo o compromisso de explicar os fenômenos que descreve, embora sirva de base para tal explicação.

3.1.2 Quanto aos meios

A pesquisa pode ser caracterizada por: Pesquisa bibliográfica e Pesquisa de opinião. Segundo Cervo, Bervian e Silva (2007), uma pesquisa de opinião procura saber os pontos de vista das pessoas acerca de algum assunto. A pesquisa de opinião abrange uma faixa muito grande de investigação que visa a identificar falhas ou erros.

3.1.3 Quanto à forma de abordagem

Caracteriza-se como pesquisa quantitativa, pois “as pesquisas quantitativas consideram que tudo pode ser quantificável, o que significa

traduzir em números opiniões e informações para classificá-las e analisá-las" (MORESI, 2004 p.57).

Segundo Malhotra (2001, p.155), "a pesquisa quantitativa procura quantificar os dados e aplicar alguma forma de análise estatística".

A razão para se conduzir uma pesquisa quantitativa é descobrir quantas pessoas de uma determinada população compartilham uma característica ou um grupo de características (LAKATOS, 1991).

Esta forma de abordagem se aplica aos objetivos desta pesquisa, pelo fato de privilegiar o significado das informações coletadas (BOA VENTURA, 2004).

3.1.4 Definição da Amostra

De acordo com Gil (1999), o universo ou população é um grupo de elementos que possuem determinadas características e a amostra é considerada como uma parcela do universo ou da população, por meio do qual se estabelecem ou estimam as características desse universo ou população. Segundo o mesmo, quando um pesquisador seleciona uma pequena parte de uma população, espera-se que ela seja representativa dessa população que pretende estudar.

O universo deste estudo é representado pelos 653 alunos do curso de Administração da Universidade Federal de Pernambuco – Campus Acadêmico do Agreste, matriculados no período de 2013.2. A amostra representa 27,5% dos alunos do universo, um total de 180. Essa amostra foi escolhida por conseguir representar um grupo heterogêneo, diversificado, e forte.

A aplicação se procedeu por contato direto do pesquisador com os alunos respondentes, dos 180 questionários 50 não foram contabilizados, por não terem sido devolvidos.

3.1.5 Definição do instrumento de coleta de dados

Geralmente a coleta de dados se inicia após definição de tema, objetivos, formulação do problema, entre outros. Nesta fase, procura-se estabelecer uma técnica para ser aplicada à pesquisa. Cervo e Bervian (1996), definem

questionário como sendo a técnica de coleta de dados mais utilizada. Almeja-se com o uso desta técnica obter repostas sobre determinado assunto. Ainda Cervo e Bervia (1996), completam ao afirmar que todo questionário deve ser impessoal, para assegurar a uniformidade na avaliação de uma situação. Desta maneira, o respondente fornece informações de seu domínio e conhecimento, sem que seja necessária a presença do pesquisador.

A escolha da aplicação de questionário, como umas das técnicas de avaliação da percepção dos estudantes deve-se ao fato de possuir alta média de confiabilidade já estabelecida (Dias, 2003).

Para averiguar possíveis falhas no questionário ou mesmo dúvidas oriundas de seu preenchimento e para fins de orientação quanto à tabulação posterior foi realizado um pré-teste, com um grupo de 24 alunos, como o pré-teste foi realizado com sucesso o resultado dos 24 alunos foi utilizado no resultado final.

Para tal, o questionário serviu para atingir os objetivos desta pesquisa, coletando opiniões acerca do tema e verificando a percepção dos estudantes de administração acerca do tema política de segurança. A partir do momento que os estudantes disponibilizam suas percepções através das informações referentes às políticas de segurança, permite-se avaliar essas informações definindo resultados probabilísticos.

O questionário é baseado na escala de Likert, permitindo que os usuários indiquem o grau de concordância, indecisão e discordância com relação às informações dadas, sendo 16 dessas questões usando a escala. O formato usado para esta pesquisa compreende por: 1) Discordo Fortemente, 2) Discordo, 3) Indiferente (Nem concordo nem discordo), 4)Concordo, e 5) Concordo Fortemente.

As perguntas contidas no questionário foram feitas pelo próprio autor, utilizando afirmativas sobre políticas de segurança da informação.

O software utilizado para a construção dos gráficos e dos percentuais da pesquisa foi o Microsoft Excel 2010.

4. APURAÇÃO E ANÁLISE DOS DADOS

Dos 180 questionários, 130 foram entregues devidamente respondidos, sendo que 02 deles foram descartados por ter tido algum erro no preenchimento. Nos próximos tópicos mostraremos o quantitativo, e a análise dos dados de cada questão.

4.1 APURAÇÃO DOS DADOS

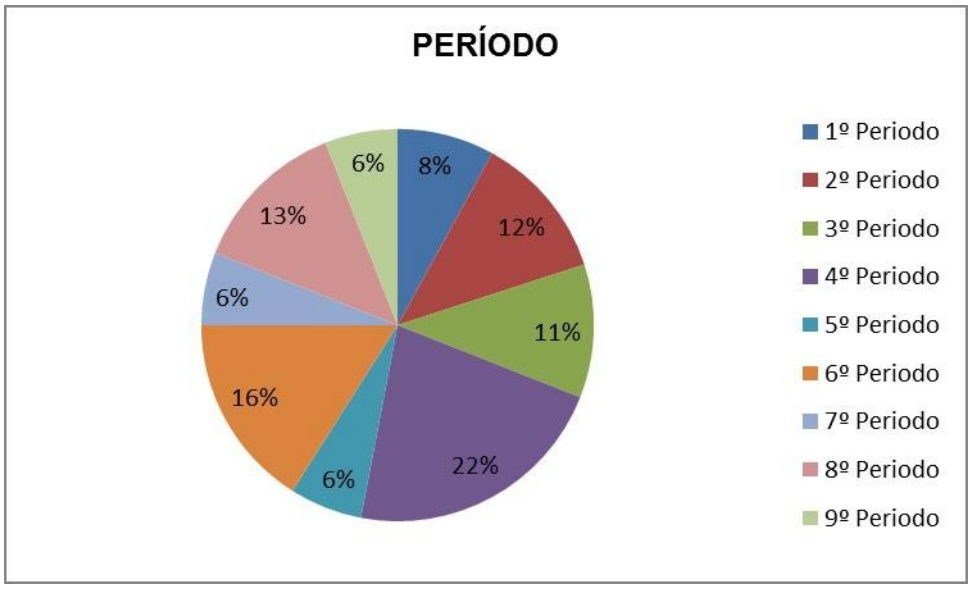
Os próximos subtópicos vão apresentar a apuração dos dados coletados pelo questionário, pelas partes definidas no questionário.

4.1.1 Parte I

Para esta primeira parte é evidenciado que os dados pessoais e profissionais dos respondentes, tais como período na universidade e se já possui vinculo empregatício na área de gestão.

Na primeira pergunta, pôde-se determinar o período que o estudante cursa na Universidade. A maioria dos estudantes está no meio do curso, mas houve uma heterogeneidade da amostra. Como mostra o gráfico 01.

Gráfico 01 - Período onde o estudante estuda.



Fonte: Dados da Pesquisa.

Na segunda pergunta, pode-se determinar quantos dos respondentes trabalham na área de gestão. A maioria dos estudantes (61%), como mostra o gráfico 02, responderam que já trabalham na área de gestão.

Gráfico 02 - Você possui Vinculo empregatício, ou estagiário, na área de gestão?

FONTE: Dados da pesquisa

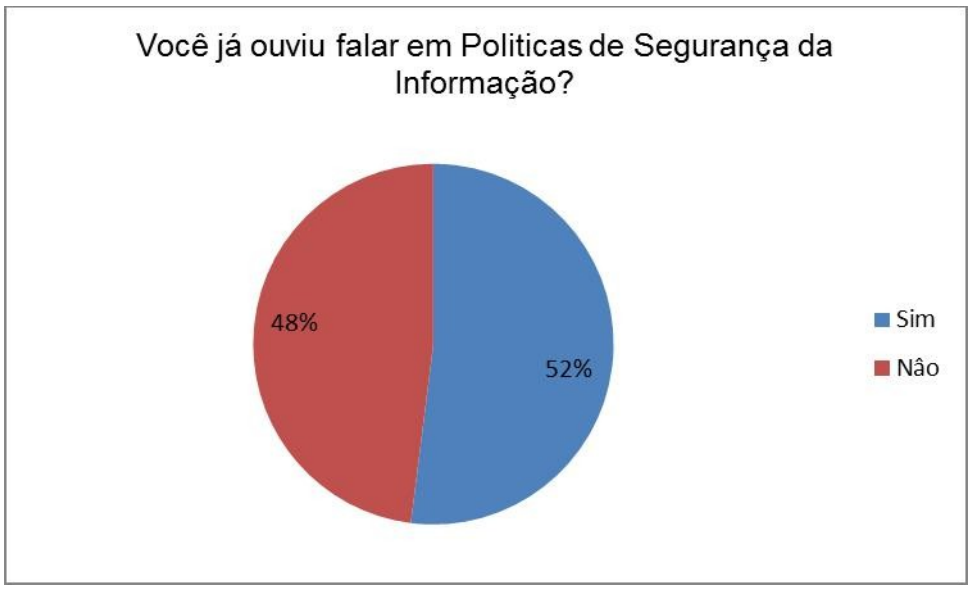
4.1.2 Parte II

Na parte II, são evidenciados questionamentos referentes ao contato que os estudantes já tiveram com Políticas de Segurança da Informação.

A primeira questão, foi: “Você já ouviu falar no assunto Política de Segurança da Informação? ”.

O resultado desta pergunta, gráfico 03, foi equilibrado. Onde 62 estudantes de administração, o que representa 48% dos entrevistados, respoderam que nunca ouvirm falar em Política de Segurança da Informação, enquanto que 66 estudantes de administração, o que representa 52% dos entrevistados, responderam que já ouviram falar em Política de Segurança da Informação.

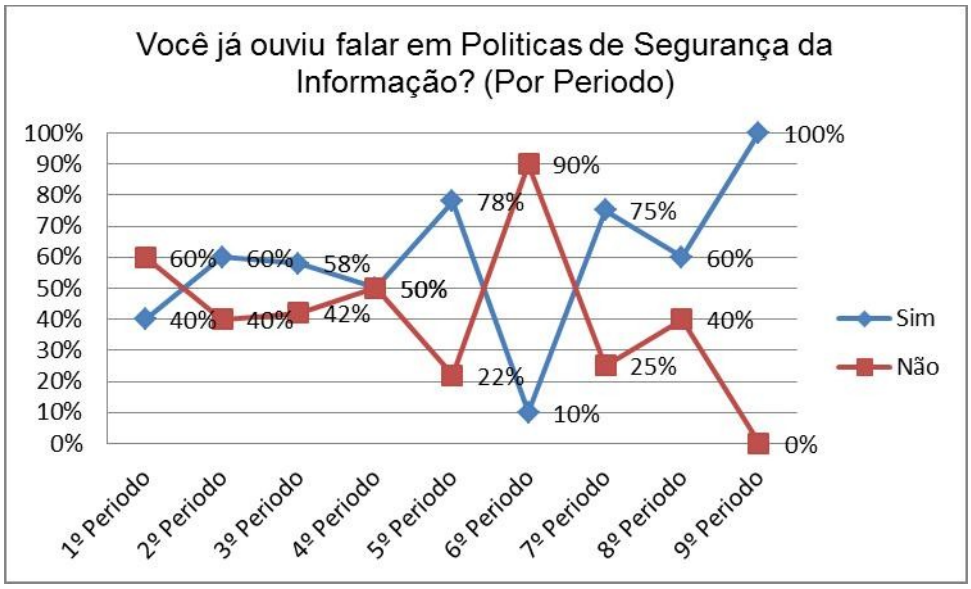
Gráfico 03 - você já ouviu falar em políticas de segurança da informação?



FONTE: Dados da Pesquisa.

Na análise dos dados por períodos, nota-se que a partir do 6º período há um grande aumento percentual entre os estudantes que já ouviram falar no assunto Política de Segurança da Informação chegando a 100% dos entrevistados do 9º periodo já terem ouvidor falar no tema, Gráfico 04.

Gráfico 04 - você já ouviu falar em políticas de segurança da informação? por períodos.



FONTE: Dados Da pesquisa

Para os que trabalham na área de gestão, foi uma segunda pergunta que questionou: “Na empresa que você trabalha existe um documento de Políticas de Segurança da Informação?”.

O resultado desta pergunta, gráfico 05, foi que 50% dos entrevistados desconhecem a existência de um documento de Política de Segurança da Informação na empresa para o qual ele trabalha, 25% dos entrevistados afirmam conhecer o documento de Políticas de Segurança da Informação, e os outros 25% afirmam que não existe o documento de Políticas de Segurança da Informação na empresa que eles trabalham.

Gráfico 05 - Na empresa que você trabalha existe um documento de Políticas de Segurança da Informação?

FONTE: Dados da Pesquisa

4.1.3 Parte III

A parte III do questionário, são evidenciados questionamentos sobre a percepção dos estudantes acerca do tema políticas de segurança da informação e sobre boas práticas em segurança da informação.

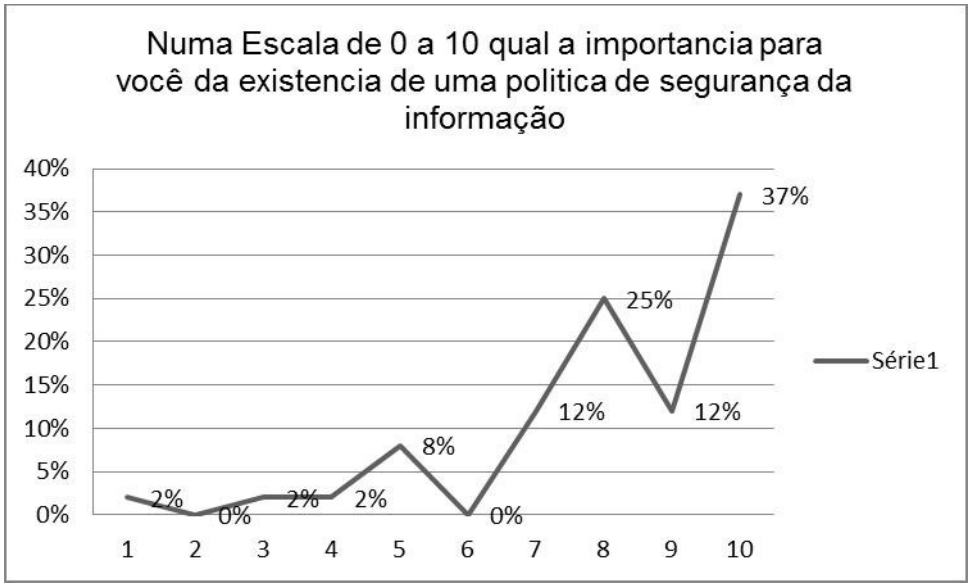
A primeira questão foi: “Numa escala de 0 a 10, qual a importância, para você, da existência de uma política de Segurança da Informação?”.

O resultado desta pergunta, gráfico 06, foi que ninguém respondeu zero, 2% responderam um, 0% respondeu dois, 2% responderam três, 2%

responderam quatro, 9% responderam cinco, 0% respondeu seis, 14% responderam sete, 27% responderam oito, 14% responderam nove, 41% responderam dez.

A segunda questão foi: “Conhecer sistemas de informação é essencial para os administradores”

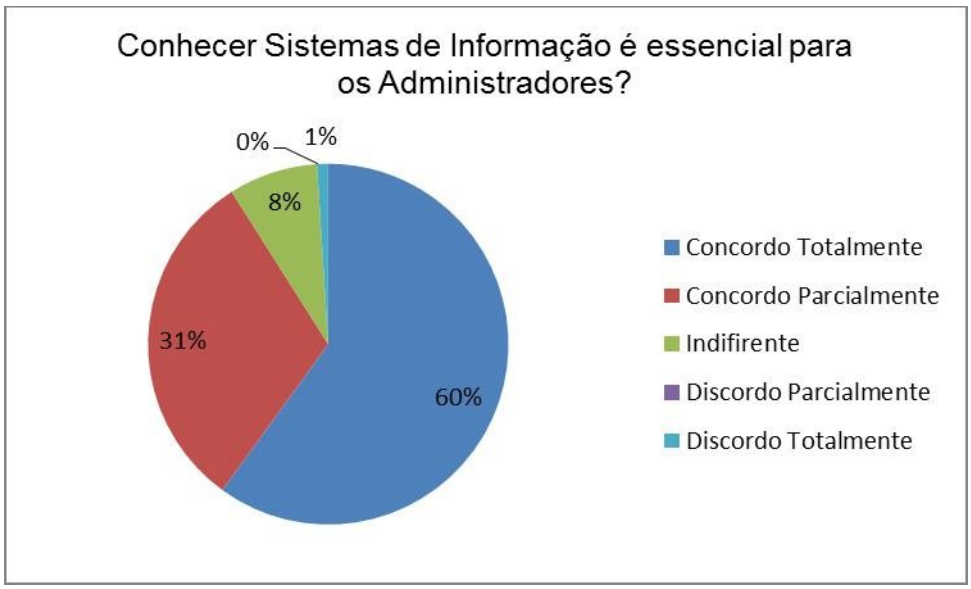
Gráfico 06 - Numa escala de 0 a 10, qual a importância, para você, da existência de uma política de Segurança da Informação?



Fonte: Dados da Pesquisa

O resultado desta pergunta, gráfico 07, foi que 60% dos estudantes de administração concordam totalmente (CT) com a afirmativa, 31% concordam parcialmente (CP), 8% são indiferentes (ID), 0% discordou parcialmente (DP), 1% discorda totalmente (DT).

Gráfico 07 - Conhecer sistemas de informação é essencial para os administradores

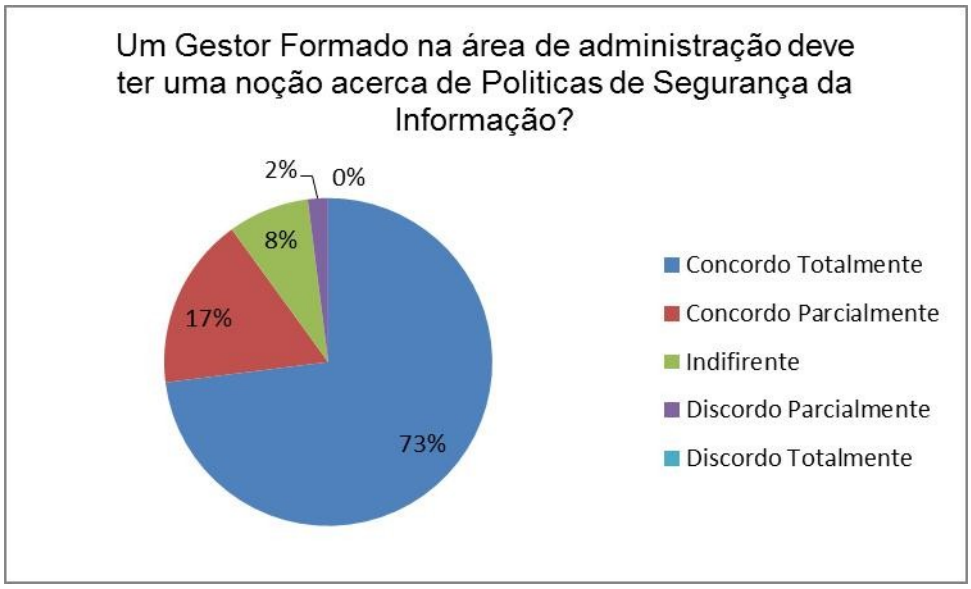


Fonte: Dados da pesquisa.

A 3ª Questão foi: “Um gestor, formado na área de administração, deve ter uma noção acerca do tema Políticas de Segurança da Informação?”.

O resultado desta pergunta, gráfico 08, foi que 73% dos estudantes de administração concordam totalmente (CT) com a afirmativa, 17% concordam parcialmente (CP), 8% são indiferentes (ID), 2% discordam parcialmente (DP), 0% discorda totalmente (DT).

Gráfico 08 - Um gestor, formado na área de administração, deve ter uma noção, mesmo que básica, acerca do tema Políticas de Segurança da Informação.



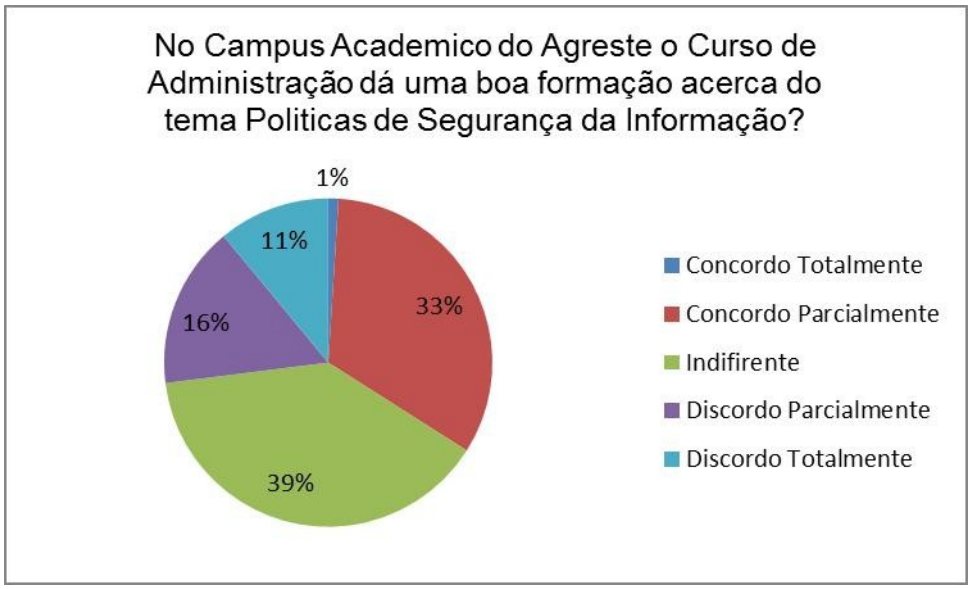
Fonte: Dados da pesquisa.

A 4ª Questão foi: “No Campus Acadêmico do Agreste o curso de Administração dá uma boa formação acerca do tema Políticas de Segurança da informação?”.

O resultado desta pergunta, gráfico 09, foi que 1% dos estudantes de administração concorda totalmente (CT) com a afirmativa, 33% concordam parcialmente (CP), 39% são indiferentes (ID), 16% discordam parcialmente (DP), 11% discordam totalmente (DT).

A 5ª Questão foi: “Obedecer a uma política de segurança da informação é uma cultura boa para a organização?”.

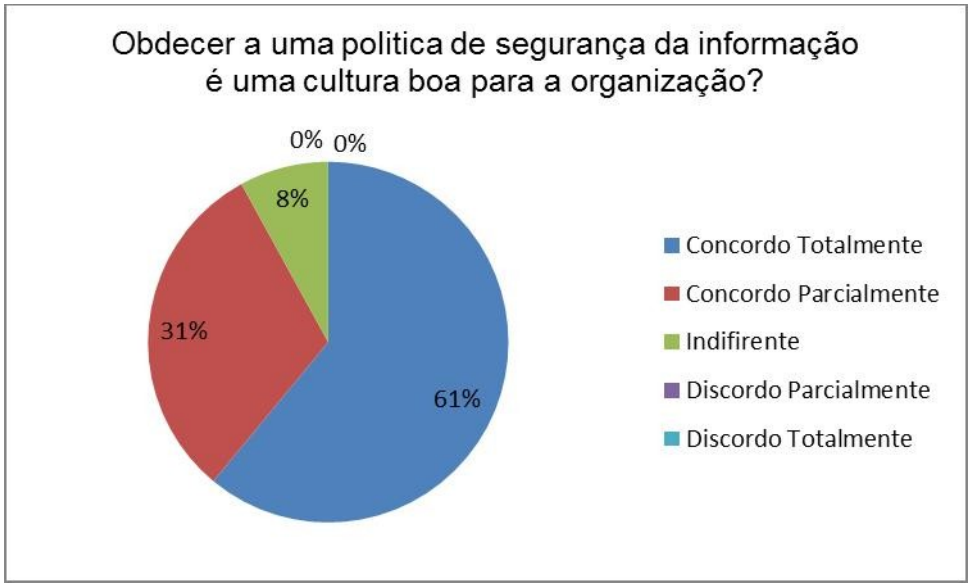
Gráfico 09 - No Campus Acadêmico do Agreste o curso de Administração dá uma boa formação acerca do tema Políticas de Segurança da informação.



Fonte: Dados da pesquisa.

O resultado desta pergunta, gráfico 10, foi que 61% dos estudantes de administração concordam totalmente (CT) com a afirmativa, 31% concordam parcialmente (CP), 8% são indiferentes (ID), 0% discordam parcialmente (DP), 0% discorda totalmente (DT).

Gráfico 10 - Obedecer a uma política de segurança da informação é uma cultura boa para a organização.

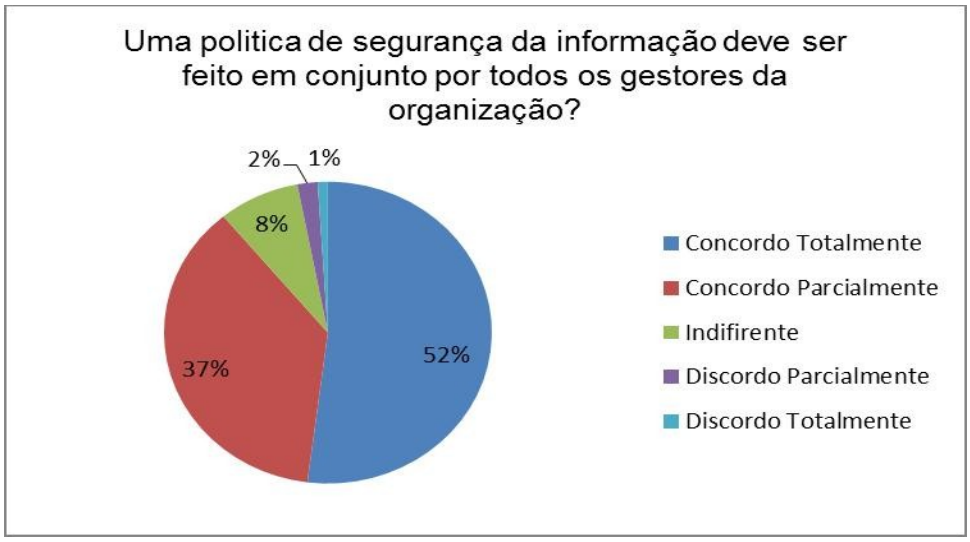


Fonte: Dados da pesquisa.

A 6ª Questão foi: “Uma Política de Segurança da Informação deve ser feita em conjunto, por todos os gestores da organização?”.

O resultado desta pergunta, gráfico 11, foi que 52% dos estudantes de administração concordam totalmente (CT) com a afirmativa, 37% concordam parcialmente (CP), 8% são indiferentes (ID), 2% discordam parcialmente (DP), 1% discorda totalmente (DT).

Gráfico 11 - Uma Política de Segurança da Informação deve ser feita em conjunto, por todos os gestores da organização.



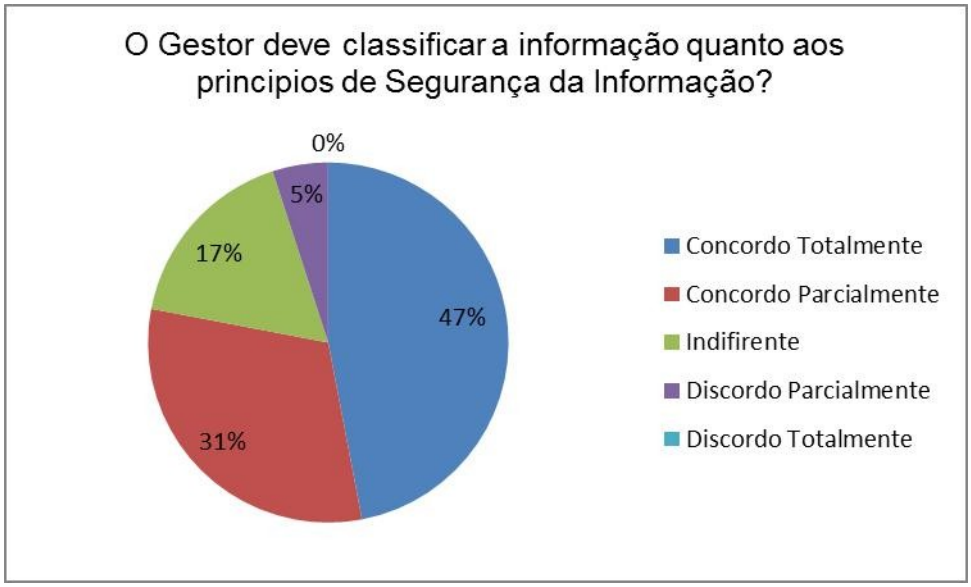
Fonte: Dados da pesquisa.

A 7ª Questão foi: “O gestor deve classificar a informação quanto aos princípios de disponibilidade, confidencialidade e integridade?”.

O resultado desta pergunta, gráfico 12, foi que 47% dos estudantes de administração concordam totalmente (CT) com a afirmativa, 31% concordam parcialmente (CP), 17% são indiferentes (ID), 5% discordam parcialmente (DP), 0% discorda totalmente (DT).

A 8ª Questão foi: “As senhas devem ser únicas e individuais, seguindo critérios de qualidade, isto é, senhas fortes com trocas periódicas?”.

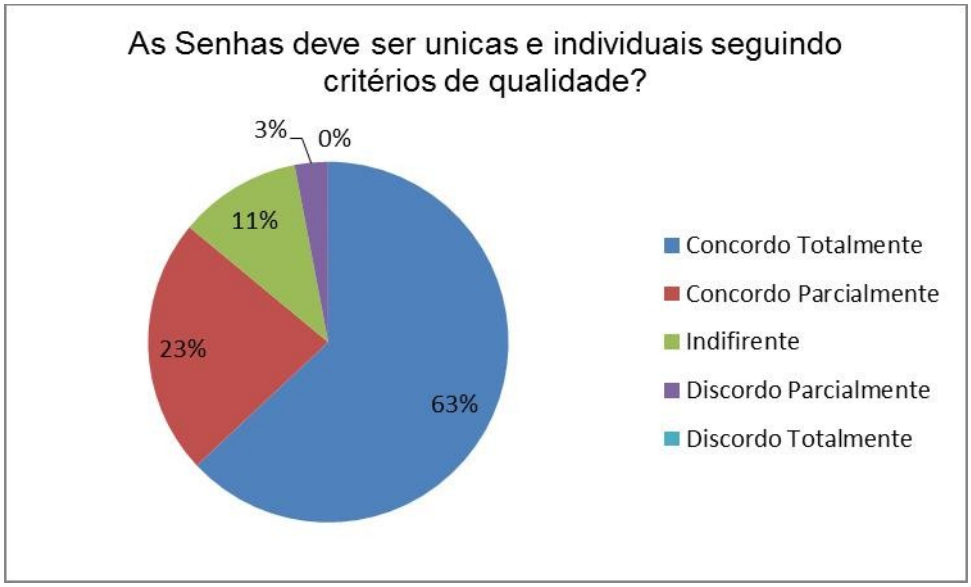
Gráfico 12 - O gestor deve Classificar a informação quanto aos princípios de disponibilidade, confidencialidade e integridade



Fonte: Dados da pesquisa.

O resultado desta pergunta, gráfico 13, foi que 63% dos estudantes de administração concordam totalmente (CT) com a afirmativa, 23% concordam parcialmente (CP), 11% são indiferentes (ID), 3% discordam parcialmente (DP), 0% discorda totalmente (DT).

Gráfico 13 - As senhas devem ser únicas e individuais, seguindo critérios de qualidade, isto é, senhas fortes com trocas periódicas



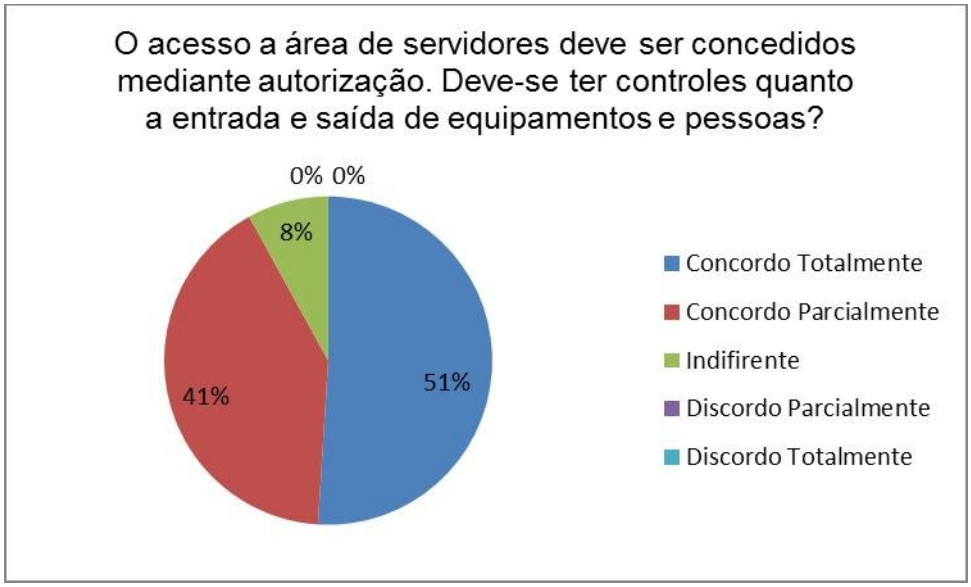
Fonte: Dados da pesquisa.

A 9ª Questão foi: “O acesso a áreas de servidores deve ser concedido mediante autorização. Deve-se ter controle quanto à entrada e saída de equipamentos e pessoas?”.

O resultado desta pergunta, gráfico 14, foi que 51% dos estudantes de administração concordam totalmente (CT) com a afirmativa, 41% concordam parcialmente (CP), 8% são indiferentes (ID), 0% discorda parcialmente (DP), 0% discorda totalmente (DT).

Nota-se que 92% dos estudantes concordam que os acessos a áreas de servidores devem ser consentidos mediante autorização. Deve-se ter controle quanto à entrada e saída de equipamentos e pessoas.

Gráfico 14 - O acesso a áreas de servidores devem ser concedido mediante autorização. Deve-se ter controle quanto à entrada e saída de equipamentos e pessoas.

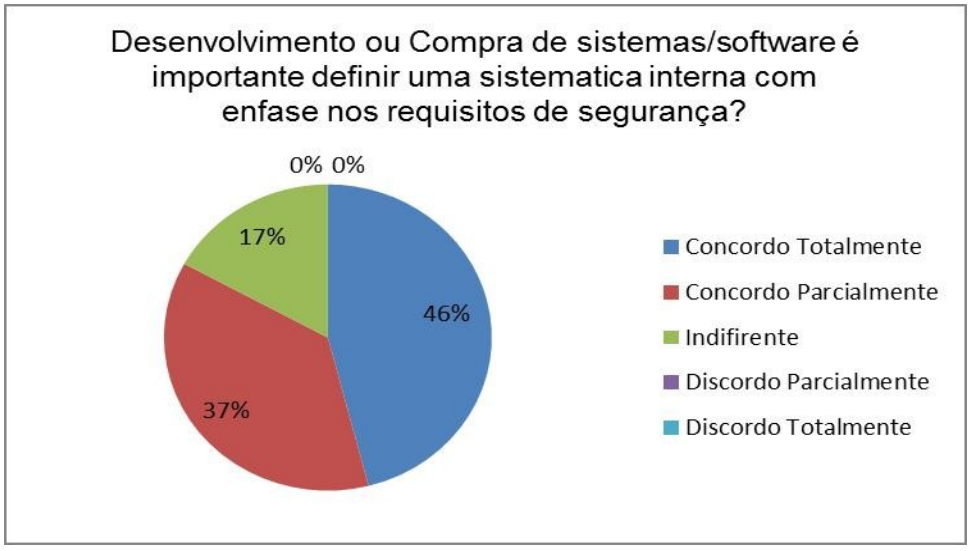


Fonte: Dados da pesquisa.

A 10ª Questão foi: “Desenvolvimento de Sistemas ou compra de Sistemas/software – é importante definir uma sistemática interna com ênfase nos requisitos de segurança?”.

O resultado desta pergunta, gráfico 15, foi que 46% dos estudantes de administração concordam totalmente (CT) com a afirmativa, 37% concordam parcialmente (CP), 17% são indiferentes (ID), 0% discorda parcialmente (DP), 0% discorda totalmente (DT).

Gráfico 15 - Desenvolvimento de Sistemas ou compra de Sistemas/software – é importante definir uma sistemática interna com ênfase nos requisitos de segurança.

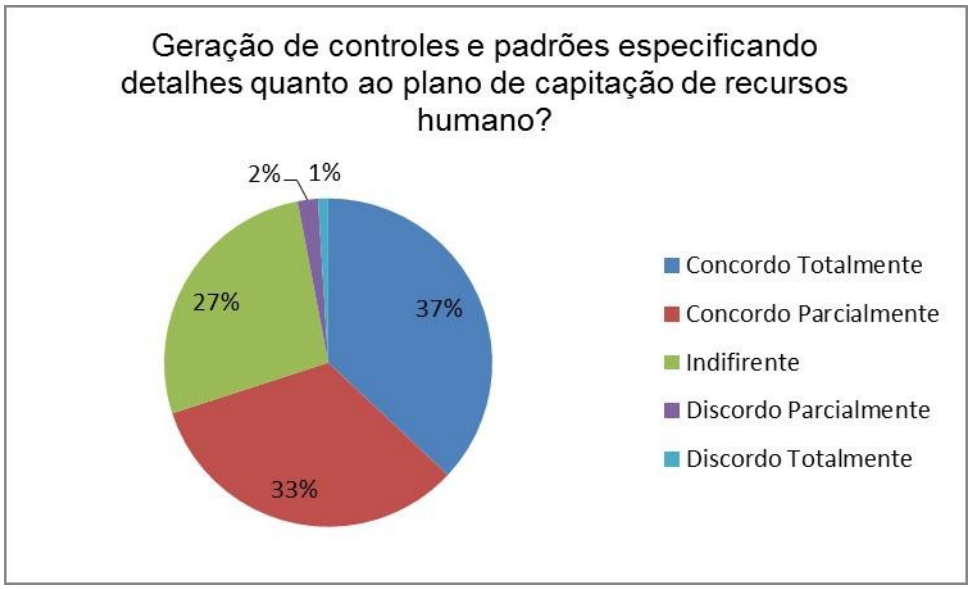


Fonte: Dados da pesquisa.

A 11ª Questão foi: “Geração de controles e padrões especificando detalhes quanto ao plano de captação de recursos humanos?”.

O resultado desta pergunta, gráfico 16, foi que 37% dos estudantes de administração concordam totalmente (CT) com a afirmativa, 33% concordam parcialmente (CP), 27% são indiferentes (ID), 2% discorda parcialmente (DP), 1% discorda totalmente (DT).

Gráfico 16, Geração de controles e padrões especificando detalhes quanto ao plano de captação de recursos humanos.

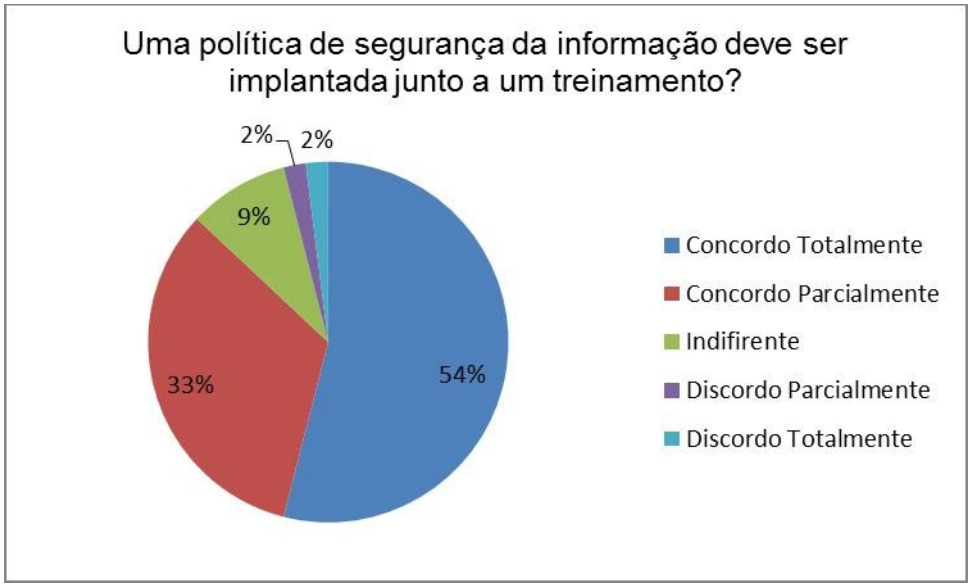


FONTE: Dados da pesquisa.

A 12ª Questão foi: “Uma política de segurança da informação deve ser implantada junto a um treinamento?”.

O resultado desta pergunta, gráfico 17, foi que 54% dos estudantes do curso de administração concordam totalmente (CT) com a afirmativa, 33% concordam parcialmente (CP), 9% são indiferentes (ID), 2% discordam parcialmente (DP), 2% discordam totalmente (DT).

Gráfico 17 - Uma política de segurança da informação deve ser implantada junto a um treinamento.

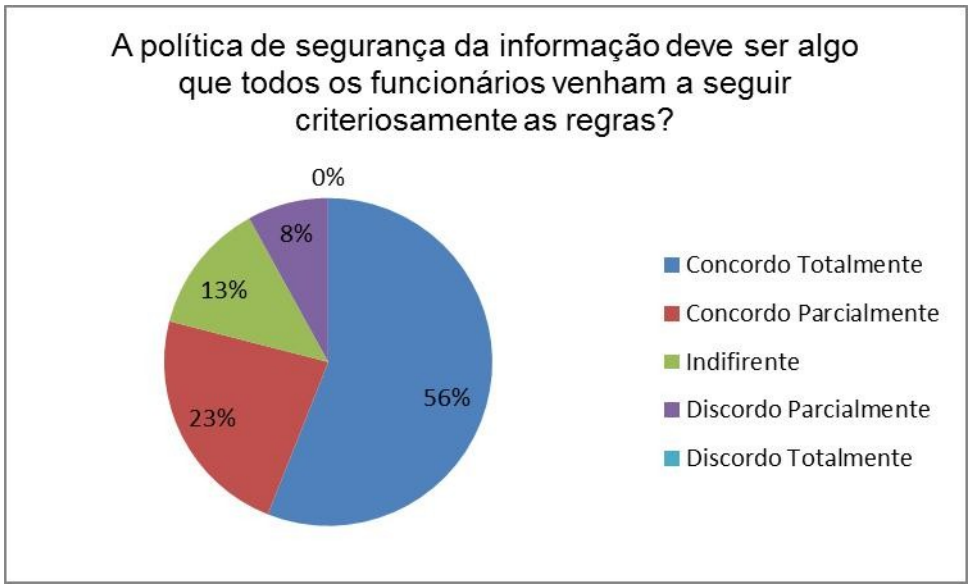


Fonte: Dados da pesquisa.

A 13ª Questão foi: “A política de segurança da informação deve ser algo que todos os funcionários venham a seguir criteriosamente as regras?”.

O resultado desta pergunta, gráfico 18, foi que 56% dos estudantes de administração concordam totalmente (CT) com a afirmativa, 23% concordam parcialmente (CP), 13% são indiferentes (ID), 8% discordam parcialmente (DP), 0% discorda totalmente (DT).

Gráfico 18 - A política de segurança da informação deve ser algo que todos os funcionários venham a seguir criteriosamente as regras.

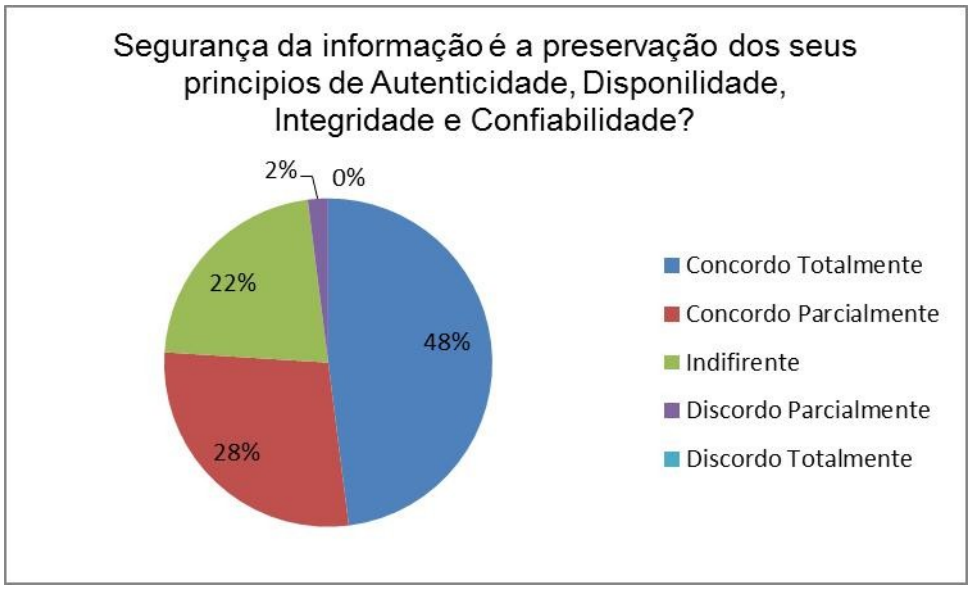


Fonte: Dados da pesquisa.

A 14ª Questão foi: “Segurança da informação é a preservação da confidencialidade, da integridade e da disponibilidade da informação; adicionalmente, outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confiabilidade?”.

O resultado desta pergunta, gráfico 19, foi que 48% dos estudantes de administração concordam totalmente (CT) com a afirmativa, 28% concordam parcialmente (CP), 22% são indiferentes (ID), 2% discordam parcialmente (DP), 0% discordam totalmente (DT).

Gráfico 19 - Segurança da informação é a preservação da confidencialidade, da integridade e da disponibilidade da informação; adicionalmente, outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confiabilidade.



Fonte: Dados da pesquisa.

A 15ª Questão foi: “Anotar senhas em algum lugar é uma boa ideia para não esquecê-las?”.

O resultado desta pergunta, gráfico 20, foi que 5% dos estudantes de administração concordam totalmente (CT) com a afirmativa, 12% concordam parcialmente (CP), 12% são indiferentes (ID), 36% discordam parcialmente (DP), 35% discordam totalmente (DT).

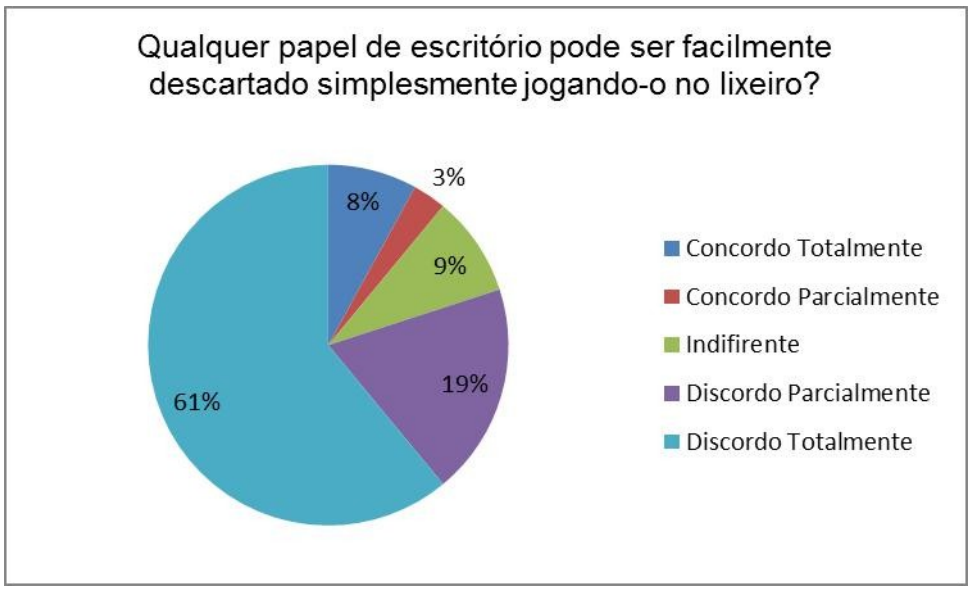
Gráfico 20 - Anotar senhas em algum lugar é uma boa idéia para não esquecê-las.

Fonte: Dados da pesquisa.

A 16ª Questão foi: “Qualquer papel de escritório pode ser facilmente descartado, simplesmente jogando-o no lixeiro?”.

O resultado desta pergunta, gráfico 21, foi que 8% dos estudantes de administração concordam totalmente (CT) com a afirmativa, 3% concordam parcialmente (CP), 9% são indiferentes (ID), 19% discordam parcialmente (DP), 61% discordam totalmente (DT).

Gráfico 21, Qualquer papel de escritório pode ser facilmente descartado, simplesmente jogando-o no lixeiro.



A 17ª Questão foi: “Costumo utilizar termos fáceis para as minhas senhas (ex. Data de Nascimento, nomes, número de celular e etc.)?”.

O resultado desta pergunta, gráfico 22, foi que 5% dos estudantes de administração concordam totalmente (CT) com a afirmativa, 11% concordam parcialmente (CP), 20% são indiferentes (ID), 23% discordam parcialmente (DP), 41% discordam totalmente (DT).

Gráfico 22 - Costumo utilizar termos fáceis para as minhas senhas (ex. Data de Nascimento, nomes, número de celular e etc.).

Fonte: Dados da pesquisa.

4.2 Análise dos dados

Após a apuração dos dados, pode-se analisar que:

- 91% dos estudantes concordam que conhecer sistemas de informação é algo essencial para os administradores;
- Ao se tratar da importância de uma Política de Segurança da Informação os estudantes deram uma média geral de 9,03, em uma escala de 0 a 10, de nível de importância para o tema;

- 90% dos estudantes concordam que os gestores, formados em administração, devem ter uma noção, mesmo que básica acerca do tema Políticas de Segurança da Informação;
- A maioria dos estudantes são indiferentes quanto à formação recebida, no CAA, acerca do tema Políticas de Segurança da Informação;
- 92% dos estudantes concordam que obedecer a uma política de segurança da informação é uma cultura boa para a organização.
- 89% dos estudantes concordam que uma Política de Segurança da Informação deve ser feita em conjunto, por todos os gestores da organização;
- 78% dos estudantes concordam que o gestor deve classificar a informação quanto aos princípios de disponibilidade, confidencialidade e integridade;
- 86% dos estudantes concordam que as senhas devem ser únicas e individuais, seguindo critérios de qualidade, isto é, senhas fortes com trocas periódicas;
- 83% dos estudantes concordam que no desenvolvimento de sistemas ou compra de sistemas/software – é importante definir uma sistemática interna com ênfase nos requisitos de segurança;
- 70% dos estudantes concordam que geração de controles e padrões especificando detalhes quanto ao plano de captação de recursos humanos;
- 87% dos estudantes concordam que uma política de segurança da informação deve ser implantada junto a um treinamento;
- 79% dos estudantes concordam que conhecer A política de segurança da informação deve ser algo que todos os funcionários venham a seguir criteriosamente as regras;
- 76% dos estudantes concordam que segurança da informação é a preservação da confidencialidade, da integridade e da disponibilidade da informação; adicionalmente, outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confiabilidade;

- 71% dos estudantes discordam que anotar senhas em algum lugar é uma boa ideia para não esquecê-las;
- 80% dos estudantes discordam que qualquer papel de escritório pode ser facilmente descartado, simplesmente jogando-o no lixeiro;
- 64% dos estudantes discordam que costumam utilizar termos fáceis para as minhas senhas (ex. Data de Nascimento, nomes, número de celular e etc.).

5 CONSIDERAÇÕES FINAIS

5.1 CONCLUSÃO

No que tange a identificação das práticas dos estudantes, relativas às políticas de segurança da informação, pode-se notar que os estudantes do curso de administração da Universidade de Pernambuco realizam muitas práticas de políticas de segurança da informação. Grande parte dos estudantes realiza troca de senhas periódicas, utilizam senhas fortes e restringem o acesso dos seus computadores com senhas. Em relação às falhas comuns na política de segurança da informação pessoal dos estudantes, pode-se observar que muitas destas práticas deixam de ser feitas por indolência dos estudantes, a maioria dos estudantes alegaram que salvam as senhas no browser de seus computadores pessoais, para economizar tempo e trabalho.

Pertinente ao preparo dos estudantes de administração para o tema "políticas de segurança da informação", nota-se que um grande número de estudantes ainda não ouviu falar sobre o assunto, e uma grande parte é indiferente quanto ao aprendizado que eles obtiveram na universidade acerca de Políticas de Segurança da Informação. Entretanto, mesmo com grande parte dos estudantes desconhecendo o tema, ou não tendo conhecimento suficiente para falar sobre ele, avaliaram a política de segurança como algo de grande importância para as organizações. As noções de políticas de segurança da informação dos estudantes são consideradas boas, porém, por insuficiência de embasamento teórico, falta segurança para os estudantes no momento em que vão expor seu pensamento acerca das políticas de segurança da informação.

Após alcançar os objetivos específicos, chega-se à conclusão da pergunta de pesquisa. Os estudantes de administração não obtêm um bom conhecimento teórico acerca do tema de Políticas de Segurança da Informação, porém com algumas das práticas realizadas pelos estudantes pôde-se concluir que os estudantes embora tenham um fraco embasamento teórico, e em grande parte desconhece a existência do tema, com a prática e o dia a dia acabaram adquirindo algumas práticas de políticas de segurança, mas

por muitas vezes sem ter a percepção que estão utilizando técnicas de segurança da informação.

5.2 Limitações

Esta pesquisa transcorreu com algumas limitações em seu desenvolvimento, uma delas é o tempo para a realização do trabalho e a continuidade com as outras obrigações acadêmicas e profissionais. Outra limitação a dependência de esperar a devolução dos questionários devidamente respondidos.

6 REFERÊNCIAS

ABNT NBR ISO/IEC 17799:2005 [Acesso em: 11 de Junho de 2014]. Disponível em: http://www.scribd.com/doc/2449992/Abnt-Nbr-Isoiec-17799-Tecnologia-da-Informacao-Tecnicas-de-Seguranca-Codigo-de-Pratica-para-a-Gestao-da-Seguranca-da-Informacao

ABNT NBR ISO/IEC 27002:2005 [Acesso 09 de julho de 2014]**.**Disponível em: http://www.ima.sp.gov.br/politica-de-seguranca-da-informacao

BOA VENTURA, Edivaldo M. **Metodologia Científica**. São Paulo: Atlas, 2004.

BAUER, Adriano Cesar. **Política de segurança da informação para redes corporativas**, 2006.

BEAL, Adriana. **Segurança da Informação: princípios e melhores práticas para a proteção dos ativos de informação nas organizações** - São Paulo: Atlas, 2005.

BORGES, N.T.; Parisi, C. Gil, L. de A.; **O Controller como Gestor da Tecnologia da Informação – Realidade ou Ficção?.** 2003.

CARUSO, Carlos A. A.; STEFFEN, Flávio Deny. *Segurança em informática e de Informações*. São Paulo: SENAC/SP, 2006.

CERT - Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil, 2006 [acesso em 10 de outubro de 2013]. Disponível em: http://www.cert.br/

CERVO, Amado Luiz; BERVIAN, Pedro Alcino. **Metodologia Científica**. São Paulo: Makros Books, 1996.

CERVO, Amado Luis; BERVIAN, Pedro Alcino; SILVA, Roberto da. **Metodologia Científica.** São Paulo: Pearson Prentice Hall, 2007.

CRUZ, José Magalhães, 2010 [acesso em: 11 de outubro de 2013] Disponível em: http://web.fe.up.pt/~jmcruz/ssi/acetat/1-intro.pdf

DIAS, Cláudia. **Segurança e Auditoria da Tecnologia da Informação**. Rio de Janeiro: Axcel Books, 2003

DUARTE, Otto Carlos Muniz Bandeira, **Segurança em Smart Grid,** 2012 [acesso em 09 de Julho de 2014]. Disponível em: http://www.gta.ufrj.br/grad/12_1/seg_smartgrid/index.html

FONSECA, Paula Fernanda, G**estão de Segurança da Informação :** o fator humano, 2009.

GURGEL, GIOVANE MONTINE MOREIRA. **O VALOR ESTRATEGICO DA INFORMAÇÃO PARA A GESTÃO DAS ORGANIZAÇÕES,** (2006).

GIL, Antonio C. **Métodos e técnicas de pesquisa social.** 5. Ed. Sã Paulo: Atlas, 1999.

HOLANDA, Roosevelt de. **O estado da arte em sistemas de gestão da segurança da Informação: Norma ISO/IEC 27001:2005** – São Paulo: Módulo Security Magazine, 2006.

ISO/IEC TR 18044:2004 [Acesso 09 de julho de 2014]. Disponível em: http://www.ima.sp.gov.br/politica-de-seguranca-da-informacao>

ISO/IEC 13335:2004. [Acesso 09 de julho de 2014]. Disponível em: http://www.ima.sp.gov.br/politica-de-seguranca-da-informacao

IMONIANA, J. O. **Carrer Development in IT Auditing: Work Internship, Work Experience or Formal Educational Training**. Revista Álvares Penteado. São Paulo. v. 5, n. 11, 2003.

LAKATOS, E. M; MARCONI, M. A. **Fundamentos de Metodologia Científica**. São Paulo, Ed Atlas, 1991.

LAUDON, K. C.; LAUDON, J. P. **Sistemas de informações gerenciais: administrando a empresa digital.** 5. ed. São Paulo/SP: Prentice Hall, 2004.

LOSSCONTROL. **A informação e sua importância**, p.1, 2003. [Acesso em 09 de julho de 2014]. Disponível em http://www.losscontrol.com.br/seguranca.htm

MALHOTRA, Naresh K. **Pesquisa de marketing: uma orientação aplicada.** 3. Ed. Porto Alegre: Bookman, 2001.

MARTINS, Alaíde Barbosa e SANTOS, Celso Alberto Saibel. Uma Metodologia para implantação de um Sistema de Gestão de Segurança de Informação, 2005.

MORAES, P. E. S.; Laureano, M. A. P.. **SEGURANÇA COMO ESTRATÉGIA DE GESTÃO DA INFORMAÇÃO**, 2005.

MORESI, Eduardo. A. D, **Metodologia da pesquisa.** Brasília-DF: Universidade Católica de Brasília, agosto, 2004.

REZENDE, Denis Alcides e ABREU, Aline França. **Tecnologia da Informação Aplicada a Sistemas de Informação Empresariais.** São Paulo: Atlas, 2000

RFC 2196 (1997) [acesso em 14 de outubro de 2013]. Disponível em: http://www.normes-internet.com/normes.php?rfc=rfc2196&lang=pt

SÊMOLA, M. **Gestão da Segurança da Informação – Uma visão executiva**. 3. Ed. Rio de Janeiro: Elsevier, 2003.

SILVA D.R.P.; STEIN, L.M. “**Segurança da Informação: uma Reflexão sobre o componente humano**”. Ciencias & Cognição, 2007

STAIR, R. M.; REYNOLDS, G. W. **Princípios de sistemas de informação: uma abordagem gerencial.** 4. ed. Rio de Janeiro/RJ: LTC, 2002

SMICALUK, A.; WILLE, M. V.; MARCONDES, E.; SLISINSKI, A.; POMBEIRO, O. J.; **Política de Segurança da Informação.** Paraná, 2007.

TECHNET, 2010 [Acesso em 10 de outubro de 2013]. Disponível em: http://technet.microsoft.com/pt-br/security/default.aspx

ULBRICH, C. H.; Valle, D. J. **Universidade H4ck3r Desvende todos os segredos do submundo dos hackers.** Ed: Digerati Books, 2003

ANEXO A

Este questionário visa inferir o conhecimento dos estudantes da UFPE-CAA acerca da percepção a respeito das políticas de seguranças da informação. e através do mesmo atingir os objetivos do trabalho de conclusão de curso com o titulo : POLÍTICA DE SEGURANÇA DA INFORMAÇÃO: UMA ANÁLISE DA PERCEPÇÃO DOS ESTUDANTES DE ADMINISTRAÇÃO DA UNIVERSIDADE FEDERAL DE PERNAMBUCO – CAMPUS ACADÊMICO DO AGRESTE.

LEGENDA:
DT – Discordo Totalmente
DP – Discordo Parcialmente
ID – Indiferente
CP – Concordo Parcialmente
CT – Concordo Totalmente

PARTE 1

1 - QUAL O SEU PERÍODO?								
1	2	3	4	5	6	7	8	9
2 - Você possui vinculo empregatício, ou estagiário, na área de gestão?								
SIM				NÃO				

PARTE 2

1 - Você já ouviu falar no assunto Política de Segurança da Informação?			
SIM		NÃO	
2 - Na empresa que você trabalha existe um Documento de Políticas de Segurança da informação?			
SIM		NÃO	DESCONHEÇO

PARTE 3

1 - Numa escala de 0 a 10, qual a importância, para você, acerca do tema política de segurança da informação?										
0	1	2	3	4	5	6	7	8	9	10
2 - Conhecer sistemas de informação é essencial para os administradores										
DT		DP		ID		CP		CT		
3 - Um gestor (Formado na área de administração) deve ter uma noção,										

mesmo que básica, acerca do tema política de segurança.

DT		DP		ID		CP		CT	

4 - No CAA o curso de Administração da uma boa formação acerca do tema políticas de segurança da informação.

DT		DP		ID		CP		CT	

5 - Obedecer a uma política de segurança da informação é uma cultura boa para a organização.

DT		DP		ID		CP		CT	

6 - Uma política de segurança deve ser feita em conjunto, por todos o gestores da organização.

DT		DP		ID		CP		CT	

7 - O gestor deve classificar a informação quantos aos princípios de disponibilidade, confidencialidade e integridade.

DT		DP		ID		CP		CT	

8 - As senhas devem ser únicas e individuais, seguindo critérios de qualidade, isto é, senhas fortes com trocas periódicas

DT		DP		ID		CP		CT	

9 - O acesso a áreas de servidores devem ser consentidos mediante autorização. Deve-se ter controle quanto à entrada e saída de equipamentos e pessoas

DT		DP		ID		CP		CT	

10 - Desenvolvimento de sistemas ou compra de sistemas/software – é importante definir uma sistemática interna com ênfase nos requisitos de segurança

DT		DP		ID		CP		CT	

11 - Geração de controles e padrões especificando detalhes quanto ao plano de captação de recursos humanos.

DT		DP		ID		CP		CT	

12 - Uma política de segurança da informação deve ser implantada junto a um treinamento.

DT		DP		ID		CP		CT	

13 - A política de segurança da informação deve ser algo que todos os funcionários venham a seguir criteriosamente as regras

DT		DP		ID		CP		CT	

14 - Segurança da informação é a preservação da confidencialidade, da integridade e da disponibilidade da informação;

DT		DP		ID		CP		CT	

15 - Anotar senhas em algum lugar é uma boa idéia para não esquecê-las

DT		DP		ID		CP		CT	

16 - Qualquer papel de escritório pode ser facilmente descartado simplesmente jogando-o no lixeiro.

DT		DP		ID		CP		CT	

17 - Costumo utilizar termos fáceis para as minhas senhas. (ex. Data de nascimento, nomes, número de celular e Etc.)

DT		DP		ID		CP		CT	