FACULDADE JESUS MARIA JOSÉ – FAJESU
CURSO DE TECNOLOGIA EM REDES DE COMPUTADORES

WASHINGTON RIBEIRO

A COMPETÊNCIA HUMANA À FRENTE DAS TECNOLOGIAS: COMO IDENTIFICAR AS FRAGILIDADES MAIS COMUNS DOS PROCEDIMENTOS DE SEGURANÇA NA REDE DE COMPUTADORES DE UMA EMPRESA

TAGUATINGA - DF
2007

WASHINGTON RIBEIRO

A COMPETÊNCIA HUMANA À FRENTE DAS TECNOLOGIAS: COMO IDENTIFICAR AS FRAGILIDADES MAIS COMUNS DOS PROCEDIMENTOS DE SEGURANÇA NA REDE DE COMPUTADORES DE UMA EMPRESA

Trabalho de Conclusão de Curso apresentado à Banca Examinadora designada pela Coordenação dos Cursos de Tecnologia da Faculdade Jesus Maria José, como requisito parcial para a obtenção do título de Tecnólogo em Redes de Computadores.

Orientador: MS. Marco Antônio Santos

TAGUATINGA - DF
2007

FACULDADE JESUS MARIA JOSÉ – FAJESU
CURSO DE TECNOLOGIA EM REDES DE COMPUTADORES

A COMPETÊNCIA HUMANA À FRENTE DAS TECNOLOGIAS: COMO IDENTIFICAR AS FRAGILIDADES MAIS COMUNS DOS PROCEDIMENTOS DE SEGURANÇA NA REDE DE COMPUTADORES DE UMA EMPRESA

WASHINGTON RIBEIRO

Trabalho de Conclusão de Curso apresentado à Banca Examinadora designada pela Coordenação dos Cursos de Tecnologia da Faculdade Jesus Maria José, como requisito parcial para a obtenção do título de Tecnólogo em Redes de Computadores.

Aprovado em 14 de dezembro de 2007

Aprovado por:

_____
Professor Mestre: Marco Antonio Martins dos Santos
Presidente – Orientador (FAJESU/Coordenação de Tecnologia)

_____
Professor Mestre: Alexandre Zaghetto
Membro (FAJESU/Coordenação de Tecnologia)

_____
Professor Mestre: Geraldo Campetti Sobrinho
Membro (FAJESU/Coordenação de Tecnologia)

Ao meu eterno amor, Leila Ribeiro,
que sonhou junto comigo essa realização
e me apoiou mesmo nos momentos que
não acreditei que seria possível.
Pelas palavras de apoio, orientações,
incentivo, carinho, compreensão
e pelas diversas noites de espera.Obrigado!

AGRADECIMENTOS

A Deus.

Ao meu orientador, professor Marco Antônio, que me ajudou a encontrar o caminho correto e tornou possível a realização deste trabalho.

Aos professores Adriano Messias, Alexandre Zaghetto, Elias Freitas, Geraldo Campetti e João Batista, que contribuíram com a experiência e tiveram paciência na ajuda da delimitação do tema de pesquisa deste trabalho.

À minha turma especial, que contribuiu com discussões e sugestões.

Ao meu grupo de estudos zero506idem formado por Clara Larissa, Claudia Fernandes, Daniela Rebeca e Lígia Vieira, companheiras de reflexões. Os trabalhos realizados foram muito importantes para o esclarecimento de diversos pontos abordados nesta pesquisa.

Aos meus companheiros de trabalho Bruno Amorim, Graziella Mello, Jaquelma Amorim, Denilson Sócrates, Alysson Oliveira, Thiago Sena e Hélio Alcântara, que participaram de forma direta na discussão de pontos importantes.

À Joelita Araujo que teve paciência para revisar todo este trabalho.

Aos gerentes dos departamentos que facilitaram o acesso as informações e apoiaram nas várias etapas deste trabalho.

À empresa pesquisada, que permitiu a realização deste trabalho.

Aos usuários da empresa pesquisada que responderam ao questionário e concederam entrevistas. A colaboração de todos foi fundamental.

A toda minha família, em especial aos meus pais, Vitória Ribeiro e Wellington Souza, que acreditaram na realização deste trabalho antes mesmo de mim.

A todos os amigos que contribuíram de alguma forma para a conclusão deste trabalho.

Esse vidro fechado
E a grade no portão
Suposta segurança
Mas não são proteção

E quando o caos chegar
Nenhum muro vai te guardar
De você

Protótipo imperfeito
Tão cheio de rancor
É fácil dar defeito
É só lhe dar poder

Se tornam prisioneiros
Das posses ao redor
Olhando por entre as grades
O que a vida podia ser

Mas quando o caos chegar
Nenhum muro vai te guardar
De você

E é com a mão aberta
Que se tem cada vez mais
A usura que te move
Só vai te puxar pra trás
[Vai te puxar pra trás]

De você - Pitty

RESUMO

Identifica as fragilidades mais comuns nos procedimentos de segurança em uma rede local de computadores de uma empresa tendo como foco principal o fator humano. Para isso documenta os procedimentos de segurança utilizados na rede de computadores, identifica os procedimentos utilizados pelos usuários para o cumprimento dos procedimentos de segurança e identificamos também a forma de aprendizagem dos usuários da rede de computadores com base nas inteligências múltiplas de Howard Gardner. Para tanto, opta por uma pesquisa de campo, descritiva. Os resultados obtidos demonstraram que as deficiências mais comuns estão nas relações profissionais mediadas pela linguagem. Os problemas identificados mostram a falta de comunicação entre os usuários e tecnólogos da rede de computadores. Essas falhas na comunicação acabaram gerando ruídos nessa interface comprometendo a segurança da rede de computadores.

Palavras-chaves: Segurança de rede de computadores, fator humano, inteligências múltiplas, linguagem.

ABSTRACT

Identified the most common weaknesses in the procedures for security in a local area network of computers of a company with the main focus the human factor. For this it was documented security procedures used in the network computers, identify the procedures used by users for the achievement of security procedures and also identify the form of learning from users of the network of computers based on the multiple intelligences of Howard Gardner. For this, we choose a descriptive fieldwork search. The results showed the deficiencies are more common in professionals relations mediated by language. The problems show a lack of communication between users and technologists of the network of computers. These flaws in the communication result in a “noise” in that interface, and consequentely compromising the security of the network of computers.

Keywords: Security of networked computers, human factor, multiple intelligences, language.

LISTA DE FIGURAS

LISTA DE GRÁFICOS

SUMÁRIO

1 INTRODUÇÃO

Quem mexe com Internet,
fica rico sem sair de casa.
Quem tem computador,
não precisa de mais nada
Estudar pra quê?
John, Pato Fu

Quando o computador pessoal e a Internet se tornaram uma realidade na década de 1970 e geraram todo este boom tecnológico que vivemos atualmente, não poderíamos imaginar que afetaria nossa forma de viver hoje. O rompimento desse paradigma gerou novas perspectivas, e hoje a maior parte da população depende de forma direta ou indiretamente dos computadores e, principalmente, da Internet. Seja para uso pessoal ou corporativo, trabalho ou diversão, informação, cultura ou lazer.

O boom tecnológico dos computadores e o da Internet não aconteceram simultaneamente, ou seja, a evolução dos computadores não está necessariamente vinculada ao advento da Internet. Primeiro foi o computador que sofreu diversas mutações até chegar aos modelos que conhecemos hoje. Na década de 1970, os computadores começaram a ser desenvolvidos com circuitos integrados, uma das principais características dessa geração, também conhecida com a quarta geração de computadores que são fabricados até os dias de hoje, conforme descreve Stallings (2003, p. 39). Aliado ao desenvolvimento do hardware, que é a parte física dos computadores, houve também uma evolução do software, que é parte lógica utilizada nos computadores. Foi nesse período que surgiram os processadores de texto, planilhas eletrônicas, bancos de dados, programas de comunicação e gerenciamento de imagens (STALLINGS, 2003, p.40).

A Internet foi criada inicialmente para garantir a segurança nas comunicações militares dos Estados Unidos da América nos anos da Guerra Fria, pois as comunicações feitas por telefone eram vulneráveis. Com o fim da guerra, a Internet passou a ser utilizada por universidades e ficou estagnada até o início dos anos 1990, quando houve uma guinada comercial e se tornou o maior fenômeno de evolução tecnológica, a rede mundial de computadores (TANENBAUM, 2003, p. 54).

Essa união entre Internet e computadores gerou um estouro comercial em um curto período de tempo e impulsionou um conceito importante nesse conjunto: as redes de computadores (TANENBAUM, 2003, p.55). A necessidade de compartilhar informações, recursos, programas e equipamentos, estimulou essa tecnologia, aliada ao custo cada vez mais reduzido dos equipamentos e serviços no decorrer dos anos. Com todas essas evoluções, os computadores passaram a ser viáveis para utilização nas empresas de médio e pequeno porte e também no uso doméstico.

Hoje é impossível imaginar como o mundo seria se não existissem as redes de computadores. Atualmente, todas as aplicações, serviços e equipamentos são fabricados para o mundo das redes, seja ela Ethernet[1], IP[2], Wi-Fi[3], Bluetooth[4], entre outras.

Com todo esse desenvolvimento, as profissões passaram a depender cada vez mais dessas tecnologias e, conseqüentemente, passou a ser exigido conhecimento tecnológico para a utilização dos computares. Com isso, passamos a ter profissionais que criam tecnologias e os demais profissionais, que dependem da tecnologia criada para melhorar o desempenho de suas funções, criando assim relações profissionais em que a tecnologia passa a ser a linguagem.

A necessidade de essa linguagem ser bem explicada pelos profissionais que a controlam e ser bem entendida pelos profissionais que a utilizam passou a ser fundamental nas relações profissionais, pois quem cria, o faz no intuito de melhorar o desempenho do profissional que irá utilizar. E quem utiliza, o faz com a expectativa de melhorar seu desempenho profissional. Quando isso não acontece, as relações são abaladas e geram-se ruídos. Esses ruídos quase sempre têm reflexos negativos nas relações profissionais e, quando não são resolvidos, podem gerar conseqüências negativas para as empresas. Na Figura 1, relação ruído, temos a representação dessa relação demonstrando quanto maior o ruído gerado pela falta de utilização correta na linguagem utilizada pelo desenvolvedor, menor certa a satisfação do utilizador. Por outro lado, quanto menor o ruído causado pela linguagem utilizada, maior será a satisfação do usuário.

[1] Tecnologia de interconexão de redes locais (Local Area Networks - LAN)
[2] Protocolo de Internet (Internet Protocol)
[3] Tecnologia de redes sem fio (Wireless Local Area Network - WLAN)
[4] Tecnologia para comunicação sem fio entre dispositivos eletrônicos

Figura 1 – Relação ruído (RIBEIRO, W.)

Em uma empresa hoje, a maioria dos setores utiliza computadores em rede. Os advogados podem fazer consultas em tribunais pela Internet enquanto redigem petições. A analista de recursos humanos prepara os contracheques dos funcionários e faz consultas na Consolidação das Leis do Trabalho (CLT) pelo computador. O economista prepara a tabela de correção do imposto de renda e analisa o índice da inflação pela página do Banco Central. O administrador faz cotações de preços para compra de materiais de escritório nas páginas de comércio eletrônico das empresas de vendas. Em todos esses exemplos, os profissionais estão em suas respectivas salas, utilizando seus computadores, que estão ligados em redes e com acesso à Internet. Eles podem comunicar-se entre si, mas não têm acesso aos arquivos dos outros nem às informações que os outros estão acessando. Quem gerencia os processos de segurança na rede é o tecnólogo por meio de suas ferramentas de trabalho.

1.1 DELIMITAÇÃO DO PROBLEMA

O mundo fascinante das redes de computadores nos remete a uma questão importante nesta globalização. Se por um lado podemos ter computadores interligados com acesso a qualquer informação, de outro lado temos nossos dados expostos quando há uma quebra de segurança. Nesse tráfego intenso de informação, todos querem ter acesso facilitado às redes, mas ninguém quer ter suas informações expostas.

No mundo coorporativo, essa situação não é diferente. A questão da segurança deixou de ser um capricho e passou a ser encarada como prioridade mais importante. Ter os computadores interligados, em diferentes pontos do escritório, em outros andares ou prédios ou até mesmo em outras cidades, estados ou até mesmo países passou a ser uma necessidade real na vida das empresas hoje.

Os problemas que enfrentamos atualmente não são diferentes dos problemas existentes antes das redes de computadores. A segurança da informação sempre foi um dos pilares nas questões tecnológicas. E essa segurança passou a ser uma das maiores preocupações com a chegada das redes de computadores, como descrito por Moreira (2007, p. 5): "uma pesquisa do Datafolha apontou, no final de março, que a segurança é a maior preocupação do brasileiro". Hoje é possível ser assaltado sem que o ladrão chegue perto da vítima. Por meio do computador, ligado a uma rede de computadores e utilizando técnicas de captura de senhas e dados, engenharia social ou outro meio desenvolvido para esse fim, o ladrão consegue executar de forma rápida seus golpes.

Em uma empresa, para manter a segurança da rede de computadores, normalmente o tecnólogo utiliza mecanismos de segurança baseados em hardware e software, ou seja, os investimentos são baseados em redundâncias dos servidores, câmeras de segurança, criptografia dos dados, senhas de acesso, anti-spam[5], antivírus[6], firewall[7], entre outros. Existem também as políticas de segurança que normalmente são escritas pelo administrador da rede, sua equipe de suporte e o responsável pelo departamento de recursos humanos e envolvem as referências, recomendações e punições para manter a ordem na rede de computadores.

Essas ferramentas são capazes de controlar e detectar uma grande parte das ameaças digitais que são lançadas todos os dias nas redes de computadores. Mas existe um ponto que ainda preocupa os administradores de redes, conhecido como o elo mais fraco da segurança de redes: o fator humano. Tanenbaum (2003, p. 543) define o fator humano da seguinte forma:

> A maior parte dos problemas de segurança é causada intencionalmente por pessoas maliciosas que tentam obter algum benefício, chamar a atenção ou prejudicar alguém. Alguns dos invasores mais comuns são estudantes, crackers, vendedores, ex-funcionários, entre outros. A partir dessa lista fica claro que tornar uma rede segura envolve muito mais do que simplesmente

[5] Anti-spam é uma ferramenta que deixa sua caixa de e-mail livre de propaganda, vírus e pornografia (TANENBAUM, 2003, p. 461)

[6] Antivírus é software que protege o computador da infecção de vírus. (TANENBAUM, 2003, p. 641)

[7] Firewall é apenas uma adaptação moderna de uma antiga forma de segurança medieval: um fosso profundo em torno do castelo. Esse recurso forçava todos aqueles que quisessem entrar ou sair do castelo a passar por uma única ponte levadiça, onde poderiam ser revistados por guardas conforme descreve Tanenbaum (2003, p. 583).

> mantê-la livre de erros de programação. Para tornar uma rede segura, com freqüência é necessário lidar com adversários inteligentes, dedicados e, às vezes, muito bem subsidiados. Você também deverá ter em mente que as medidas utilizadas para interromper a atividade de adversários eventuais terão pouco impacto sobre os adversários "mais espertos".

Inerente ao desequilíbrio que o fator humano causa na segurança, o tecnólogo continua a investir mais pesado em hardware e software para tentar barrar as falhas cometidas. Mas contra o fator humano ainda não foi possível criar nenhum mecanismo, seja baseado em hardware ou em software, capaz de deter os estragos causados.

1.2 JUSTIFICATIVA

A maior preocupação do tecnólogo atualmente é garantir a segurança da rede de computadores dificultando a ação do fator humano, para isso os investimentos normalmente são feitos nos processos de segurança. Mas quanto maior a segurança baseada nestes processos, menor será a usabilidade para os usuários.

Vejamos um exemplo: preocupado em garantir que seus usuários utilizem senhas mais fortes, o suporte determina que as senhas sejam trocadas de 30 em 30 dias, tenha no mínimo oito dígitos entre letras e números e não sejam iguais às dez últimas utilizadas. O usuário, que nunca precisou trocar sua senha, agora precisa se adaptar à nova regra de segurança. Ainda visando à segurança, o suporte determina que toda vez que o usuário for acessar a Internet digite novamente a senha para garantir que ele está acessando. O usuário preocupado com sua produtividade, executará o processo exigido pelo tecnólogo, mas irá criar mecanismos para facilitar a utilização e a lembrança da senha. Baseado nas regras impostas pelo tecnólogo o usuário cria uma senha forte, mas para não esquecer anota em um papel e guarda em sua gaveta, ou em cima da mesa ou cola no monitor. Com isso o usuário coloca todo o procedimento de segurança criado pelo tecnólogo em risco uma vez que este pedaço de papel com a senha pode ir para o lixo ou ser visto por outras pessoas. Na figura 2 podemos visualizar a relação de equilíbrio entre os procedimentos de segurança *versus* as facilidades de utilização.

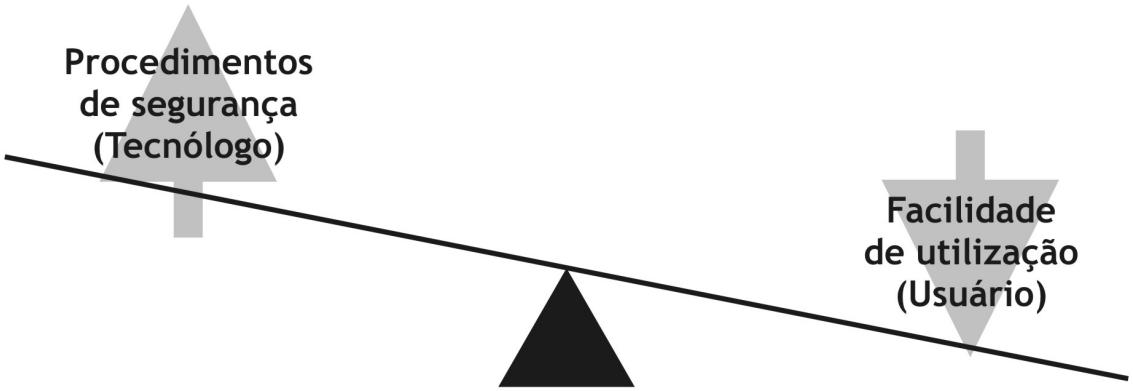

Figura 2 – Procedimentos de segurança x facilidade de utilização (RIBEIRO, W.)

Dessa forma, a utilização de rotinas de segurança da rede de computadores no ambiente de trabalho baseadas em processos estarão seguindo os mesmos passos: quanto maior a implementação de políticas de segurança, menor será a facilidade de utilização da tecnologia para o usuário e maior será o desgaste entre as duas partes.

O foco da segurança está no processo e não nas pessoas. E, por mais óbvio a necessidade de melhorar essa relação, o tecnólogo prefere investir mais em tecnologia, criando novas formas, regras e ferramentas para restringir mais a usabilidade do usuário, chegando às vezes a se tornar uma paranóia, em vez de segurança.

Mas para trabalhar com uma visão mais humanística nessa relação profissional e atingir de forma mais direta seus usuários, o tecnólogo terá de utilizar ferramentas que saem da área tecnológica como e pensamento sistêmico para ter uma visão mais ampla e abrangente de todo o contexto, conforme definido por Nogueira (2001, p. 48). Assim é possível formar um leque de opções para entender e explicar aos seus usuários como trabalhar questões de segurança na rede de computadores.

Uma proposta para ferramenta de apoio ao tecnólogo, que será apresentada em detalhes no referencial teórico, é a teoria das inteligências múltiplas, desenvolvida por um grupo de pesquisadores de Harvard chefiada por Howard Gardner. Segundo Gardner (1995), foram relacionadas as seguintes inteligências: musical, corporal-cinestésica, lógico-matemática, lingüística, espacial, intrapessoal, interpessoal e naturalista. Trabalhando as inteligências múltiplas com os usuários de uma rede de computadores será possível estimular e potencializar as habilidades. Criando uma interface amigável e entendendo como cada um resolve problemas, assimila conceitos e aprende novas técnicas na utilização da tecnologia,

como argumenta Campetti (2007, p. 68), “as inteligências não são objetos que podem ser contados, e sim, potenciais que poderão ser ou não ativados, dependendo dos valores de uma cultura específica”.

Com o uso dessa ferramenta, apontaremos diretrizes para melhorar a interação entre usuário e tecnólogo em uma rede de computadores com uma visão interdisciplinar. Mas ela não funcionará sozinha, trabalhará em conjunto com as ferramentas de hardware e software utilizadas hoje para manter a segurança das redes de computadores.

1.3 OBJETIVO GERAL

Identificar as fragilidades mais comuns nos procedimentos de segurança em uma rede local de computadores de uma empresa tendo como foco principal o fator humano.

1.4 OBJETIVOS ESPECÍFICOS

- Documentar os procedimentos de segurança na rede local de computadores da empresa.
- Identificar os procedimentos utilizados pelos usuários para o cumprimento dos procedimentos de segurança.
- Identificar a forma de aprendizagem dos usuários da rede local de computadores com base nas inteligências múltiplas.

1.5 PERGUNTA DE PESQUISA

Quais as fragilidades mais comuns nos procedimentos de segurança em uma rede local de computadores de uma empresa tendo como foco principal o fator humano?

1.6 DESENVOLVIMENTO E PLANEJAMENTO DO PROJETO

O objetivo desta pesquisa é apresentar resultados que irão identificar e fundamentar as fragilidades mais comuns dos procedimentos de segurança em uma rede local de

computadores com foco na relação humana, apresentando as linhas de visão dos dois lados envolvidos na relação, usuário e tecnólogo. Com esses alicerces, abre-se um caminho para chegar a uma interseção, fazendo com que eles coexistam e possam manter um relacionamento produtivo. O aprendizado será uma via de mão dupla na qual os caminhos trilhados levarão o usuário e o tecnólogo para o mesmo resultado, como mostra a comparação de Chauí (1982, p. 7) sobre o aluno e o instrutor de natação.

> Não se ensina o outro a nadar, fazendo-o imitar seus próprios gestos soltos na areia. Lança-se n'água com o outro para que ele aprenda a nadar lutando contra as ondas, fazendo o corpo coexistir com o corpo ondulante das águas que o repelem e acolhem, descobrindo que a luta e o diálogo não se travam com o instrutor, mas com a água.

Assim como o instrutor de natação, o tecnólogo não pode ensinar o usuário a imitar seus passos. O usuário irá aprender nas situações reais do dia-a-dia tendo sempre em mente os ensinamentos repassados pelo tecnólogo.

2 METODOLOGIA DE PESQUISA

Vou procurar um provedor
Procurar um provedor
Celestial
Chico Science & Nação Zumbi

A pesquisa centra-se no levantamento dos procedimentos executados pelos usuários de uma rede de computadores, dos conhecimentos sobre as políticas de segurança e conhecimentos técnicos, portanto, desenvolvemos uma pesquisa descritiva com base em seus objetivos que irá apontar diretrizes para auxiliar o tecnólogo a gerenciar melhor o fator humano dentro da rede de computadores. É importante ressaltar que não pretendemos com isso elaborar uma receita de sucesso e sim apontar diretrizes que possam otimizar a segurança na rede de computadores. É preciso criar mecanismos que auxiliem o tecnólogo a identificar as variáveis para utilização correta. A identificação dessas variáveis multifacetadas pode gerar resultados diferenciados e análises diferentes, conforme descreve Gil (2006, p. 42):

> Algumas pesquisas descritivas vão além da simples identificação da existência de relações entre variáveis, e pretendem determinar a natureza dessa relação. Neste caso, tem-se uma pesquisa descritiva que se aproxima de explicativa. Há, porém, pesquisas que, embora definidas como descritivas com base em seus objetivos, acabam servindo mais para proporcionar uma nova visão do problema, o que as aproxima das pesquisas exploratórias.

Portanto, utilizamos os seguintes instrumentos: documentos da empresa; questionário escrito e fechado que será aplicado aos usuários da rede de computadores; entrevista individual de sete usuários que serão selecionados com base em questionário fechado e que apresentarem informações dúbias nas questões respondidas; notas de campo.

Para conseguir ter uma maior profundidade na análise dos instrumentos descritos, utilizamos a pesquisa de campo, possibilitando assim a flexibilidade no planejamento e facilitando a reformulação dos objetivos no decorrer da pesquisa em caso de necessidade. Outro ponto determinante é o foco direcionado em um único grupo, de acordo com Gil (2006, p. 53):

> Já no estudo de campo, estuda-se um único grupo ou comunidade em termos de sua estrutura social, ou seja, ressaltando a interação entre seus componentes. Dessa forma, o estudo de campo tende a utilizar muito mais técnicas de observação do que de interrogação.

Levando-se em consideração que o pesquisador está inserido no cenário de pesquisa, o levantamento dos instrumentos é de extrema importância e apresenta resultados fidedignos e respostas mais confiáveis dos pesquisados.

2.1 CENÁRIO DA PESQUISA

A pesquisa foi realizada em uma empresa que tem sede e foro em Brasília, Distrito Federal, e circunscrição sobre todo o território nacional. A empresa é composta de 95 funcionários de áreas de atuação diferenciadas, seis gerentes e é dirigida por 27 diretores. Tem por base congregar e representar o filiado na defesa de seus direitos e interesses, tanto profissionais como de natureza salarial, coletivos e individuais e promover a valorização da empresa entre outros. Por questões éticas e para resguardar a segurança da empresa, as demais informações serão mantidas em sigilo.

2.2 PARTICIPANTES DA PESQUISA

Os 95 funcionários da empresa são divididos em departamentos e tem áreas de atuação distintas. São advogados, gerentes, administradores, contadores, economistas, secretárias, tecnólogos em informática, assistentes e auxiliares administrativos e estagiários. O suporte técnico tem oito funcionários para atender a todos os usuários da rede de computadores. Preocupados com os princípios éticos e a segurança das informações da empresa já citados, identificamos cada usuário desta pesquisa por meio de nomes fictícios baseados na mitologia grega e romana, assim como os departamentos serão identificados com as letras do alfabeto grego.

2.3 INSTRUMENTOS UTILIZADOS PARA O LEVANTAMENTO DOS DADOS

O objetivo desta pesquisa é identificar as fragilidades mais comuns dos procedimentos de segurança na rede de computadores de uma empresa. Para isso foram selecionados instrumentos que apontaram as variáveis necessárias, a saber:

2.4 DOCUMENTOS DA EMPRESA

Os documentos que norteiam as regras para utilização da rede de computadores e definem as políticas de segurança na empresas são:

- Circular 2007, assinada pelo departamento alfa.
- Termo de Compromisso, elaborado pelo departamento alfa.

A íntegra da Circular 2007 e a íntegra do Termo de Compromisso encontram-se no anexo 1 e anexo 2, respectivamente.

Outro documento está em fase de estudos e discussão para uma posterior implantação:

- Políticas de Segurança da Informação da Empresa, elaboradas pelo departamento delta.

2.5 QUESTIONÁRIO FECHADO

O questionário foi elaborado com respostas fechadas a fim de analisar o conhecimento técnico, o conhecimento profissional e as competências profissionais dos entrevistados. O questionário fechado encontra-se no anexo 7.3. As perguntas foram as seguintes:

1. Qual sua idade?
2. Qual sua formação acadêmica?
3. Seu trabalho está relacionado à informática?
4. Já fez algum curso de informática?
5. Você conhece as políticas de segurança da empresa?
6. Quando você recebe um e-mail que contém um SPAM, o que acontece?
7. Para imprimir um documento que está aberto no Microsoft Word, qual dessas opções você mais utiliza?

8. Para ler suas mensagens de sua conta de e-mail externo (particular), você:
9. Quando há um problema em outro departamento, você:
10. Quando você recebe um arquivo em anexo ao e-mail, você é capaz de identificar qual a extensão do arquivo recebido?
11. Você já participou de algum treinamento sobre segurança promovido pela empresa?
12. Quando você tem problemas (qualquer um) em seu computador de trabalho:
13. Marque as atividades que você mais gosta de fazer:

As opções de resposta disponibilizadas para as questões 7, 8, 9, 12 e 13 podem ser consultadas no anexo 7.3 desse trabalho.

As perguntas 1, 7, 9 e 13 se referem às habilidades das competências profissionais com foco nas inteligências múltiplas de Gardner, que serão abordadas com detalhes no capítulo metodológico. Com essas respostas é possível identificar quais as inteligências são mais difundidas entre os usuários e qual a melhor forma de abordagem deve ser utilizada para passar informações e treinamentos. As perguntas 2, 4 e 12 se referem à formação e à atualização profissionais com foco no funcionário e na sua visão da empresa. As perguntas 3, 5, 8 10, 11 e 12 abordam o conhecimento técnico na área de informática com ênfase na rede de computadores.

As perguntas foram dispostas em ordem aleatória de assunto, assim com as respostas de cada pergunta, para dificultar a identificação de padrões de lógica pelos funcionários. O questionário foi validado por uma equipe de oito profissionais que trabalham na área de suporte da rede de computadores da empresa, que ajudaram no aprimoramento das questões para a realidade da empresa e de seus usuários.

2.6 ENTREVISTAS INDIVIDUAIS

Após a análise do questionário fechado, foram convidados sete usuários para aprofundar a discussão dos pontos levantados. A entrevista foi realizada em formato de bate-papo, deixando assim o clima mais agradável e relaxado e o entrevistado mais à vontade para expressar suas opiniões. Além dos usuários, foi realizada uma entrevista com o suporte da empresa para esclarecer os pontos apresentados pelos usuários e fornecer informações sobre algumas medidas implantadas. As íntegras das entrevistas encontram-se nos anexos 4, 5, 6, 7, 8, 9, 10 e 11.

2.7 NOTAS DE CAMPO

As notas de campo foram coletadas pelo pesquisador no período da realização da pesquisa. Foram relatados os atendimentos que foram feitos no dia, o usuário solicitante, o problema informado, o problema solucionado e um resumo do atendimento.

3 REFERENCIAL TEÓRICO

O mundo muda,
a gente muda.
O mundo muda,
a gente muda,
o mundo muda.
I change, you change
we change I
André Abujamra, Karnak

3.1 REDES DE COMPUTADORES

O conceito mais simples para definição de uma rede de computadores é dado por Tanenbaum (2003, p. 18) como um conjunto de computadores, ou módulos processadores, independentes, conectados por um sistema de comunicação, que pode ser por fios, ondas de rádio freqüência, entre outros, com o intuito de trocarem informações conforme demonstrado na figura 1.

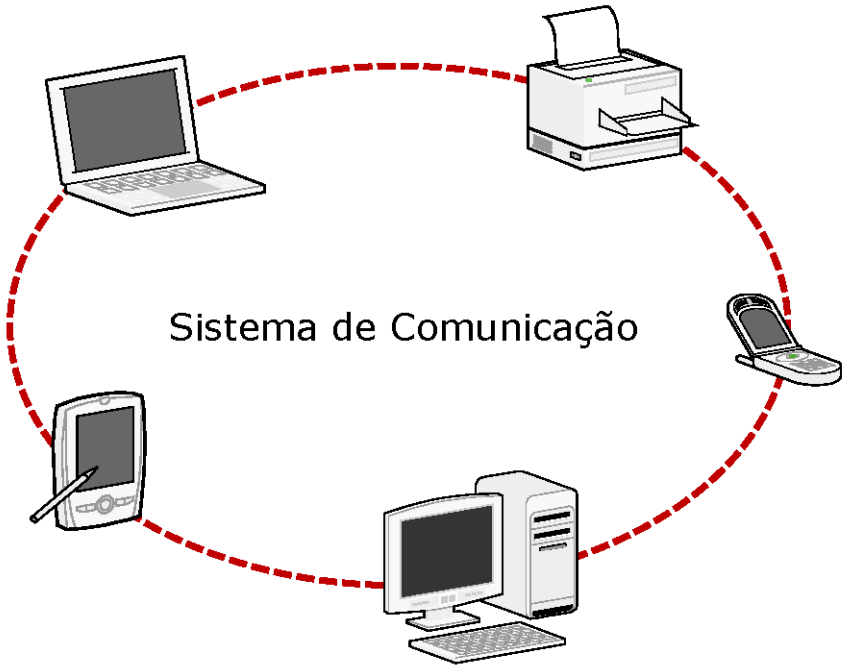

Figura 3 – Sistema de comunicação (SOARES, 2003, p. 11).

Uma rede de computadores pode ser classificada de várias formas, tamanhos, tecnologias utilizadas, aplicabilidades, topologias e conexões, mas neste trabalho de pesquisa necessitaremos apenas do conceito básico.

3.2 SEGURANÇA EM REDE DE COMPUTADORES

Segurança é o ato ou efeito de tornar seguro, dar estabilidade, firmeza, conforme descreve Houaiss (2007). Esse é um conceito geral e que abrange as mais diversas formas de segurança imagináveis. Para garantir a segurança de uma rede de computadores precisamos pensar na segurança física que envolve desde segurança do local onde a rede está montada até a saída do lixo; na segurança lógica que envolve criptografia dos dados[8], senhas, antivírus entre outros; e o fator humano. Simplificando o conceito e aplicando-o em uma rede de computadores, a segurança será responsável por garantir que as informações trafegadas na rede estejam livres de pessoas não autorizadas (TANENBAUM, 2003, p. 543).

Para garantir a segurança em uma rede de computadores, normalmente, a equipe de suporte utiliza diversas ferramentas e métodos, que na maioria das vezes são baseados em hardware e software como, por exemplo: backup, antivírus, firewall, controle de acesso das estações e senhas de acesso à rede. Todos esses procedimentos são baseados em mecanismos de prevenção e detecção de vulnerabilidades. Analisando o conceito de segurança e os mecanismos de prevenção e detecção, podemos afirmar que segurança não pode ser considerada uma tecnologia, mas um processo como expõe Wadlow (2001, p. 4).

> A segurança é um processo. Pode-se aplicar o processo seguidamente à rede e à empresa que a mantêm e, dessa maneira, melhorar a segurança dos sistemas. Se não iniciar ou interromper a aplicação do processo, sua segurança será cada vez pior, à medida que surgirem novas ameaças e técnicas.

Nessa mesma linha de conceituação, Schneier (2001, p. 12) vai mais fundo e começa seu livro, *segurança.com*, com a frase: “Escrevi este livro em parte para corrigir um erro.”. O erro a que Schneier se refere é considerar que apenas com a criptografia era possível proteger suas informações de todas as ameaças digitais. Schneier ainda destaca:

[8] A palavra criptografia vem do grego e significa “escrita secreta”, segundo Tanenbaum (2003, p. 545).

> Desde que escrevi o livro[9], tenho me mantido como consultor de criptografia: projetando e analisando sistemas de segurança. Para minha surpresa inicial, descobri que os pontos fracos não tinham nada a ver com a matemática. Eles estavam no hardware, no software, nas redes e nas pessoas. Trechos lindos de matemática se tornaram irrelevantes devido a uma programação ruim, um sistema operacional falho ou uma senha mal escolhida. Aprendi a ver além da criptografia, para o sistema inteiro, para descobrir os pontos fracos. Comecei a repetir alguns sentimentos que você irá adquirir no decorrer deste livro: "segurança é uma corrente: ela é tão segura quanto seu elo mais fraco." "Segurança é um processo, e não um produto".

E esse processo de segurança precisa ser contínuo e sempre atualizado, pois as tecnologias evoluem a todo instante e, com elas, as formas de ataque à segurança. Além de manter o hardware e software atualizados e seguros, é necessário uma interface amigável com o elo mais fraco da segurança, o fator humano.

3.3 FATOR HUMANO

Manter um processo de segurança funcionando perfeitamente em uma rede de computadores é quase uma utopia nos dias atuais. E um dos principais fatores de quebra no elo é o fator humano, como descreve Schneier (2001, p. 255):

> A segurança de computador é difícil (talvez até mesmo impossível), mas imagine por um momento que tenhamos conseguido. A criptografia forte está onde é exigida; protocolos seguros estão fazendo o que precisa ser feito. O hardware é seguro; o software é seguro. Até mesmo a rede é segura. É um milagre. Infelizmente, isso ainda não é suficiente. Para que esse milagroso sistema de computador realize algo útil, ele terá que interagir com usuários de alguma forma, em algum momento e por algum motivo. E essa interação é o maior risco à segurança de todos eles. As pessoas normalmente representam o elo mais fraco na corrente da segurança, e cronicamente são responsáveis pela falha dos sistemas de segurança.

Nesse processo, que inclui inúmeros problemas e variáveis, seria simples se todos os problemas fossem baseados somente em tecnologia. Sempre haverá a interação com o ser humano. Na maior parte dos casos, as falhas são causadas por pessoas que, de alguma forma, estão envolvidas com a empresa, como sintetiza Tanenbaum (2003, p. 767):

---

[9] *Applied Cryptography* de Bruce Schneier, 1996 .

> Os registros policiais mostram que a maioria dos ataques não é perpetrada por estranhos que grampeiam uma linha telefônica, mas por pessoas ressentidas com a empresa a que pertencem. Conseqüentemente, os sistemas de segurança devem ser projetados tendo em vista esse fato.

Projetar os sistemas de segurança tendo, também, como foco o fator humano é um trabalho que requer, além dos conhecimentos técnicos em segurança, o envolvimento de outros departamentos, principalmente na contratação e no treinamento dos funcionários de uma empresa. Wadlow (2001, p. 92) enumera alguns fatores importantes que contribuem para esses ataques:

> Habilidade, motivação e oportunidade são as condições necessárias para o sucesso de um ataque. O pessoal da empresa, sejam funcionários ou contratados por empreitada, membros do grupo de segurança ou trabalhadores de outros departamentos da empresa, são os favorecidos em termos de habilidades e oportunidades. Se qualquer um deles tiver a motivação necessária, poderá ser muito perigoso para a segurança da rede.

Mas evitar uma demissão ou uma insatisfação de funcionário, por exemplo, são variáveis que um profissional em segurança de redes não é capaz de mensurar em um sistema, o que acaba se tornando um problema com sérias conseqüências para a segurança.

Preocupados com os aspectos sociais que podem influenciar um profissional de tecnologia, Souza *et al.* (2005) apresenta em sua pesquisa, baseada em um estudo de caso, os pontos que podem melhorar a qualidade do trabalho das equipes de produção de engenharia de software. O estudo mostra que o bom relacionamento profissional e o convívio familiar podem influenciar de forma positiva na produção dos profissionais envolvidos.

3.4 ENGENHARIA SOCIAL

Além dos fatores já mencionados sobre as fragilidades do fator humano, ainda há a questão da engenharia social, que tem como foco principal o ser humano. A engenharia social pode ser definida como uma metodologia utilizada para obter informações desejadas sem a necessidade de tecnologia, como sintetiza Schneier (2001, p. 266):

> A engenharia social evita a criptografia, segurança de computador, segurança de rede e tudo o que for tecnológico. Ela vai diretamente para o elo mais fraco de qualquer sistema de segurança: o pobre ser humano sendo forçado a realizar seu trabalho, e precisando de toda a ajuda que puder obter.

Schneier (2001) cita o exemplo de Kevin Mitnick, um dos maiores engenheiros sociais da história, que tinha tanto sucesso em seus ataques, baseados na engenharia social, que dificilmente precisava fazer ataques técnicos.

A necessidade de investir em pessoas, além do investimento em tecnologias, está se tornando uma tendência crescente nas empresas como Rezende (2006, p. 42) argumenta:

> As empresas estão procurando dar mais atenção ao ser humano, pois é ele que faz com que as engrenagens empresarias funcionem perfeita e harmonicamente, buscando um relacionamento cooperativo e satisfatório para ambas as partes, com objetivos comuns.

Com essa visão holística em uma empresa, as barreiras de segurança estarão mais firmes e a possibilidade de falhas nos sistemas de segurança serão menores.

3.4 INTELIGÊNCIAS MÚLTIPLAS

Inteligência é definida como a faculdade de conhecer, compreender e aprender ou, mais especificamente, é a capacidade de aprender e organizar os dados de uma situação ou, ainda, a capacidade de resolver problemas e empenhar-se em processos de pensamento abstrato conforme definição do *Dicionário Houaiss* (2007). Assim, sempre que precisamos tomar decisões referentes à resolução de um problema é a inteligência que nos guiará para opção mais correta. Antunes (2003, p. 11) faz uma análise sobre a inteligência:

> Analisando de maneira sucinta as raízes biológicas da inteligência, descobre-se que ela é produto de uma operação cerebral e permite ao sujeito resolver problemas e, até mesmo, criar produtos que tenham valor específico dentro de uma cultura. Desta maneira, a inteligência serve para nos tirar de alguns "apertos" sugerindo opções que, em última análise, levam-nos a escolher a melhor solução para um problema qualquer.

Os produtos criados nesses casos podem resultar em soluções diferenciadas. Comumente, em nossa cultura, estamos acostumados a dar maior valor para as respostas mais sucintas que apontam para as habilidades lingüísticas e lógicas.

Essas habilidades, que podemos considerar inteligências de acordo com o conceito, formam a base para os testes de QI desenvolvidos pelo psicólogo Alfred Binet, no início do

século 20, em Paris. Os quais tinham como objetivo predestinar quais as crianças parisienses teriam sucesso e quais fracassariam nas séries primárias (GARDNER, 1995, p. 12).

Hoje, existem testes de QI mais desenvolvidos, capazes de aferir principalmente, o grau de aptidão escolar, mas sempre baseados na lógica e na linguagem apenas. Gardner (1995, p. 13) propõe uma rota alternativa e multifacetada para a inteligência:

> É uma visão pluralista da mente, reconhecendo que as pessoas têm forças cognitivas diferenciadas e estilos cognitivos contrastantes. Eu também gostaria de introduzir o conceito de uma escola centrada no indivíduo, que seriamente esta visão multifacetada de inteligência. Este modelo de escola baseia-se, em parte, nos achados científicos que ainda não existam no tempo de Binet: a ciência cognitiva (o estudo da mente) e a neurociência (o estudo do cérebro). É uma abordagem assim que chamei minha "teoria de inteligências múltiplas".

Dessa forma, Gardner aponta oito inteligências, a saber: inteligência musical, inteligência corporal-cinestésica, inteligência lógico-matemática, inteligência lingüística, inteligência espacial, inteligência interpessoal, inteligência intrapessoal e inteligência naturalista.

A inteligência musical é apresentada normalmente em músicos, que tem facilidade em identificar sons diferentes percebendo nuanças entre eles. Discernem com facilidade os tons, melodias, ritmos, timbres e freqüências, além do domínio para compor e cantar. Além dos cantores, músicos e afins que têm esta inteligência desenvolvida, podemos classificar outros profissionais que utilizam o domínio dessa habilidade para trabalhar como, por exemplo, mecânicos que conseguem identificar problemas no carro apenas pelos sons; professores que têm controle da classe de alunos por meio do timbre de voz, pessoas que conseguem identificar o humor pelo tom de voz de outra pessoa (ABREU-E-LIMA, 2006, p. 123).

Ter capacidade de controlar o corpo ou partes para resolver problemas como fazem os jogadores de futebol e outros esportes é uma habilidade da inteligência corporal-cinestésica. Além dos esportistas também temos os dançarinos, artistas, cirurgiões, escultores que utilizam cadeias de raciocínios para executar seus movimentos de forma concisa. Ainda podem agregar, nas situações, objetivos para completar a resolução da atividade (ANTUNES, 2006, p. 112).

Provavelmente, a inteligência lógico-matemática é uma das mais difundidas e respeitadas em nossa cultura, juntamente com a inteligência lingüística. Pessoas que possuem

as características dessa inteligência são, normalmente, mais respeitadas. Nogueira (2004, p. 27) sintetiza da seguinte forma:

> Competência em desenvolver e/ou acompanhar cadeias de raciocínios, resolver problemas lógicos e lidar bem com cálculos e números, normalmente verificadas em matemáticos, engenheiros, físicos, etc. Porém, não é necessariamente uma competência apenas existente nos profissionais que escolheram a área de exatas. Como bom exemplo disto, podemos mencionar os advogados, principalmente os de defesa, que criam uma seqüência tão lógica de fatos e acontecimentos, que normalmente acabam por defender e absolver criminosos que notoriamente cometeram o delito, porém o mecanismo criado por sua defesa torna-se tão lógico, que os jurados não enxergam outra saída a não ser o perdão.

Resolver problemas, charadas, efetuar cálculos, trabalhar com hipóteses são algumas das habilidades para a inteligência lógico-matemática que têm destaque nas profissões de cientistas, matemáticos, engenheiros, programadores, arquitetos, entre outros.

E juntamente com a inteligência lógico-matemática, a inteligência lingüística fecha o ciclo dos famosos testes de QI criados por Binet, formando assim as habilidades mais tradicionais conhecidas. Gardner (1995, p.25) descreve a inteligência lingüística:

> O dom da linguagem é universal, e seu desenvolvimento nas crianças é surpreendentemente constante em todas as culturas. Mesmo nas populações surdas, em que uma linguagem manual de sinais não é explicitamente ensinada, as crianças freqüentemente "inventam" sua própria linguagem manual e a utilizam secretamente. Dessa forma, nós vemos como uma inteligência pode operar independentemente de uma específica modalidade de input ou de um canal de output.

Na inteligência lingüística, o uso correto da forma de se expressar é uma das características principais, além da facilidade no uso de vocabulários, tanto na forma escrita como na forma oral. Escritores, advogados, poetas, oradores, políticos, vendedores, publicitários são alguns dos exemplos de profissões que têm domínio dessa inteligência.

Imaginem a seguinte situação descrita por Nogueira (2004, p. 29):

> Um arquiteto, ao sentar em frente à sua prancheta, desenha a terceira sala do lado esquerdo do elevador, localizada no 28º andar de um prédio. Na sala, será colocado um conduíte na parte frontal, esquerda e inferior, tendo como referência a porta de entrada.

A forma de compreender e visualizar essas informações são características da inteligência espacial que também está relacionada à percepção de formas de objetos;

movimentar-se em uma cidade nunca visitada apenas consultando um mapa, recriar desenhos usando a memória e recriar movimentos são características dessa inteligência que normalmente é apresentada em pilotos, cirurgiões, motoristas, pintores, escultores, entre outros.

A habilidade que uma pessoa tem para se relacionar com outras pessoas, compreender e perceber o humor, o sentimento, a emoção é característica da inteligência interpessoal, que também engloba a forma de organizar trabalhos em grupo. Segundo Gardner (1995, p. 27), é possível obter avanços dessa inteligência até a fase adulta:

> A inteligência interpessoal está baseada numa capacidade nuclear de perceber distinções entre os outros, em especial, contrastes em seus estados de ânimo, temperamentos, motivações e intenções. Em formas mais avançadas, essa inteligência permite que um adulto experiente perceba as intenções e desejos de outras pessoas, mesmo que elas os escondam.

Normalmente essa inteligência é marcante em líderes comunitários, políticos com alto índice de popularidade, professores, ativistas, negociadores, líderes religiosos, entre outros (ABREU-E-LIMA, 2006, p. 121)

Apontando para o eu, a inteligência intrapessoal é a capacidade que o indivíduo tem em se conhecer melhor, saber controlar suas emoções, sentimentos, projetos, falhas, entre outros. Abreu-e-Lima (2006) sintetiza:

> Ter um modelo mental de quem são como pessoas, desenhar projetos pessoais para curto, médio e longo prazos; reconhecer as diferentes emoções sentidas e vividas, suas causas e conseqüências, ter autoconhecimento, refletir, articular esse conhecimento por intermédio de outras inteligências de forma artística: poesia (lingüística), pintura (espacial e corporal-cinestésica), música (musical); utilizar esse autoconhecimento para atingir objetivos pessoais.

Os profissionais que se destacam nessa inteligência são terapeutas, poetas, oradores motivacionais, psicólogos, artistas, ativistas, músicos, filósofos, líderes espirituais, entre outros.

A última inteligência descoberta por Gardner foi a inteligência naturalista que consiste na capacidade de identificar e compreender formas e padrões na natureza. Saber observar, reconhecer padrões, classificar, categorizar e colecionar são algumas das habilidades destacadas nessa inteligência. Os profissionais que se destacam nessa linha são os

naturalistas, fazendeiros, caçadores, ecologistas, biólogos, paisagistas entre outros (ABREU-E-LIMA, 2006, p. 122).

A base dos estudos das inteligências múltiplas realizada por Gardner são os testes empíricos e os quais apontam para o cruzamento de várias inteligências em graus diferenciados para o resultado satisfatório de uma profissão, conforme teoriza Gardner (1995, p. 30):

> Na medida em que quase todos os papéis culturais exigem várias inteligências, torna-se importante considerar os indivíduos como uma coleção de aptidões, e não como tendo uma única faculdade de solucionar problemas que pode ser medida diretamente por meio de testes de papel e lápis. [...] Assim é de suprema importância avaliar a combinação particular de capacidades que pode destinar o indivíduo para uma determinada posição vocacional ou ocupação.

Contudo, é necessário saber utilizar de forma correta essa rota alternativa baseada nas inteligências múltiplas. Não existe uma receita pronta ou um pó mágico que basta aplicar e irá funcionar. O suporte terá de procurar os caminhos corretos para obter sucesso. Gardner (1995, p. 36) resume:

> Finalmente, nosso mundo está cheio de problemas; para termos a chance de resolvê-los, precisamos utilizar da melhor forma possível as inteligências que possuímos. Talvez um primeiro passo importante seja o de reconhecer a pluralidade das inteligências e as muitas maneiras pelas quais os seres humanos podem apresentá-las.

Essa rota alternativa apresenta novos conceitos e põe o profissional de administração de segurança de redes em um novo campo de atuação: para administrar o elo mais fraco de sua corrente, terá de trabalhar sua interdisciplinaridade, ou seja, somente seus conhecimentos técnicos não serão suficientes para atuar de forma direta e minimizar um dos maiores problemas enfrentados atualmente.

Nogueira (2004, p. 15) descreve um breve panorama do mercado de trabalho e as exigências para a contratação de um profissional:

> Muito se exige desse novo profissional, por exemplo, fluência em alguns idiomas, domínio das ferramentas básicas de informática, habilidade de comunicação, liderança, criatividade, facilidade de relacionamento com pessoas e mais dezenas de outras habilidades e competências.

Atualmente, as exigências do mercado de trabalho, para um profissional, vão além dos conhecimentos adquiridos nos anos de graduação e/ou cursos técnicos. Para ser um bom profissional, é preciso ter um espectro de competências desenvolvidas, além de saber aplicá-las da forma correta.

3.6 PENSAMENTO SISTÊMICO E VISÃO HOLÍSTICA

O pensamento sistêmico é definido por Nogueira (2000, p. 48) como uma forma que o indivíduo enxerga os problemas dos outros de forma abrangente. Em uma empresa esse pensamento é extremamente necessário, pois a interconexão dos departamentos é cada vez maior.

> Um profissional com visão sistêmica nunca vai responder: "isto não é da minha área" – "não sou o responsável por isso" – "não posso ajudar, pois não me compete", etc. Esse profissional terá competência para resolver o problema, ou no mínimo encaminhá-lo da melhor forma a quem de direito, dando pelo menos um destino à resolução de um determinado problema.

Mas é preciso mais que enxergar os problemas de outro departamento, em uma empresa, é preciso saber como atuar na resolução desses problemas, ter uma visão globalizada e sintetizar os fragmentos de forma abrangente. Segundo Crema (1989, p. 68):

> O paradigma holístico desenvolveu-se a partir de uma concepção sistêmica, nele subjacente. Em suma, essa abordagem consiste na consideração de que todos os fenômenos ou eventos se interligam e se inter-relacionam de uma forma global; tudo é interdependente.

Apresentar aos usuários e tecnólogos de uma empresa os conceitos do pensamento sistêmico e da visão holística pode desenvolver resultados satisfatórios na resolução de problemas e facilitar a comunicação entre os departamentos.

4 ANÁLISE E DISCUSSÃO DE DADOS

Computadores fazem arte
Artistas fazem dinheiro
Cientistas criam o novo
Artistas pegam carona
Pesquisadores avançam
Artistas levam a fama.
Fred Zero 4, mundo livre s/a

O principal objetivo deste trabalho é identificar as fragilidades mais comuns nos procedimentos de segurança em uma rede local de computadores de uma empresa tendo como foco principal o fator humano. Baseados nessa prerrogativa, analisamos os documentos que dão o cerne para as orientações de segurança na rede de computadores. Após a análise, desenvolvemos um questionário fechado que foi aplicado nos funcionários da rede de computadores, exceto os que trabalham no departamento delta, que são os funcionários do suporte. Após a aplicação do questionário, executamos a tabulação dos dados e selecionamos sete usuários para um bate-papo individual, em que foram esclarecidos alguns pontos que apresentaram divergências nos questionários fechados. Após a análise do questionário fechado e das entrevistas, elaboramos um roteiro com os pontos conflitantes entre os funcionários e fizemos uma entrevista, no formato de bate-papo, com a equipe do departamento delta. Por fim, foram feitas algumas notas de campo relatando os pontos importantes que foram detectados no momento da aplicação do questionário fechado e no decorrer da pesquisa.

4.1 DOCUMENTOS DA EMPRESA

A preocupação com a segurança de rede de computadores, no último ano, foi um dos pontos de maior relevância para a empresa. Além da Circular 2007 e do Termo de Compromisso apresentados aos usuários da rede, está em fase de estudos o documento que constituirá as Políticas de Segurança da Informação da Empresa. Também está sendo executado um monitoramento para verificar o cumprimento dos documentos vigentes.

4.1.1 CIRCULAR 2007

A Circular 2007 informa aos usuários que, a partir da data de publicação, serão implementados critérios para utilização da Internet e acesso a rede de computadores. O documento tem cinco tópicos e apresenta:

- o termo de compromisso que foi encaminhado aos usuários para conhecimento e cumprimento; esse termo será analisado a seguir;

- as contas de e-mail, acesso aos sistemas da empresa e login à rede de computadores serão de responsabilidade do departamento alfa, que é responsável pelo processo de contratação e demissão de funcionários. Essa medida visa ao controle preciso na criação e bloqueio dos usuários, pois esse departamento é quem faz o controle de contratações e demissões;

- após a demissão do funcionário não será permitido o uso do e-mail institucional, nem o redirecionamento, para um e-mail particular. Essa medida tem por objetivo eliminar o uso indevido do e-mail coorporativo por um funcionário que não faz parte da empresa;

- as senhas utilizadas pelos usuários, em todos os sistemas e na rede, deverão ser mantidas em sigilo e o usuário será responsabilizado pelo uso indevido;

- por fim, o último item informa que o departamento delta, que é responsável pelo suporte da rede, fará uma vistoria nas estações de trabalho com o intuito de aplicar as normas estabelecidas no termo de compromisso em um período determinado pelo departamento alfa. Após esse período serão aplicadas as penalidades de acordo com o termo. Esse ponto prepara os usuários para terem conhecimento do termo de compromisso.

4.1.2 TERMO DE COMPROMISSO

O documento tem como teor principal as normas para utilização dos recursos da rede de computadores, acesso a Internet, utilização do e-mail corporativo e declarações de responsabilidades sobre os itens descritos. Essas normas estão divididas em:

- declaração de que o usuário não utilizará a rede de computadores para qualquer finalidade ilegal ou proibida, respeitando todas as leis e regulamentos locais, estaduais, federais e internacionais. O usuário será responsabilizado por qualquer ação ilegal que for comprovada, pela utilização de sua senha de acesso. A empresa informa, no final do termo,

que as estações de trabalho são monitoradas, e dessa forma, é possível comprovar qualquer tipo de irregularidade. Ainda no final do termo, o usuário é informado de que qualquer falta das normas descritas no documento consistirá em falta grave e pode resultar na ruptura do contrato de trabalho por justa causa;

- sites de jogos on-line, rádio on-line, bate-papo de qualquer espécie, sites de relacionamento e sites de conteúdo pornográfico ou discriminatório têm acesso expressamente proibido;

- o e-mail da empresa não pode ser utilizado:

1) para proveito pessoal, cadastros para recebimento de pesquisas, concursos, pirâmides, correntes, lixo eletrônico, spam ou quaisquer mensagens periódicas ou não-solicitadas como comerciais ou não;
2) difamar, abusar, perturbar a tranqüilidade alheia, perseguir, ameaçar ou de qualquer forma violar direitos de terceiros;
3) publicar, distribuir ou divulgar quaisquer matérias ou informações inadequadas, profanas, difamatórias, transgressoras, obscenas, indecentes ou ilegais;
4) anunciar ou oferecer para venda ou compra de bens ou serviços, com qualquer finalidade comercial;
5) transmitir ou carregar qualquer material que contenha vírus, "cavalos-de-tróia", "bombas-relógio" ou quaisquer programas prejudiciais ou nocivos;
6) interferir ou desordenar redes conectadas à rede de computadores da empresa ou violar regulamentos, normas ou procedimentos.

Ainda sobre e-mails, o termo solicita a autorização ao usuário para acesso aos e-mails recebidos e enviados que estão armazenados no Outlook Express[10] e o monitoramento da estação de trabalho;

- para utilização da rede de computadores o termo define:

1) os drives de rede devem ser utilizados apenas para gravação de arquivos inerentes ao trabalho, sendo proibido a gravação de qualquer tipo de arquivo de cunho pessoal;
2) nas estações de trabalho é proibida a instalação de qualquer tipo programa sem o conhecimento e autorização do departamento delta;
3) O usuário que mais utiliza a estação de trabalho é responsável em informar ao departamento delta sobre qualquer anormalidade na estação;

[10] Outlook Express é um programa de gerenciamento de e-mails que normalmente fica instalado na estação de trabalho.

4) mudanças na localização da estação, instalação ou qualquer tipo de ocorrência que influencie no funcionamento dos recursos da estação devem ser informadas ao departamento delta.

Fica demonstrado na análise do termo de compromisso que a empresa tenta se resguardar de eventuais problemas que os usuários possam cometer na utilização das ferramentas de trabalho. A nota de campo do dia 18/08/2007 mostra que o documento foi apresentado aos usuários individualmente e não houve nenhuma palestra para apresentação e esclarecimento de dúvidas por parte dos funcionários.

Alguns pontos do Termo no Compromisso apresentaram divergências e estão sendo analisados pelo departamento alfa e pelo departamento delta e terão melhorias na implantação das políticas de segurança.

4.1.3 POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO DA EMPRESA

O documento está em fase de elaboração pelo departamento delta e consiste em uma poderosa documentação a implantação das políticas de segurança da empresa. Dividido em duas seções, temos na primeira seção os elementos comuns da política, divididos em introdução, termos e definições e estrutura da política; e na segunda seção, as políticas, divididas em políticas de segurança, segurança organizacional, controle e classificação dos ativos de informação, segurança pessoal, segurança física e ambiental, gestão das operações e comunicações, controle de acesso e desenvolvimento e manutenção de sistemas. A minuta do documento está no anexo 3. Por ser uma versão inicial e passível de alterações, o documento não foi analisado, apenas analisamos os procedimentos para elaboração.

Em nota de campo do dia 23 de agosto de 2007 mostram a ausência de contribuições dos usuários e outros departamentos na elaboração das políticas de segurança, que estavam em fase de desenvolvimento até o momento desta análise. Principalmente, as contribuições do departamento alfa, que é responsável pelo gerenciamento dos recursos humanos da empresa. Contudo, após as experiências com a implantação do Termo de Compromisso existe uma pré-disposição dos departamentos alfa e delta de trabalhar em conjunto as políticas de segurança.

4.2 QUESTIONÁRIO FECHADO

Após a análise dos documentos da empresas, elaboramos um questionário fechado, embasado com as informações contidas na documentação e nas notas de campo. O propósito do questionário foi identificar, de forma objetiva, os conhecimentos técnicos e as competências profissionais do corpo funcional, o conhecimento das normas de segurança implantadas pela empresa e as habilidades das competências profissionais com foco nas inteligências múltiplas de Gardner. Os questionários foram aplicados em todos os funcionários presentes à empresa e utilizam a rede de computadores, que corresponde a 87 pessoas e 99% deles foram respondidos. Com bases nas informações recolhidas, foram criados gráficos para melhor apresentação dos resultados.

4.2.1 FORMAÇÃO E ATUALIZAÇÃO PROFISSIONAL

Para identificar a formação acadêmica e a atualização profissional dos funcionários da empresa, foram elaboradas duas questões. Nessas questões também foram analisados os investimentos da empresa nos cursos de atualização profissional.

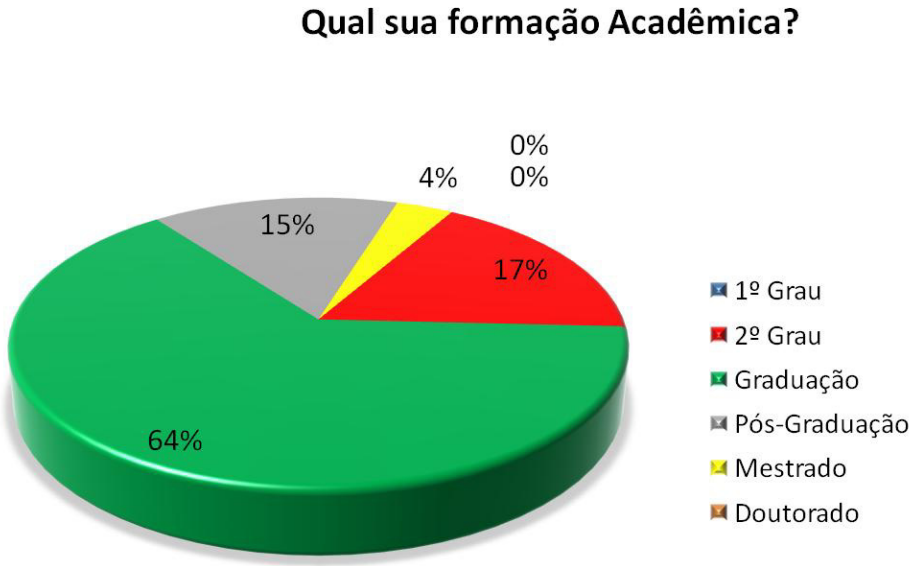

Gráfico 1 – Formação acadêmica

O gráfico 1 mostra que mais de 80% dos funcionários são graduados; desses, mais de 20% têm pós-graduação em suas áreas de atuação. Esses números demonstram que o corpo funcional da empresa está muito bem qualificado.

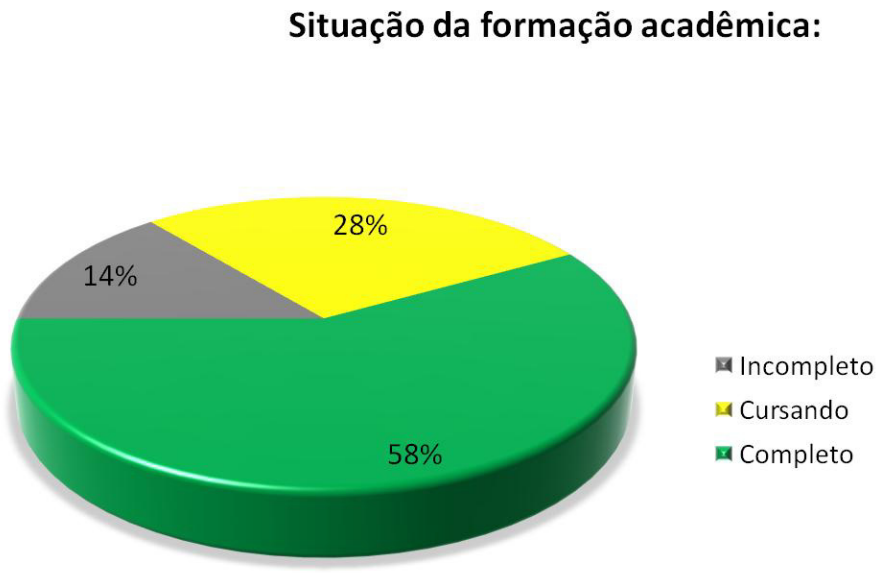

Gráfico 2 – Situação da formação acadêmica

A fim de saber qual o andamento da formação acadêmica dos funcionários, solicitamos que informassem no questionário a situação. Apenas 14% dos funcionários estão com os cursos incompletos, 58% já concluíram e 28% estão cursando conforme mostra o gráfico 2.

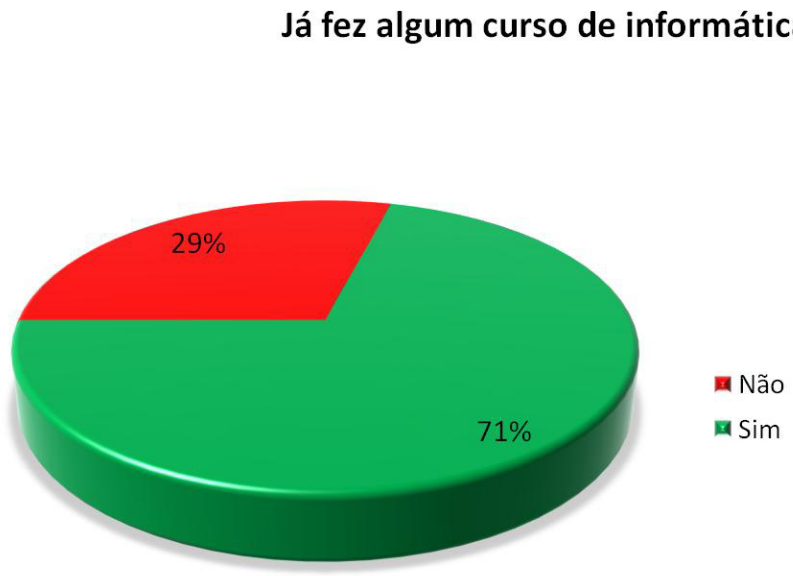

Gráfico 3 – Curso de informática

Além da formação acadêmica, perguntamos aos funcionários se já fizeram algum curso na área de informática e mais de 70% responderam que sim como indica o gráfico 3.

Gráfico 4 – Curso de informática financiado pela empresa

Para os que responderam sim no gráfico 3, perguntamos se os cursos de informática foram financiados pela empresa e apenas 38% responderam afirmativamente. Os demais, 68%, arcaram com os custos dos cursos de informática.

Após a leitura desses dados, fica evidenciado que existe uma preocupação do corpo funcional em se manter atualizado na área de informática. Os dados também mostram que o investimento da empresa na atualização profissional na área de informática está em apenas 38%, conforme demonstrado no gráfico 4.

4.2.2 CONHECIMENTO TÉCNICO EM INFORMÁTICA

Depois de traçar um perfil básico dos usuários da rede de computadores da empresa, analisamos os conhecimentos técnicos em informática. Perguntamos como o trabalho está relacionado com a informática, sobre as políticas de segurança da empresa, a realização de treinamentos sobre segurança. Por fim, consideramos dois cenários distintos, porém relacionados ao recebimento de e-mails, que, atualmente, é considerado uma das principais

portas de entradas de ameaças à segurança da rede de computadores como indica Fortes (2007, p. 16).

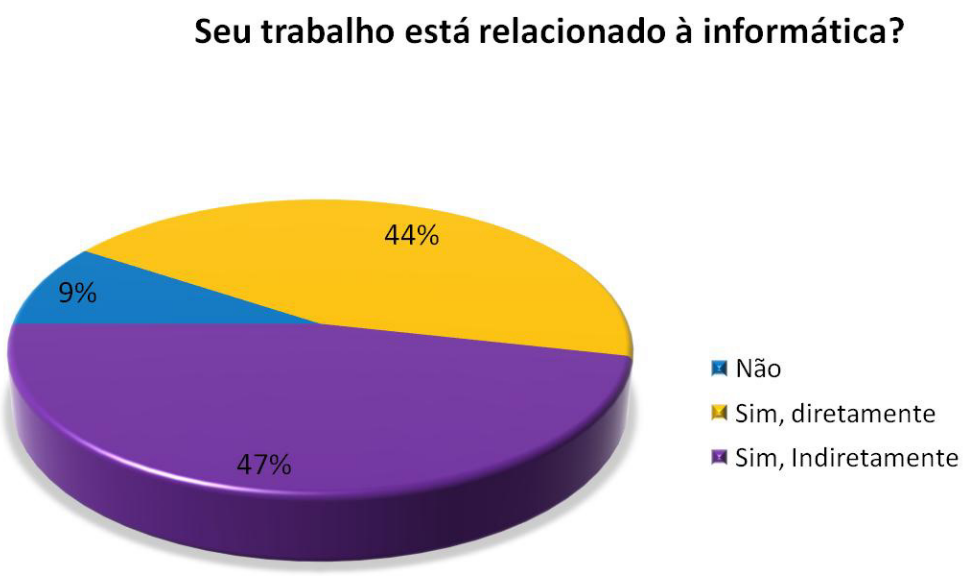

Gráfico 5 – Trabalho relacionado à informática

Questionamos os usuários da rede de computadores sobre qual a relação de seus trabalhos com a informática e 44% responderam que estão diretamente relacionados. Outros 47% responderam que estão indiretamente relacionados, como indica o gráfico 5. É importante ressaltar que o questionário não foi aplicado na equipe delta, que é responsável pela rede de computadores e trabalha diretamente com informática.

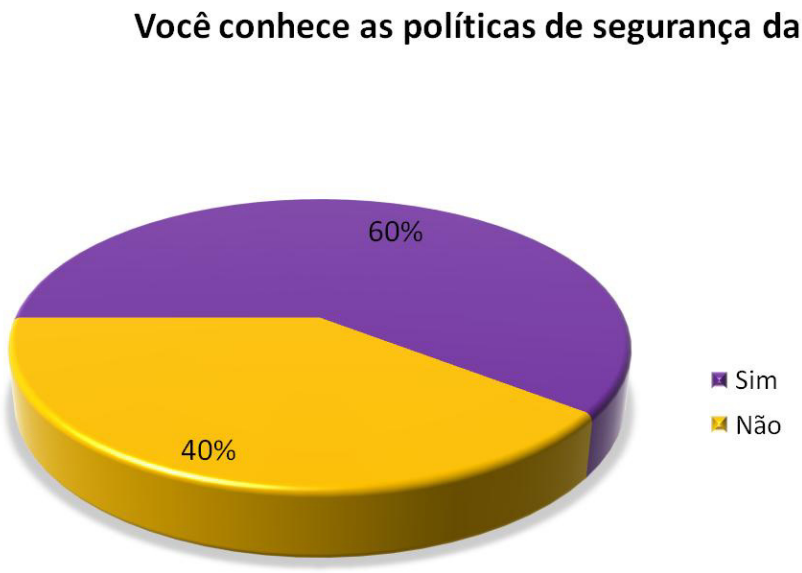

Gráfico 6 – Políticas de segurança

Conforme exposto neste estudo, as Políticas de Segurança da Empresa ainda estão em fase de estudos e, portanto, não formam implantadas. Perguntamos aos funcionários se conhecem as políticas de segurança e mais da metade, 60%, respondeu que sim e 40% respondeu que não, conforme mostra o gráfico 6.

Como o e-mail é o foco principal nas questões de segurança, perguntamos aos usuários como ele utiliza a conta de e-mail particular.

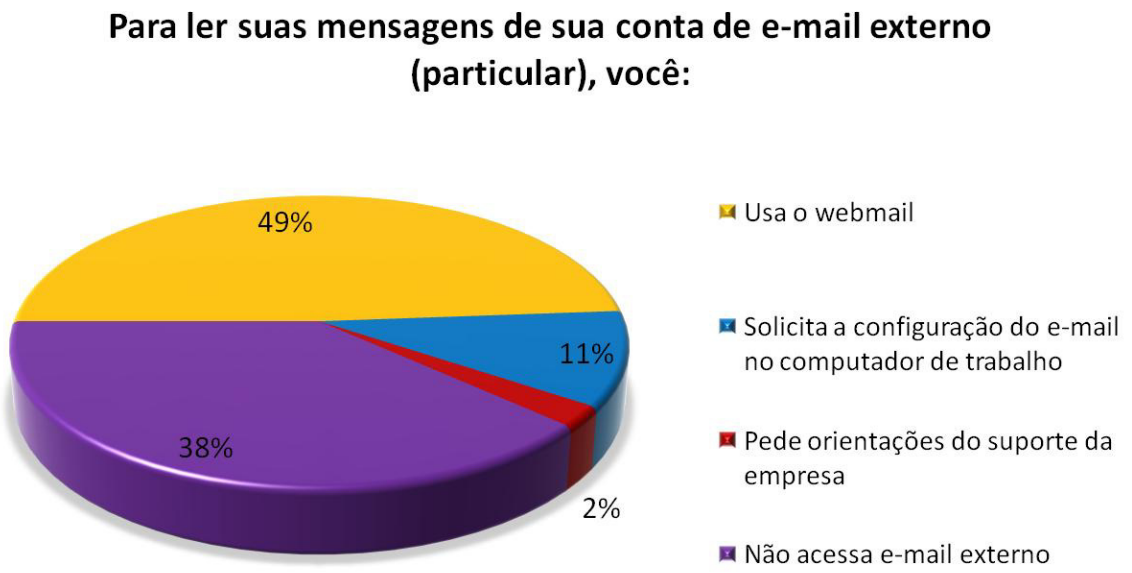

Gráfico 7 – E-mail externo

Como ilustra o gráfico 7, quase 50% dos funcionários que utilizam o e-mail particular acessam por webmail, 11% informaram que solicitam a configuração do e-mail no computador de trabalho e 2% solicitam orientações do suporte. Os outros 38% dos usuários informaram que não acessam e-mail externo.

Em nota de campo do dia 9/10/07, foi relatado que os usuários do departamento ômega questionaram o pesquisador sobre esta pergunta 8, que foi fonte do gráfico 7:

> Nota de campo 09/10/07: Na aplicação do questionário no departamento ômega, muitos usuários questionaram o motivo da pergunta 8, para ler suas mensagens de sua conta de e-mail externo (particular), você:
> Para não influenciar nas respostas limitamos a responder que não havia nada de especial. Os usuários informaram que não acessavam nenhum tipo de site, somente da empresa. Ao término da aplicação do questionário, relatei a situação ao suporte que informou que os usuários do departamento ômega tiveram o acesso ao alguns sites bloqueados.

Podemos verificar que o motivo do questionamento foi porque alguns usuários já tinham o acesso de sites restrito ou monitorado pelo departamento delta. Dessa forma a única opção que teriam para responder a pergunta é que não acessa e-mail externo.

Gráfico 8 – Treinamento sobre segurança promovido pela empresa

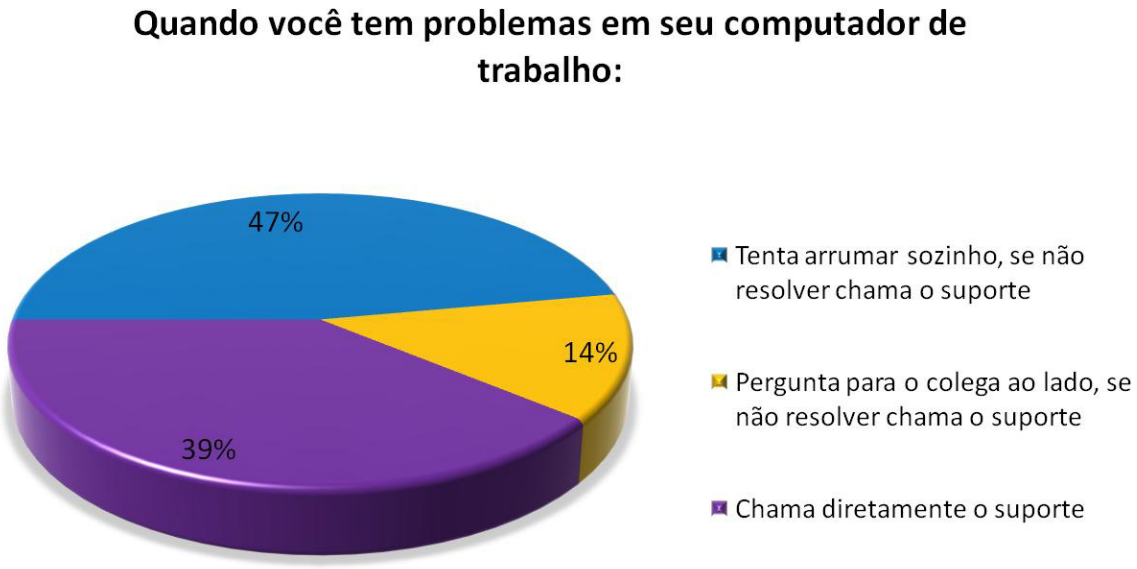

Gráfico 9 – Problemas no computador

Para identificar as formas de treinamento que a empresa oferece aos usuários, perguntamos se já haviam recebido algum treinamento sobre segurança promovido pela

empresa e 91% dos usuários responderam que não. Apenas 9% afirmaram ter recebido algum tipo de treinamento sobre segurança conforme mostra o gráfico 8.

Identificamos a forma com que o usuário reage diante de um problema em seu computador de trabalho. “Tenta arrumar sozinho” foi marcado por 47% dos funcionários, 14% perguntam para um colega ao lado e 39% chamam diretamente o suporte, conforme gráfico 9.

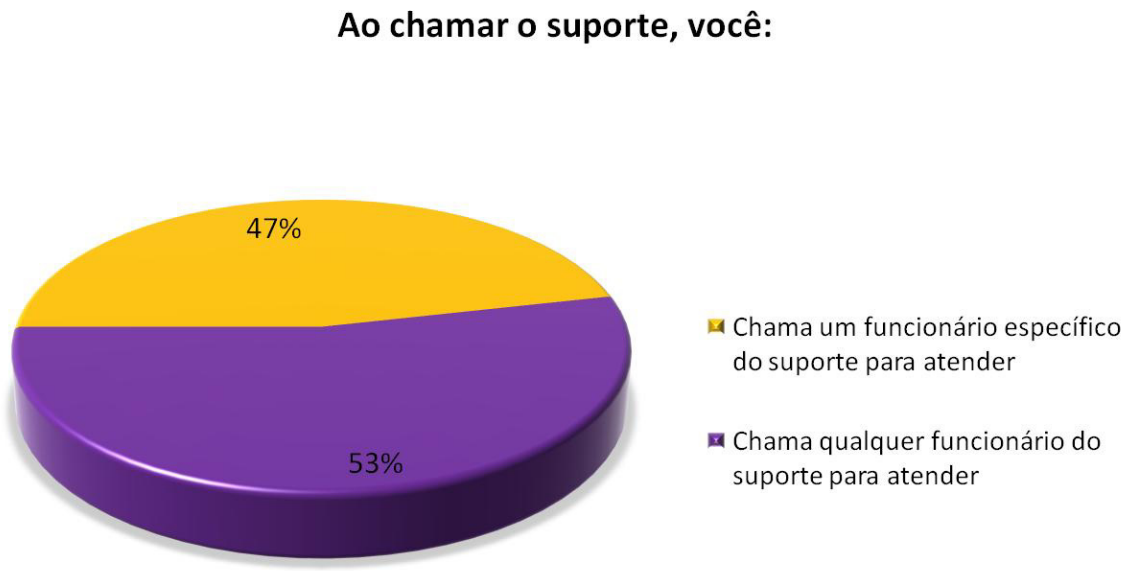

Gráfico 10 – Relacionamento com o suporte

Ao chamar o suporte, identificamos que 47% chamam um funcionário específico e 53% chamam qualquer funcionário como mostra o gráfico 10. O intuito dessa pergunta é identificar e documentar a preferência dos usuários por determinados tecnólogos do suporte. Nas notas de campo da semana de 01/10/07 à 05/10/07, foi observado que alguns usuários solicitavam sempre o mesmo tecnólogo para resolver seus problemas. Existe a possibilidade de o tecnólogo acionado ter as inteligências, lingüística e interpessoal desenvolvida, mas é necessário o acompanhamento e documentação das habilidades de todo o departamento delta para verificação das inteligências múltiplas.

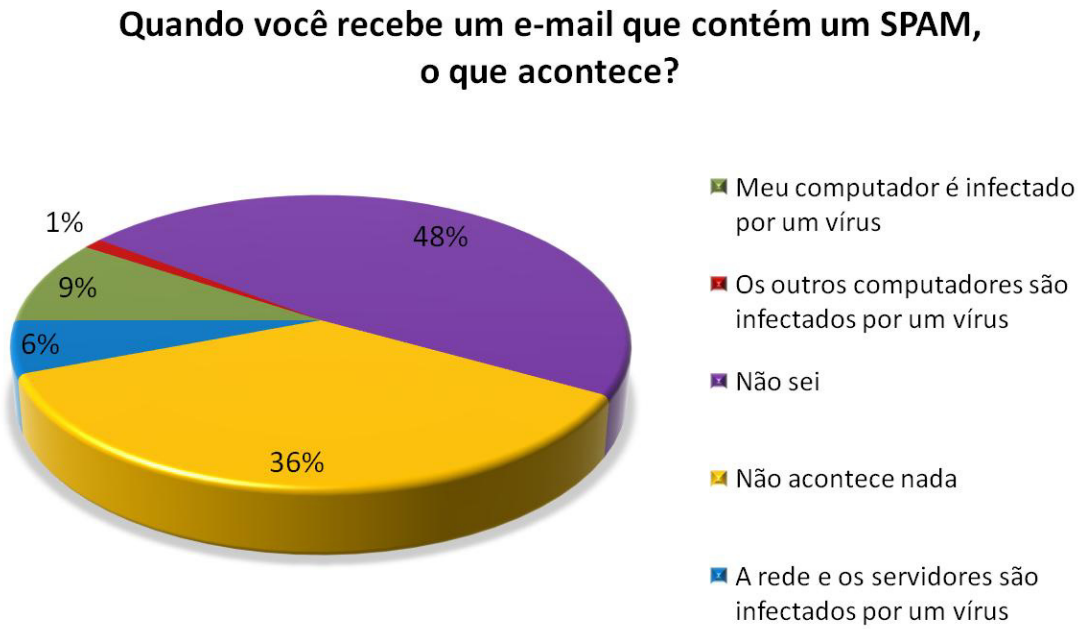

Gráfico 11 – SPAM

Analisando a questão de e-mails, colocamos no primeiro cenário, o recebimento de um e-mail que contém um SPAM pelo usuário e perguntamos o que acontece quando abre o e-mail. Apenas 36% dos usuários responderam que não acontece nada. A maior parte dos funcionários, 48%, responderam que não sabem e 16% responderam que o computador de trabalho, a rede ou os servidores são infectados por um vírus como indica o gráfico 11.

Como apenas 36% dos usuários identificaram de forma correta um SPAM, selecionamos os dados dos outros 64% e geramos gráficos para identificar melhor estes usuários.

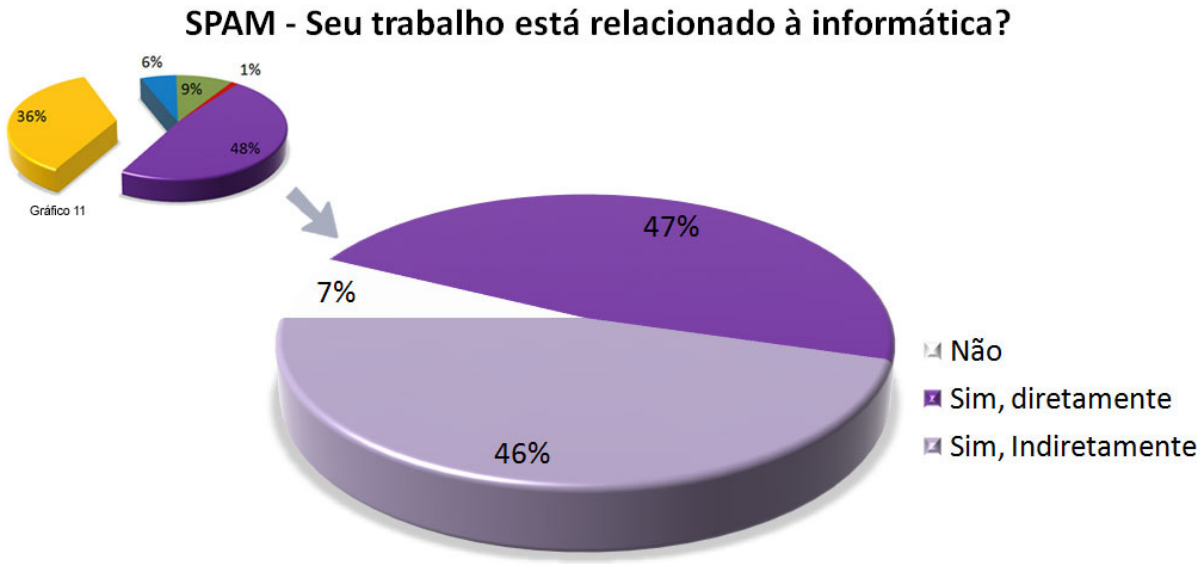

Gráfico 12 – SPAM x Trabalho relacionado à informática

Primeiro, verificamos qual o relacionamento do trabalho com a informática e 47% informaram que têm um relacionamento direto, como mostra o gráfico 12. Esse número mostra que os usuários que não identificaram de forma correta um SPAM e consideram seu trabalho diretamente relacionado à informática é maior se comparado ao grupo geral, que é de 44% como indica o gráfico 5.

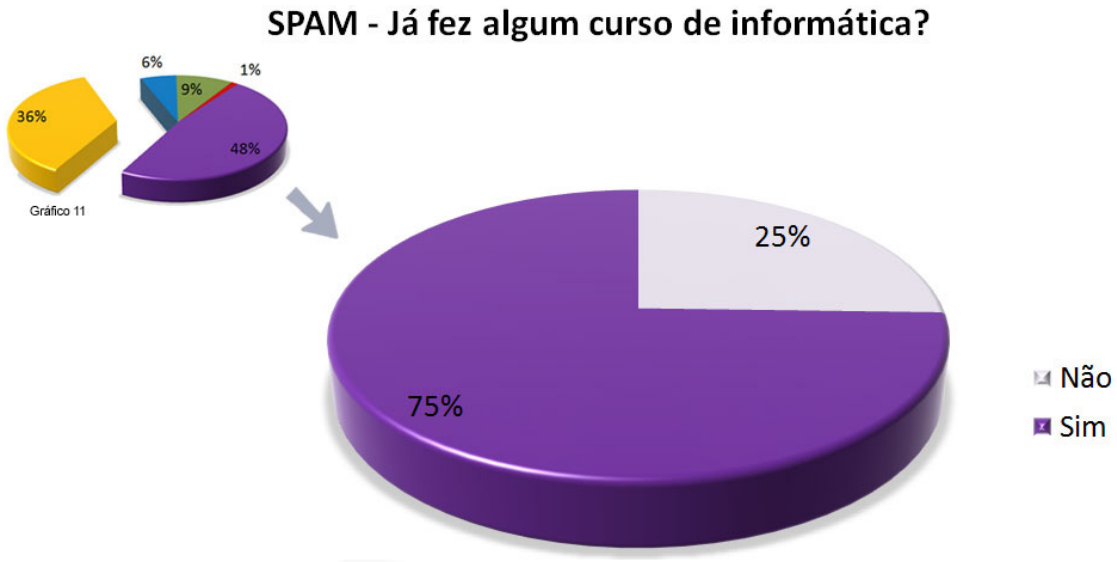

Gráfico 13 – SPAM x Curso de informática

Segundo, analisamos se esses usuários já fizeram algum curso de informática. 25% responderam que não, mas a maioria, 75%, respondeu que sim, conforme exposto no gráfico 13.

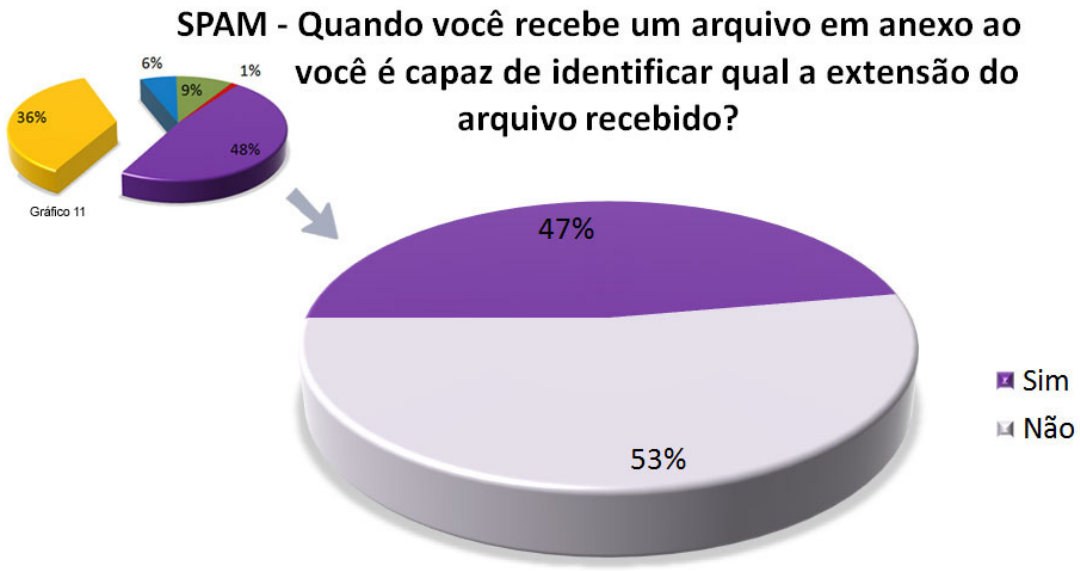

Gráfico 14 – SPAM x Identificação da extensão de arquivo anexo ao e-mail

Terceiro, buscamos as respostas sobre a identificação da extensão de um arquivo recebido anexado a um e-mail. 47% responderam que são capazes de identificar a extensão do arquivo recebido. Mas 53%, mais da metade, não sabem identificar a extensão de um arquivo recebido por e-mail como demonstra o gráfico 14.

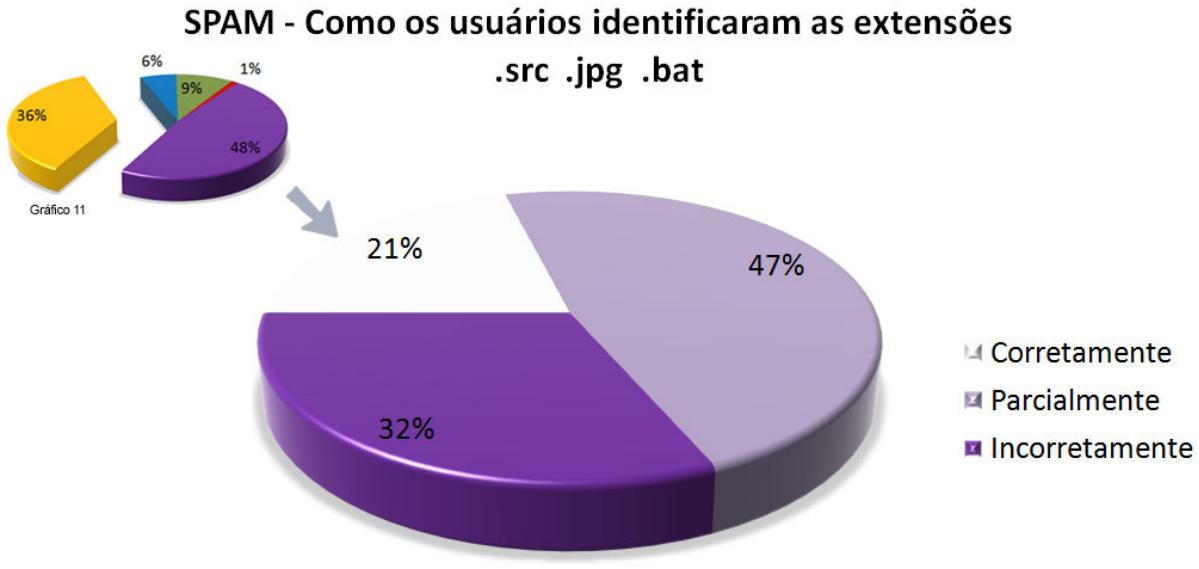

Gráfico 15 – SPAM x Extensão de arquivos recebidos por e-mail

Para finalizar essa análise do primeiro cenário, verificamos como se portaram os 47%, do gráfico 14, dos usuários que responderam que sabem identificar a extensão de um arquivo anexado e quais podem conter vírus. Apenas 21% dos usuários identificaram de forma correta e marcaram as extensões, .src[11] e .bat[12], como arquivos que podem conter vírus. 47% dos usuários identificaram parcialmente, ou seja, assinalaram apenas uma das opções corretas e 32% não conseguiram identificar corretamente as extensões, marcando a extensão .jpg[13], como mostra o gráfico 15.

Sabendo que um SPAM é apenas uma propaganda que chega na caixa de e-mails sem a autorização do usuário e que em alguns casos essa mensagem é utilizada para enviar um vírus, podemos dizer que existe uma confusão de conceitos e formas de visualização dos problemas referentes a segurança conforme demonstrado nos gráficos 11, 12, 13, 14 e 15.

No segundo cenário, perguntamos aos usuários se seriam capazes de identificar a extensão de um arquivo recebido como anexo ao e-mail. 42% disseram que não são capazes de identificar a extensão do arquivo recebido por e-mail. Mas a maioria, 56%, informou que sabe identificar a extensão do arquivo recebido como mostrar o gráfico 16.

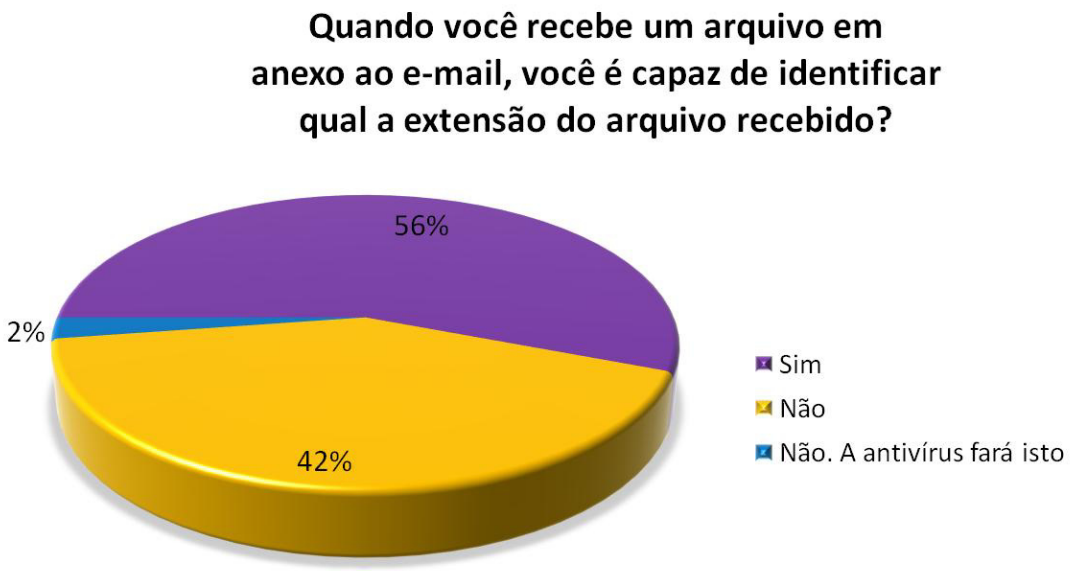

Gráfico 16 – Identificação da extensão de arquivo anexo ao e-mail

[11] SCR (SCReen saver), protetor de tela.
[12] BAT (Batch), arquivo de lote para execução de comandos.
[13] JPG ou JPEG (Joint Photographic Experts Group), arquivo de imagem .

Para os 56% que responderam que são capazes de identificar a extensão de um arquivo recebido por e-mail, informamos três opções de extensão de arquivos e pedimos que os usuários identificassem quais poderiam conter um vírus. Os opções foram: .scr que ficou com 36%, .jpg com 17% e .bat com 47% conforme mostra o gráfico 17 .

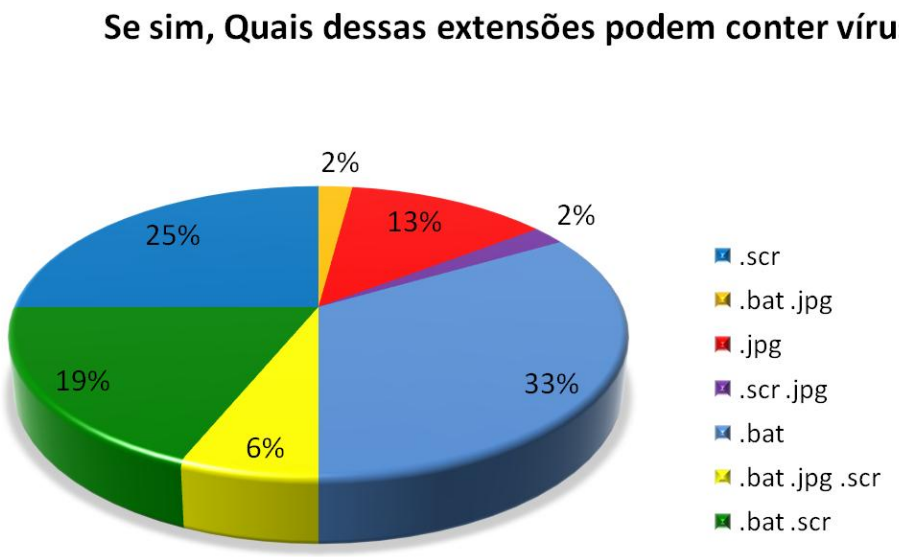

Gráfico 17 – Extensão de arquivos recebidos por e-mail

Analisando detalhadamente as respostas dessa questão, verificamos que apenas 19% dos usuários conseguiram identificar de forma totalmente correta as extensões que podem conter vírus. 54% apenas identificaram parcialmente, ou seja, marcaram apenas uma das opções corretamente e 27% dos usuários marcou incorretamente as opções como mostra o gráfico 14.

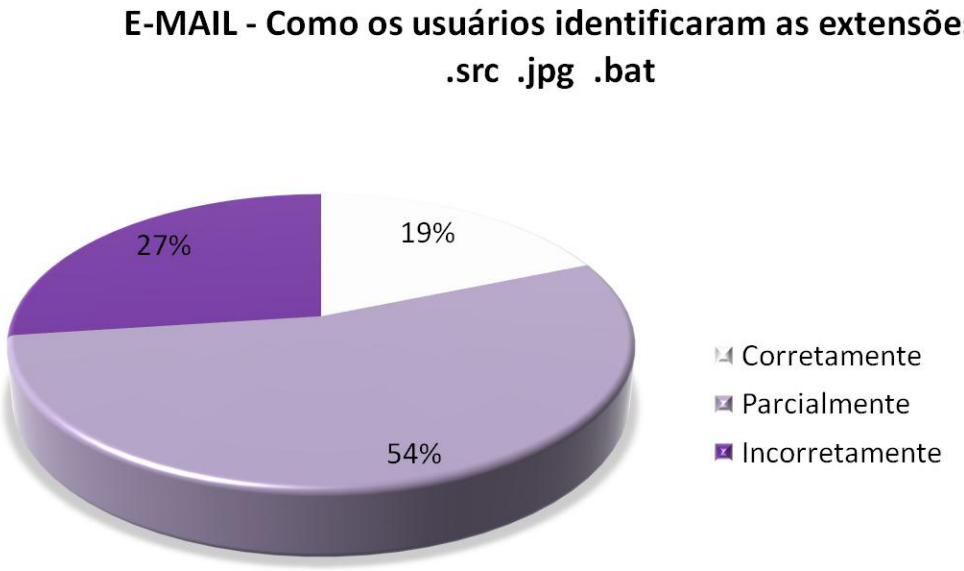

Gráfico 18 – E-MAIL x Identificação da extensão de arquivo anexo ao e-mail

Fazendo o cruzamento dos dados dos dois cenários que estão dispostos no gráfico 11 com os dados do gráfico 16, identificamos que apenas 16% dos funcionários conseguiram responder corretamente ao que é o SPAM e identificar corretamente as extensões dos arquivos recebidos. 45% dos que responderam corretamente o que é um SPAM identificaram parcialmente a extensão dos arquivos em anexo e 39% identificaram incorretamente conforme mostra o gráfico 19.

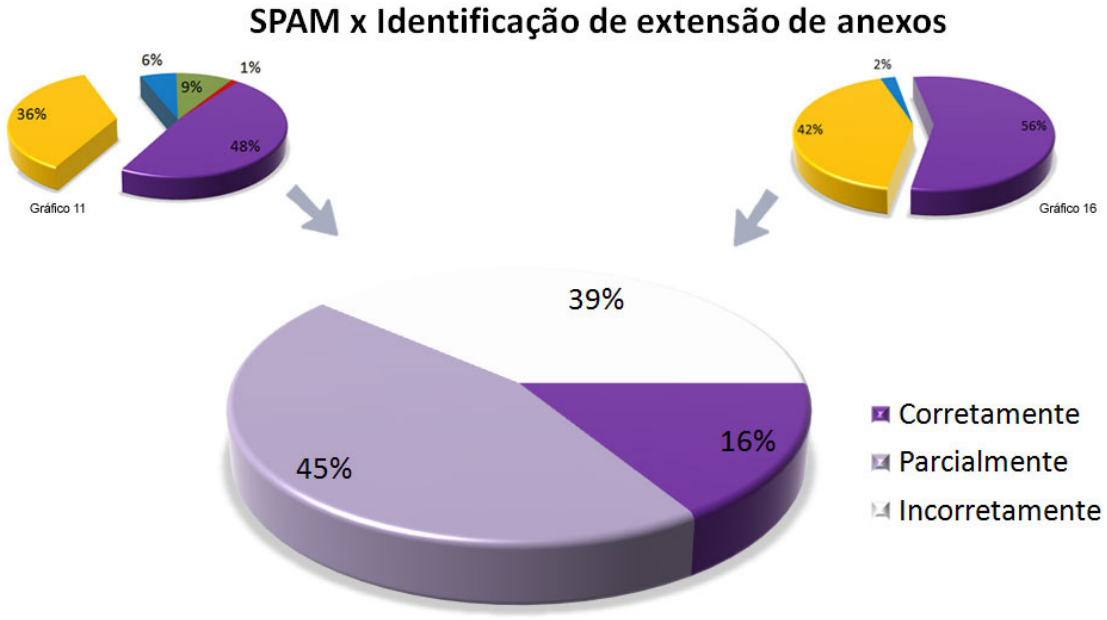

Gráfico 19 – SPAM x E-MAIL x Identificação da extensão de arquivo anexo ao e-mail

Com base nos dados do gráfico 19, fica evidente que a maior parte dos usuários da rede de computadores da empresa não está preparada para lidar com os problemas nos e-mails, e o suporte não oferece nenhum tipo de treinamento para os usuários.

4.2.3 HABILIDADES DAS COMPETÊNCIAS PROFISSIONAIS

Para identificar as habilidades dos usuários da rede de computadores da empresa perguntamos a faixa etária, a forma de aprendizagem, a forma de análise em grupo e as atividades que mais gosta de fazer.

No gráfico 20, temos as faixas etárias dos usuários da empresa. O maior número de usuários está na faixa de 31 a 40 anos, formando 41% do total. Em segundo vem a faixa de 21 a 30 anos, com 27%, seguida da faixa de 41 a 50 anos, com 16%. Abaixo de 20 anos temos 13% e, finalizando, com 3% do total a faixa de idade acima de 51 anos.

Segundo Antunes (2003, p. 105), existem diversas formas de trabalhar as inteligências múltiplas, uma dessas formas é trabalhar com atividades de acordo com a faixa etária. Neste sentido identificamos as faixas etárias dos usuários da rede de computadores, a saber: 41% têm idade entre 31 a 40 anos, 27% têm idade entre 21 a 30 anos, 16% têm idade entre 41 a 50 anos, 13% têm idade abaixo de 20 anos e apenas 3% têm idade acima de 51%, conforme mostra o' gráfico 20.

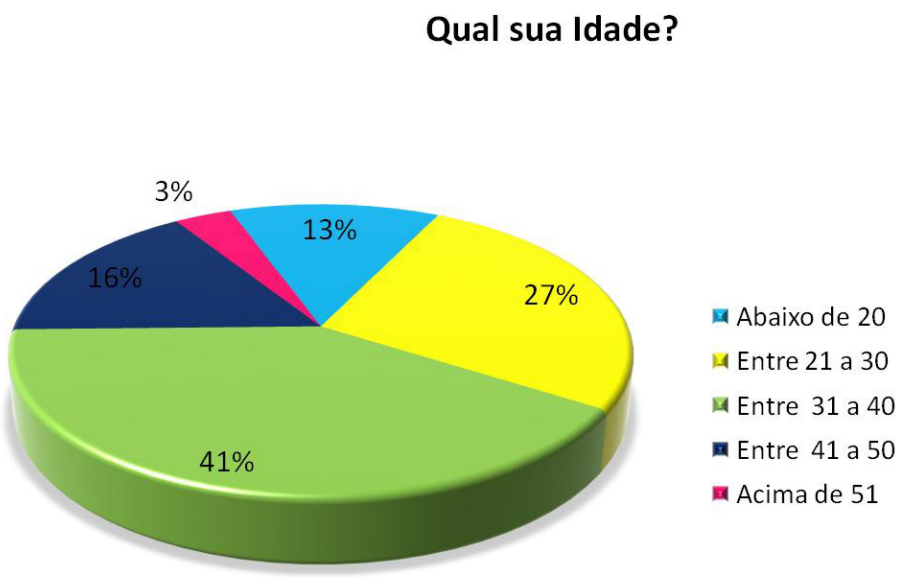

Gráfico 20 – Faixa Etária

Perguntamos qual o processo mais utilizado na impressão de um documento aberto do Microsoft Word[14] os usuários. Nas respostas incluímos uma opção cinestésica, que utiliza a tecla de atalho, CTRL + P, pelo teclado; uma opção espacial, que utiliza o desenho da impressora; uma opção lingüística, que utiliza a opção do menu ARQUIVO, IMPRIMIR e uma opção para acionar o suporte fazer a impressão. Com a identificação dessas opções, é possível identificar a maneira que cada usuário assimila a execução da maioria dos procedimentos usados no computador.

Foi detectado comportamento diferenciado em usuários com faixa etária abaixo de 20 anos na execução de tarefas relacionadas à tecnologia no período da pesquisa. Alguns usuários dessa faixa etária informaram que utilizam de forma moderada a impressão de documento, principalmente para leitura (gráfico 21). Questionados se eles não liam os documentos, informaram que preferiam ler no monitor conforme nota de campo do dia 03/10/07.

> Nota de campo 03/10/07: Alguns usuários do departamento ômega informaram que utilizam pouco a impressora (pergunta 7). Ao serem questionados, informaram que preferem ler os textos na tela do computador.

Baseados nesse comportamento elaboraram algumas perguntas, informais, aos usuários, conforme descrito em nota de campo do dia 04/10/07

> Nota de campo 04/10/07: Voltamos ao departamento ômega para conversar com os usuários sobre alguns procedimentos tecnológicos que utilizavam. Perguntamos como eles conversam com os amigos? Eles informaram que usam o MSN, o Orkut e em último caso o telefone. Perguntamos quando instalam um software novo lêem as instruções ou manuais? Eles informaram que na maioria dos casos não. É mais fácil e rápido aprender utilizando a ferramenta. Por fim, como fazem os trabalhos escolares? Eles informaram que utilizam a Internet como principal fonte de pesquisa e que quase nunca utilizam livros impressos, pois muitos podem ser encontrados na Internet.

Embora o tema descrito nas notas de campo não seja o foco deste trabalho, temos alguns indícios de comportamento diferenciado baseado na tecnologia e recomendamos para estudos futuros.

Analisando o gráfico 21, percebemos um equilíbrio na forma de utilização das opções de impressão disponíveis no questionário. 39% dos usuários informaram que

[14] Microsoft Word

selecionam com o mouse a opção do menu ARQUIVO, IMPRIMIR, 31% dos usuários disseram que utilizam a opção no teclado CTRL + P e 30% dos usuários clicam com o mouse no desenho da impressora. Nenhum usuário informou que aciona o suporte para impressão do documento.

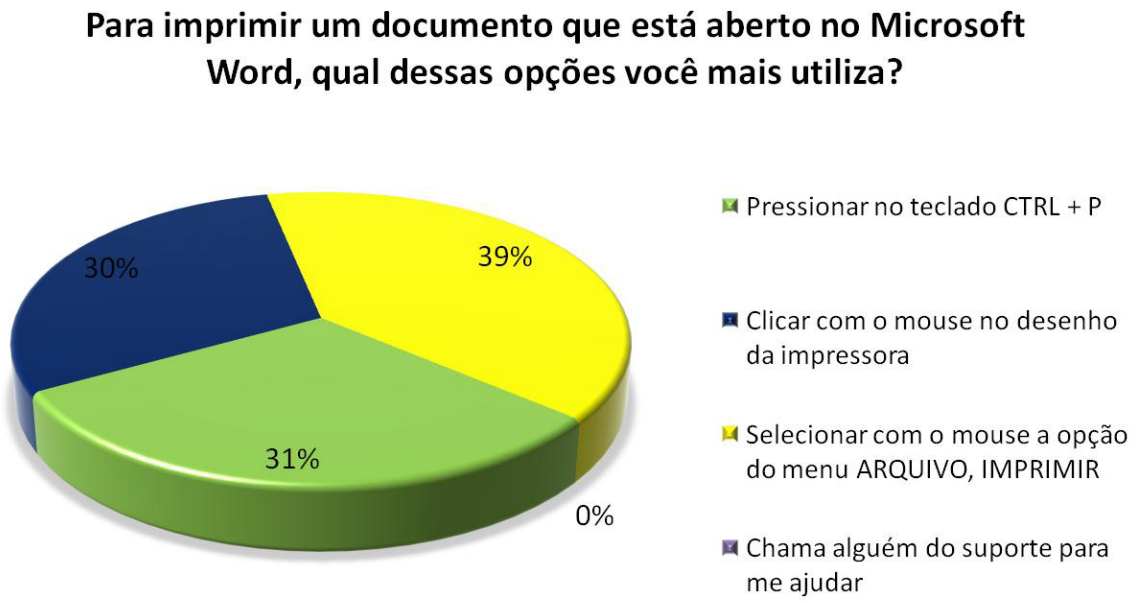

Gráfico 21 – Impressão de documentos

Outra análise que podemos ter, relacionado aos dados do gráfico 21, é a questão de segurança na impressão de documentos. 30% dos usuários utilizam a opção "clicar com o mouse no desenho da impressora". Sabendo-se que em um ambiente de rede as impressoras são localizadas em pontos estratégicos e de fácil acesso na empresa e são compartilhadas, ou seja, são utilizadas por vários usuários, ao clicar no desenho da impressora o software, normalmente, a impressão é enviada para a impressora que estiver configurada como padrão. É comum que o usuário mude a impressora padrão em determinadas situações e esqueça essa mudança depois. A conseqüência desse esquecimento é o desaparecimento de documentos conforme descrito em nota de campo do dia 10/10/07.

> Nota de campo 10/10/07: O departamento delta recebeu um chamado da usuária Deliades que solicitou a configuração da impressora, pois já havia mandado imprimir o documento três vezes e não saiu na sua impressora. Ao chegar à estação de trabalho da usuária, o suporte verificou que estava tudo funcionando e que as impressões foram mandadas para outra impressora. O problema que a impressora que estava selecionada era em outro departamento e ao clicar na impressora o software mandava para a

> impressora selecionada e não para impressora que estava em sua mesa. Ao retornar ao departamento delta, o suporte informa o ocorrido e diz que é comum este tipo de incidente.

Analisando a situação descrita na nota de campo do dia 10/10/07 podemos afirmar que este tipo de situação pode comprometer informações importantes da empresa e que os procedimentos de seguranças utilizados, atualmente, pela empresa não são capazes de detectar e corrigir essa falha.

Para detectar quais os usuários da rede de computadores possuem uma visão holística, elaboramos a seguinte pergunta: "quando há um problema em outro departamento, você:". 21% dos usuários marcaram a opção "não faço nada" e 25% marcaram "nenhuma dessas opções". A soma das duas opções chega a quase metade dos usuários, 46%, e demonstra que não possuem uma visão holística. Já a outra metade, 54%, demonstrou possuir uma visão holística. A opção "vou até o departamento e ofereço ajuda dentro das minhas limitações" foi escolhida por 33% dos usuários, a opção "vou até o departamento e pergunto em que posso ajudar" ficou com 14% e com 7% a opção "vou até o departamento ajudar a solucionar o problema como mostra o gráfico 22.

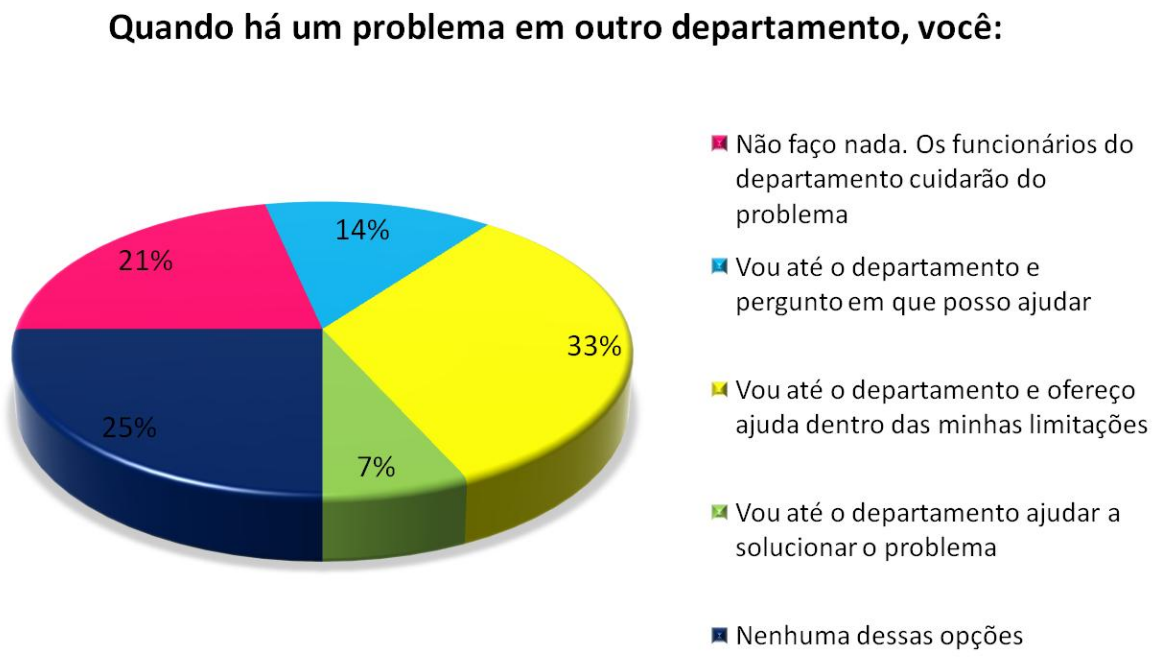

Gráfico 22 – Problema em outro departamento

Importante ressaltar que a análise de conjuntura da empresa e a tomada de decisões para a rede de computadores baseada na visão holística é fundamental, pois todos

procedimentos executados em uma estação de trabalho tem reflexos diretos para toda a rede e conseqüentemente envolvem todos os usuários.

Com o intuito de detectar quais inteligências múltiplas cada usuário possui e quais podem ser desenvolvidas, elaboramos uma questão onde os usuários identificaram as atividades que mais gostam de fazer. As atividades foram apresentadas na questão, em ordem aleatória. Para fazer a análise das respostas e chegar ao resultado descrito no gráfico 23 agrupamos as atividades por área de relação conforme sugere Nogueira (2001, p. 144).

As atividades apresentadas aos usuários foram: escutar música que faz parte da inteligência musical; jogar xadrez, trabalhar com planilha e matar charadas ou desafios formam a inteligência lógico-matemática; ler, falar em público e escrever compõem a inteligência lingüística; trabalhar em equipe, socializar-se e fornecer feedback fazem parte da inteligência interpessoal; relaxar e revisar suas ações são habilidades da inteligência intrapessoal; ler mapas e plantas compõem a inteligência espacial; praticar esportes e dançar formam a inteligência corporal-cinestésica; visitar uma exposição da inteligência naturalista.

Após a tabulação e análise dos dados sobre as atividades, tivemos um usuário com inteligência lógico-matemática, cinco com inteligência lingüística, cinco com inteligência interpessoal, treze com inteligência intrapessoal, cinco com inteligência espacial, setenta com inteligência musical, quinze com inteligência corporal-cinestésico e vinte e oito com inteligência naturalista, como podemos verificar no gráfico 23.

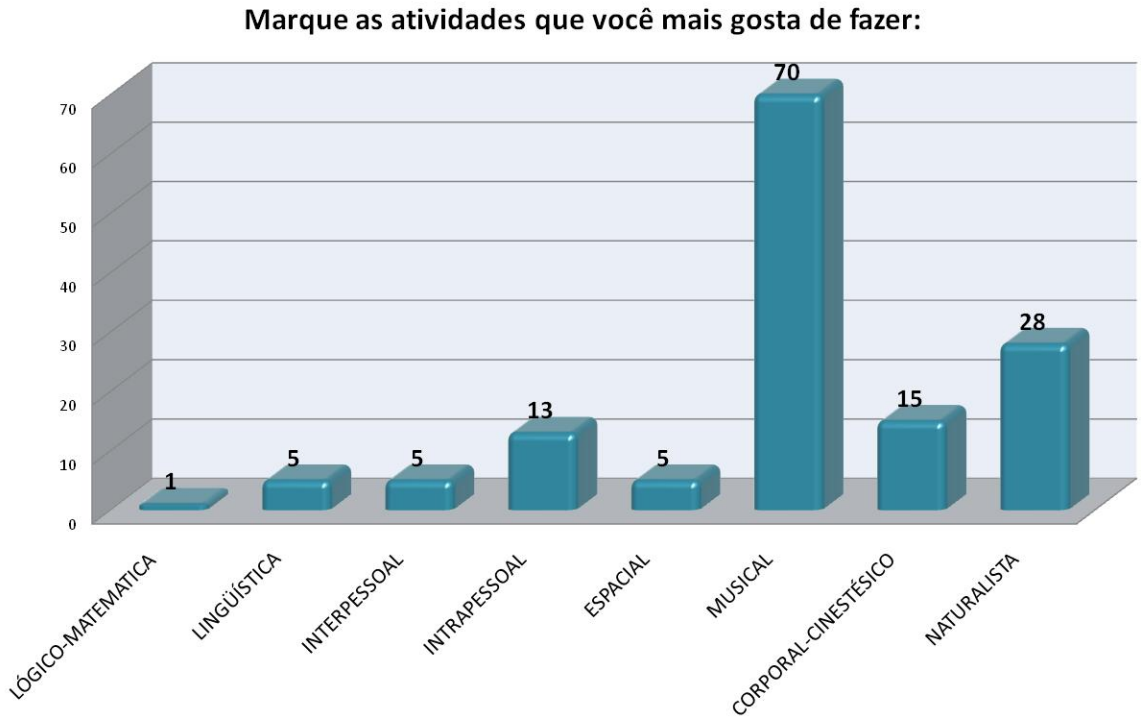

Gráfico 23 – Atividades que mais gosta de fazer

Estes números mostram possíveis indicações de inteligências desenvolvidas e indicações das inteligências que possuem apontamentos de desenvolvimento. A necessidade de executar mais testes para confirmar ou refutar essas informações são necessárias.

4.3 ENTREVISTAS INDIVIDUAIS

As partes a seguir foram retiradas das entrevistas individuais realizadas fora do horário de expediente. Os usuários convidados para entrevista foram selecionados para aprofundar a discussão de pontos relevantes. As entrevistas ocorreram no formato de bate-papo on-line. Depois da compilação das informações das entrevistas, elaboramos uma entrevista, com a equipe delta, para esclarecer alguns pontos que apresentaram discordância de opiniões entre os usuários.

Os principais pontos abordados nas entrevistas foram aqueles que apresentaram divergências e não ficaram claros no questionário fechado. A importância de dar voz aos usuários de rede é fundamental para melhor compreensão e execução dos termos e processos de segurança da empresa. Os usuários selecionados foram Peon, Eos, Artemis, Hermes, Boreas, Ares e Hera.

Na análise dos documentos de segurança da empresa, verificamos que o documento sobre as políticas de segurança, item 4.1.3, está em fase de elaboração, portanto não foi implementado. Perguntamos aos usuários, no questionário fechado, se conhecem as políticas de segurança da empresa e 60% respondeu que sim. Com base nessas informações começamos a entrevista solicitando aos usuários, Hermes, Hera, Boreas, Ares e Artemis, que estão dentro desse percentual, detalhes sobre essas políticas de segurança.

> **PESQUISADOR:** No questionário, você colocou que conhece as políticas de segurança da empresa. Poderia me dizer quais são?
>
> **HERMES:** enumerando:
> os usuários não podem logar em + de 1 pc por vez
> é proibido o acesso a sites de bate papo e afins
> assim como sites pornográficos
> os acessos dos usuários são relatados
> os usuários de um setor têm acesso somente as pastas da rede que correspondem a seus serviços
>
> **HERA:** veja bem
> alguns sites são bloqueados
> não pode usar o e-mail da instituição com fins particulares
> as pastas na rede também não podem ser usadas para este mesmo fim
> quer mais?!
>
> **BOREAS:** Bloqueio de site
> o não acesso a músicas
> MSN
>
> **ARES:** Acesso restrito a alguns sites. Especificamente aqueles com conteúdo pornográfico, sites de relacionamento, compartilhamento de vídeos ou arquivos, etc.
>
> **ARTEMIS:** sim, não acessar sites que possam comprometer a integridade das informações da entidade, como exemplos, sites de relacionamentos.

Os usuários Hermes e Hera foram os que mais citaram pontos; os demais usuários Boreas, Ares e Artemis relacionaram alguns pontos, mas a principal preocupação de todos foi com o acesso a Internet. Todos relataram restrições ou bloqueios a algum tipo de site principalmente com conteúdo pornográfico. Embora não exista nenhum documento sobre políticas de segurança, fica claro nas respostas que os usuários, além de afirmarem conhecer as políticas de segurança, sabem quais os principais tópicos dessas políticas.

Perguntamos à equipe delta por que os usuários afirmam conhecer as políticas de segurança se não existem tais políticas.

> **PESQUISADOR:** Nos questionários, a maioria dos usuários respondeu que conhecer as políticas de segurança da empresa. A que fator se deve essa resposta, já que não existem políticas de segurança?
>
> **EQUIPE DELTA:** Isso se deve ao fato de que os usuários associaram o "termo de utilização" a uma política de segurança da empresa.

Se analisarmos a conjuntura, podemos notar que os usuários consideram o termo de compromisso, item 4.1.2, como "políticas de segurança" conforme descreve a equipe delta. Então perguntamos à equipe delta se consideram o termo como parte das políticas de segurança:

> **PESQUISADOR:** Em entrevistas individuais foi verificado que as políticas de segurança a que os funcionários se referem são, na verdade, o termo de compromisso e o bloqueio no acesso a Internet de determinados sites e serviços. Podemos considerar esse termo e os bloqueios com parte da política de segurança?
>
> **EQUIPE DELTA:** Sim, esse termo pode ser considerado como um início. Porém, espero que efetivamente esse início dê lugar a uma política de segurança consolidada.
> Obviamente uma política de segurança é algo muito mais complexo do que um termo de responsabilidade. Porém, isso indica um início de preocupação em relação à segurança da informação por parte dos dirigentes da empresa.

Até a equipe delta faz alguma confusão com o termo de responsabilidade e as políticas de segurança. Como não houve nenhuma palestra de esclarecimento aos usuários, é natural que essa confusão exista. Questionamos a equipe delta sobre qual é a previsão para a implantação das políticas de segurança.

> **PESQUISADOR:** existe alguma previsão para implantar? ou será sempre como neste caso, corretivo?
>
> **EQUIPE DELTA:** Ainda não existe previsão para o início de um projeto de política de segurança. Mas, devido aos últimos problemas, outras medidas de segurança deverão ser implementadas.

Embora exista um ruído entre a equipe delta e os usuários referente à existência ou não de políticas de segurança, na implantação do termo de compromisso e nas restrições de acesso, principalmente de sites, não houve por parte da equipe delta iniciativa de esclarecer os pontos que geraram problemas aos usuários. Perguntamos à equipe delta se existe algum tipo de treinamento regularmente ou se tem sido oferecidas palestras.

> **PESQUISADOR:** Qual o procedimento com os usuários hoje? Existe algum tipo de treinamento? A equipe delta faz palestras de prevenção e atualização?

> **EQUIPE DELTA:** Também não. Na realidade, essa é uma questão que se volta para a política de segurança. Esse tipo de treinamento comumente realizado através de palestras e workshops deve ser contemplado na política de segurança. Sem uma política de segurança, não há uma estrutura sólida para se implementar outros projeto de segurança.

Embora não responda diretamente à questão, a equipe delta deixa claro que qualquer tipo de palestra ou treinamento relacionado às questões de segurança deve ser contemplado na política de segurança, que não existe ainda. Com isso temos um impasse, pois não houve nenhum tipo de treinamento aos usuários, que sentem necessidade de participar mais ativamente do processo, conforme relata Ares e Hera:

> **PESQUISADOR:** Como essas políticas foram colocadas para você? Houve uma palestra?
>
> **HERA:** não
> na verdade foram impostas
> não houve nenhum tipo de levantamento
> das nossas reais necessidades
> nem nada
> apenas comunicaram perante circular
>
> **ARES:** Não fomos chamados a opinar. Algum tipo de consulta é interessante. Sem "democratismos" (excesso de democracia). Mas acho que ouvir a opinião dos funcionários por meio de um formulário em que ele explicite os acessos de trabalho e pessoais que têm mais relevância seria necessário. A partir dele poder-se-ia então formular uma política de segurança.

A consciência dos dois usuários, principalmente de Ares, mostra que a participação na elaboração das políticas de segurança visa a melhorar a forma de implantação das regras e a uma melhor aceitação e participação entre os usuários. Essa participação é importante, pois faz com que o usuário se sinta responsável pelo processo.

Como não houve nenhum tipo de palestra ou treinamento aos usuários, informamos à equipe delta sobre os questionamentos e perguntamos se a forma de implantação foi muito dura por parte da empresa e se existe a intenção de rever o processo e fazer palestras de esclarecimento aos funcionários:

> **PESQUISADOR:** Alguns usuários questionaram a forma como foram implantadas essas regras. Como aconteceu essa implantação?
>
> **EQUIPE DELTA:** Aconteceu de uma forma não muito convencional e eficaz. Simplesmente solicitaram aos usuários que tomassem o devido conhecimento e a partir de então o termo vigoraria.

PESQUISADOR: Você acha que a empresa foi muito incisiva na implantação?

EQUIPE DELTA: Sim. Desta forma gerou grandes dúvidas para os usuários que de repente se viram obrigados a seguirem certas normas, e ainda sem existir nenhum tipo de treinamento, palestra, ou qualquer outra forma que pudesse ser possível o conhecimento sobre o assunto segurança da informação

PESQUISADOR: Então ainda existe a possibilidade de uma palestra com orientação aos funcionários?

EQUIPE DELTA: Acredito e espero que isso venha a acontecer. Isso é um fator crucial na implantação de uma política de segurança bem sucedida.

Dessa forma, ficam confirmados os relatos de Ares e Hera sobre a importância da participação dos usuários na elaboração das políticas de segurança da empresa. Existe também a predisposição da equipe delta para a realização dessa aproximação.

Durante a entrevista de alguns usuários, que disseram conhecer as políticas de seguranças, foi levantado um ponto sobre a eficácia das políticas - na verdade o termo de responsabilidade - na execução dos trabalhos diários dos usuários. Perguntamos a esses usuários se as políticas ajudam ou atrapalham seu trabalho:

PESQUISADOR: E você considera que essas políticas ajudam ou atrapalham seu trabalho?

BOREAS: em meu trabalho, especificamente atrapalha
dentro do que eu uso e da consciência que eu tenho
essa forma de proibição
pra mim... é equivocada

ARES: Há pontos positivos e negativos. Como positivos eu ressaltaria o fato de que ao proibir o acesso a estas páginas o que a instituição objetiva é maior foco no trabalho e maior produtividade. Como ponto negativo eu ressalto que a política não deixa claro exatamente quais sites podem ser acessados. Concordo com o veto aos sites acima. Mas há alguns acessos que, mesmo se caracterizando como pessoais, contribuem para o conforto do indivíduo e, desde que feitos moderadamente, em nada perturbam o bom andamento do trabalho. Então, como forma de melhorar a política, eu sugeriria explicitar melhor a questão dos acessos proibidos e adotar algum instrumento que permita maior tolerância. Assim procedendo eu diria que contribuiria mais do que atrapalharia o meu trabalho.

Embora Boreas não informe diretamente, acessava sites que agora são proibidos e considera esse tipo de acesso normal, já que fazia de forma consciente. Já Ares faz uma análise mais profunda informando pontos positivos e negativos e acredita que os acessos a sites para o uso pessoal podem contribuir para o conforto do indivíduo. Pedimos para Ares esclarecer melhor essa frase.

PESQUISADOR: "contribuem para o conforto do indivíduo" seria uma forma de ter o funcionário do lado da empresa?

ARES: O exercício profissional hoje não pode ser mais encarado como uma linha de produção, exceto para aquelas funções que realmente trabalham como tal. O ideal seria que ele tivesse que comparecer fisicamente ao trabalho e realizar muitas tarefas a partir de outros locais que não o de trabalho (escritório pessoal, residência, em trânsito, etc.). Assim ele poderia administrar melhor o seu tempo entre o trabalho e seus afazeres e interesses pessoais. Infelizmente esta não é a relação de trabalho que nos é colocada. Então a informática, e seu uso, pode contribuir para esta compatibilização, isto é, entre trabalho e afazeres e vida pessoal. É neste sentido que eu utilizei a expressão "conforto do indivíduo".

Temos então mais um ponto a ser considerado pela equipe delta: não desestruturar as zonas de conforto do usuário e construir uma sólida política de segurança. Parece fácil, mas lidar com o "conforto do indivíduo" de cada usuário de uma rede de computadores é uma tarefa extremamente complicada, pois os usuários, em geral, não querem cumprir as normas de segurança.

A fim de analisar o cumprimento do termo, perguntamos aos entrevistados se eles cumprem as políticas de segurança.

PESQUISADOR: e você cumpre essas políticas?

BOREAS: hoje sim
antes não
mas o que eu acessava antes
não era nada grave
não baixava
nada e nem ia em bate papo

HERMES: 80% das vezes, eu diria

Boreas informa que atualmente cumpre as normas, mas que antes não e justifica que os acessos que fazia não eram graves. Porém, tivemos uma surpresa com a resposta de Hermes, que disse respeitar as normas em 80% dos casos. Perguntamos então o que acontecia nos outros 20%.

PESQUISADOR: e os outros 20%?

HERMES: como dizer... "escapuliu"
são os "5 minutinhos" de lazer no trabalho
se o trabalho desenvolvido for muito estressante, isso não impede de ter um minuto de relax e aí sim, com o tempo, pode a vir prejudicar o desempenho

Hermes argumenta que, em condições de trabalho estressantes, o usuário precisa de um tempo para espairecer e depois retornar ao trabalho. Pela forma das respostas, percebemos que Hermes não mudou a forma de trabalho e também não está preocupado com os monitoramentos aos sites que acessa. Perguntamos a ele se a implantação das regras iria ajudar na segurança.

> **PESQUISADOR:** Me parece que as regras implantadas não mudaram sua forma de trabalhar. Você considera que essas regras irão ajudar na segurança ou irão apenas monitorar os usuários que não trabalham?
>
> **HERMES:** acho que irão provocar mais insatisfação do que melhoria no trabalho, parece realmente ter o intuito de inibir e monitorar e não de otimizar.

Essa insatisfação, relatada por Hermes, foi detectada em outras entrevistas quando o assunto em discussão era políticas de segurança.

> **PESQUISADOR:** Na sua opinião, qual é o objetivo dos bloqueios?
>
> **EOS:** Cortar o acesso da Internet dos funcionários!!! Aff...sei lá... Acho que a empresa quer que os funcionários produzam mais, deve ser...mas só gerou insatisfação!!! Querendo ou não, sempre tem um pouquinho do dia que vc não faz nada!!!
>
> **ARES:** Não apenas este fator específico, ou seja, baixa orientação e inexistência de disseminação. Como ela não é democrática desde o seu início, a probabilidade de boa aceitação é baixíssima. Logo, o corpo funcional fica insatisfeito.

Alinhados as afirmações de Hermes, Eos e Ares também relatam essa insatisfação dos usuários sobre a implantação das regras de segurança. Nas entrevistas, percebemos que os usuários estavam questionando a forma como foram implantadas as regras de segurança. Não houve nenhum tipo de orientação por parte da empresa, não perguntaram quais eram as necessidades, as demandas dos usuários. É importante salientar que a empresa não observou os conflitos que gerou nos usuários a implantação do termo de compromisso. O intuito do documento era trazer aos usuários uma conscientização para utilização dos recursos disponibilizados pela empresa para execução das tarefas diárias.

> **PESQUISADOR:** Então o problema foi a falta de orientação e não o bloqueio?
>
> **HERA:** sim
> totalmente
> porque a empresa tem sim que se preocupar com a segurança de suas informações
> se existem normas elas tem que serem seguidas, por mais que incomodem...

BOREAS: a falta de informação pesa mais.... mesmo assim, acredito que a maioria não tenha conhecimento de que essa medida tomada pela empresa seja para efeito de segurança. O aspecto levantado é a preocupação com quem está usando o mecanismo de trabalho para outra finalidade, foi dessa forma que foi passada.

EOS: Isso...De repente tentaram mudar da água pro vinho! Não dá certo, todo ser humano tem dificuldade de se adaptar, não pode ser assim! O bloqueio de sites como orkut e jogos é necessário, eu acho, mas bloquear geral, além de sites, quer bloquear tempo tmb! Esse tipo de coisa gera muita insatisfação, tenho certeza que não gera retorno nenhum pra empresa!

Os usuários confirmam que o maior problema foi a falta de orientação e mostram quais os possíveis caminhos que a empresa pode seguir para minimizar os problemas na implantação das regras de segurança. Para Hera, a empresa precisa se preocupar com a segurança mesmo que haja incômodo para a execução. Essa afirmação mostra que existe um comprometimento por parte dos usuários, só precisa ser estimulado. Questionamos os usuários sobre se a implantação das regras fosse de outra forma, como eles agiriam

PESQUISADOR: e você acha que se fosse apresentado de outra forma iria mudar alguma coisa?

BOREAS: talvez... o sentimento das pessoas... no aspecto de aceitação, sim... tudo que vem de forma educada, explicativa, penso que a resposta é mais pro positivo do que pro negativo

HERA: de repente o impacto ou até mesmo a maneira que você enxerga as coisas
se fosse comunicado, explicada a real necessidade dessas normas
dar motivos para tais mudanças, pois o que parece é que tudo isso é feito como uma penalidade
a conscientização seria diferente

Boreas aborda a questão emocional. Essa visão é fundamental, pois é possível trabalhar de forma colaborativa, fazendo com que o usuário se sinta parte do processo, dessa forma se sentirá responsável na execução das normas de segurança. Podemos perceber esse fator no final da entrevista com Ares quando questionamos o usuário sobre a leitura do termo de compromisso.

PESQUISADOR: Nas políticas de segurança, existe alguma orientação sobre abertura de email, SPAM?

ARES: Se existe eu não tomei conhecimento. Pode ter sido por omissão da minha parte; se isto ocorreu, a atitude não foi dolosa.

PESQUISADOR: vc não leu o termo de compromisso?
mas assinou?

> **ARES:** Lembro-me de ter assinado um documento. Lembro da interdição de certos acessos, aqueles que mencionei na resposta à primeira pergunta. Não me lembro do conteúdo do restante. Mas creio que uma política não se implanta assim, com base num documento escrito e assinado em circunstâncias e momentos muito específicos. Ela precisar ser disseminada para ser bem aceita.

Ares demonstra ter conhecimento do termo de compromisso, embora o considere como políticas de segurança; Ares assinou sem a interpretação correta de todos os itens. Fica claro que os usuários assinaram o termo sem nenhum questionamento e quando tiveram a oportunidade de se pronunciar sobre as questões que os incomodam, na entrevista, fizeram-no de forma coerente e responsável. Citaram quais os pontos problemáticos e apontaram sugestões para resolução.

A questão do SPAM, que foi abordada no dialogo acima com Ares, gerou muita confusão nas respostas do questionário fechado (ver gráficos 11 a 15): apenas 36% dos usuários conseguiram identificar corretamente um SPAM. Expusemos esses dados à equipe delta.

> **PESQUISADOR:** Houve uma confusão nos questionários sobre o que é um SPAM e como identificar a extensão de um vírus no e-mail. Você acha que falta um canal de comunicação entre usuário e a equipe delta? Evitando assim alguns problemas e desgastes?
>
> **EQUIPE DELTA:** Sim, acho isso essencial. Esse canal de comunicação seria contemplado nas palestras e treinamentos realizados na política de segurança.

A equipe delta considera importante ter um canal de comunicação com os usuários para esclarecer problemas como o relacionado ao SPAM. Perguntamos por que ainda não implantaram se o consideram tão importante.

> **PESQUISADOR:** se as políticas de seguranças são tão importantes porque ainda não foram implantadas?
>
> **EQUIPE DELTA:** Acredito que deva ser uma medida que traria uma grande mudança na forma e no hábito de trabalho das pessoas, além de envolver recursos financeiros. Isso aliado ao fato de ser uma medida preventiva, e conforme sabemos aqui no Brasil, em sua grande maioria, as coisas funcionam de forma apenas corretiva.

Baseado nas entrevistas individuais, pode-se dizer que os usuários deixam transparecer essa grande mudança na forma e no hábito de trabalho a que a equipe delta se refere. Os usuários sentem essa necessidade de participar de forma construtiva e colaborativa. Recortamos uma parte da entrevista com a usuária Artemis que demonstra claramente o senso

crítico e o discernimento para utilização correta de uma ferramenta que foi bloqueada para utilização pelo termo de compromisso.

> **PESQUISADOR**: Ter um funcionário insatisfeito pode comprometer a produtividade?
>
> **ARTEMIS:** Sim, pode, pode inclusive trazer danos à entidade, mas não consigo ver que o não acesso à Internet possa trazer insatisfações
>
> **PESQUISADOR:** Então considera corretas as políticas de segurança adotadas pela empresa?
>
> **ARTEMIS:** Sim, estão corretas.
> Inclusive neste momento, não sei se estou interferindo negativamente neste processo.
>
> **PESQUISADOR:** Bom, segundo o conceito que você colocou não estamos comprometendo a integridade das informações da empresa, certo? ou errado?
>
> **ARTEMIS:** Acredito que não
>
> **PESQUISADOR:** Então podemos dizer que o bate-papo, usado de forma correta, pode ser útil para a empresa?
>
> **ARTEMIS:** Sim, muito positivo, já utilizei o MSN como ferramenta de trabalho e tinha um resultado muito eficaz, inclusive de customização.
>
> **PESQUISADOR:** Então vamos chegar a um consenso...
> As políticas de segurança proíbem o uso, mas estamos comprovando que pode ser útil... utilizando de forma correta as ferramentas disponíveis, podemos ter produtividade, ou seja, as políticas de segurança teriam que ser revistas em alguns pontos. Certo?
>
> **ARTEMIS:** Correto, utilizado com critérios, passa a ser uma ferramenta de trabalho eficaz e com informações em tempo real.

Para a empresa conseguir um maior alcance das normas de segurança é necessário conhecer o perfil dos seus usuários e assim traçar, de formar objetiva, um plano de implantação das políticas de segurança. Questionamos a equipe delta sobre esse perfil.

> **PESQUISADOR:** Vc conhece o perfil dos seus usuários?
>
> **EQUIPE DELTA:** O que seria exatamente o perfil dos usuários? Conhecimento técnico??
>
> **PESQUISADOR:** Escolaridade, conhecimentos em informática, idade
>
> **EQUIPE DELTA:** De alguns, sim
>
> **PESQUISADOR:** daqueles que já apresentaram problemas ?
>
> **EQUIPE DELTA:** Problemas de segurança??
> ou problemas técnicos??

PESQUISADOR: Sim. problemas de segurança?

EQUIPE DELTA: Veja bem, os incidentes de segurança estão relacionados a grande parte dos usuários. Não haveria como traçar um perfil específico destes usuários.

Nesse trecho fica clara a necessidade de uma mudança, por parte da equipe delta, na forma de tratamento que o departamento e a empresa dão aos usuários. Saber quem são, como trabalham, como estudam, como se divertem, enfim, ter uma visão mais humana dos usuários e não considerar que todos são iguais e que devem ser tratados como máquinas. A utilização das inteligências múltiplas na abordagem aos usuários pode representar uma rota alternativa que possibilite o tecnólogo entender melhor como seus usuários.

5 CONSIDERAÇÕES FINAIS

E nossa história não estará pelo avesso
Assim, sem final feliz.
Teremos coisas bonitas pra contar.
E até lá, vamos viver
Temos muito ainda por fazer
Não olhe para trás
Apenas começamos.
O mundo começa agora
Apenas começamos.
Renato Russo, Legião Urbana

Apresentamos neste trabalho um diagnóstico sobre as principais fragilidades nos procedimentos de segurança em uma rede local de computadores com foco na relação humana. Na análise dos dados, ficou demonstrado que os dois lados, usuários e suporte técnico, formam os pilares dos procedimentos de segurança da empresa.

Na análise de dados evidenciamos que os usuários da rede de computadores buscam se preparar, tanto acadêmica quanto tecnologicamente, para execução das suas tarefas. Esses dados são confirmados nas entrevistas individuais, nas quais os usuários demonstraram a capacidade de utilização de suas formações. Contudo, existe uma barreira que impede o usuário de participar de forma efetiva dos procedimentos de segurança. Essa barreira acaba gerando ruídos, que ficaram demonstrados no questionário e nas entrevistas, nas quais o entendimento e a execução de medidas corretivas e preventivas ficaram prejudicados.

Assim como o tecnólogo demonstrou preparação, principalmente tecnológica, para lidar com os procedimentos de segurança, também enfrentou os mesmos problemas encontrados pelos usuários no planejamento das ações de segurança.

No final da pesquisa, após a análise e discussão dos dados, identificamos um ponto que não foi abordado no momento da definição dos objetivos deste trabalho; a falta de comunicação entre os dois lados. Os dois lados, tecnólogo e usuário, enfrentam os mesmos problemas, têm os mesmos objetivos, mas não conseguem se comunicar. A falta de comunicação e a utilização da linguagem para diminuir as barreiras impostas pela tecnologia foram os pontos que apresentaram mais fragilidade nos procedimentos de segurança em uma rede local de computadores da empresa.

Esse problema, na utilização da linguagem é uma questão muito importante, pois muitas questões relatadas pelos usuários e pelos tecnólogos poderiam ser evitadas se os dois lados utilizassem a linguagem de forma correta para se comunicar.

É preciso demonstrar ao tecnólogo que nem tudo é tecnologia e que fator humano pode ser utilizado ao seu favor. A forma de abordagem que o tecnólogo utiliza no momento de atender ao usuário pode ser determinante na relação profissional. Nas entrevistas individuais, os usuários ressaltaram a necessidade de manter um diálogo com os tecnólogos e a importância de participar das decisões, dentro das possibilidades.

Analisando a formação acadêmica, os tecnólogos não receberam nenhum tipo de formação ou orientação com ênfase nas relações humanas. Não foram instruídos formalmente para trabalhar e entender a linguagem do usuário.

Precisamos rever nossos conceitos sobre educação superior no Brasil, onde existe uma tendência de encurtar cada vez mais os semestres de um curso, retirando das grades curriculares matérias que não têm o conteúdo técnico para determinada formação, esquecendo que precisamos trabalhar a interdisciplinaridade, a pluralidade na formação profissional. E essa interface se demonstrou essencialmente importante para auxiliar nas questões técnicas de forma que ficassem bem resolvidas. Como no caso desta pesquisa, a segurança da rede de computadores.

Apresentar ao tecnólogo outras vias para resolução de problemas que não sejam técnicas, como a teoria das inteligências múltiplas, abordada em detalhes neste trabalho, seria uma forma de aperfeiçoar a abordagem dos tecnólogos nas relações humanas. Com o uso correto da inteligência lingüística e da inteligência interpessoal, por exemplo, que formam a base para uma boa abordagem, o tecnólogo poderia evitar diversos problemas e desgastes nos cenários que foram expostos na empresa pesquisada.

Por sua vez, os usuários precisam ser estimulados a desenvolver uma visão holística, ou seja, desenvolver uma visão além das suas atribuições e competências. Essa necessidade fica demonstrada nos equívocos que os usuários cometem ao considerar o termo de compromisso como política de segurança ou acessar sites que foram proibidos pelo termo de compromisso e ainda afirmarem que não estão fazendo nada de errado.

O usuário precisa ser estimulado a ter um pensamento sistêmico, pois se tiver sua máquina infectada por um vírus, porque acessou um site proibido, por exemplo, provavelmente infectará toda a rede. Assim colocará em risco todas as informações da empresa, inclusive as próprias informações que armazena como endereços de e-mails, telefones, dados bancários, entre outros. Com o desenvolvimento do pensamento sistêmico,

que possibilita ao usuário entender de forma geral o funcionamento de todas as partes de uma rede de computadores, o usuário entenderá que se a empresa perde, ele também perde, pois faz parte do grupo.

Trabalhar o fator humano pode levar à empresa a vanguarda nas questões que envolvem as tecnologias e o ser humano. Mas é preciso utilizar a linguagem, de forma correta, na implantação das regras dentro da empresa, pois se aplicarmos de forma colaborativa as normas, podemos trazer os usuários para trabalhar do lado do tecnólogo e gerar estímulos positivos.

Traçando um paralelo entre a segurança da rede de computadores e a letra apresentada na epígrafe deste trabalho, temos uma suposta proteção com vidros, grades e muros, que garante a segurança, o que pode ser comparado às ferramentas tecnológicas utilizadas pelo tecnólogo para garantir a segurança na rede de computadores. Mas a letra diz que, quando o caos chegar, nada será suficiente para te proteger de você. De nada adiantarão os vidros, grades e muros, pois não irão garantir a proteção de você. Na rede de computadores, os esforços dos tecnólogos em ter um firewall mais seguro, antivírus eficiente, criptografias fortes não serão capazes de deter o ser humano – dele mesmo. No referencial teórico deste trabalho, ficou demonstrado, segundo os autores citados, que o caos na segurança de rede de computadores, na maior parte dos casos, é desencadeado pelo fator humano. O ser humano sempre estará inserido no contexto, seja usuário ou tecnólogo e nenhum muro vai te guardar... de você.

Por muitas vezes perseguimos a perfeição e esquecemo-nos de trabalhar para diminuir as barreiras levantadas pela linguagem. Precisamos trabalhar com o foco na solução dos problemas, mas às vezes não é possível melhorar tudo de uma vez. Precisamos ter o foco direcionado para o principal agente de todos os processos, o ser humano.

Precisamos ser a mudança que queremos ver.[15]

[15] Mahatma Gandhi

6 REFERÊNCIAS

ABREU-E-LIMA, Denise Martins de. **Um modelo macro-organizacional de formação reflexiva de professores de língua(s)**: articulações entre a abordagem comunicativa através de projetos e o desenvolvimento de competências sob a temática das inteligências múltiplas. Tese de Doutorado, Unicamp. Campinas, 2006. p. 100-157.

ANTUNES, Celso. **As inteligências múltiplas e seus estímulos.** 10. ed. Campinas: Papirus, 2006. 137 p.

CASTELLS, Manuel; CARDOSO, Gustavo. **A sociedade em rede:** do conhecimento à ação política. Portugal: Casa da Moeda, 2006.

CAMPETTI, Mônica Z. P.; CAMPETTI SOBRINHO, Geraldo. **Atitude!**: o que ninguém pode fazer por mim. Brasília: LGE, 2007. 130 p.

CHAUÍ, Marilena. Ensinar, aprender, fazer filosofia. **Revista do ICHL da UFG**, v. 2, n. 1, p. 1-10, jan./jul. 1982.

FORTES, Débora. **Os espiões querem seu pc***:* spyware, cavalos-de-tróia, vermes... veja como sobreviver sem ficar paranóico. Coleção Info 2007: Segurança, São Paulo, ed. 40, p. 15-21, abr. 2007.

GARDNER, Howard. **Inteligências múltiplas***:* a teoria na prática. Porto Alegre: Artes médicas. 1995. 257 p.

GIL, Antônio Carlos. **Como elaborar projetos de pesquisa**. 4. ed. 8. reimpr. São Paulo: Atlas, 2006.

GRIMAL, Pierre. **Dicionário da mitologia grega e romana**. 3. ed. Rio de Janeiro: Bertrand Brasil, 1997. 616 p.

HOUAISS. **Dicionário da língua portuguesa**. Referência online: http://houaiss.uol.com.br. Acessado em outubro de 2007.

MOREIRA, Isabel Moreira. **Recado da redação***:* fique esperto! Coleção Info 2007: Segurança, São Paulo, ed. 40, p. 5, abr. 2007.

NOGUEIRA, Nilbo Ribeiro. **Desenvolvendo as competências profissionais**: um novo enfoque por meio das inteligências múltiplas. 9. ed. São Paulo: Érika. 2004. 156 p.

REZENDE, Denis Alcides; ABREU, Aline França de. Tecnologia da informação aplicada a sistemas de informação empresariais: o papel estratégico da informação e dos sistemas de informação nas empresas. In: _____. **Empresa e sistemas**. 4. ed. São Paulo: Atlas, 2006. Cap. 1, p. 29-61.

CREMA, Roberto. **Introdução à visão holística**: breve relato de viagem do velho ao novo paradigma. São Paulo, Summus, 1989. 133 p.

SCHNEIER, Bruce. **Segurança.com:** segredos e mentiras sobre a proteção na vida digital. Rio de Janeiro: Campus, 2001. 268 p.

SOARES, Luiz Fernando Gomes; LEMOS, Guido; COLCHER, Sérgio. **Redes de computadores**: Das LANs, MANs e WANs às Redes ATM. 2. ed. Rio de Janeiro: Campus, 2003. 700 p.

SOUZA, Carlos Daniel Pereira de; BITTENCOURT, Cláudio Félix de; MATTA, Max Jorge Lacerda da; PAULA Osvaldo Luís Ribeiro de. **Aspectos Sociais no ambiente de engenharia de software**: o profissional e seus relacionamentos familiares e profissionais. Dissertação de pós-graduação, Upis, Faculdades Integradas, Brasília, 2005. 168 p.

STALLINGS, William. Arquitetura e organização de computadores. In: _____. **Evolução dos computadores**. 5. ed. São Paulo: Pretince hall, 2003. p. 17-49.

TANENBAUM, Andrew S. **Redes de computadores**. 4. ed. Rio de Janeiro, Campus, 2003. 943 p.

WADDLOW, Thomas A. **Segurança de redes**: projeto e gerenciamento de redes seguras. Rio de Janeiro, Campos, 2001. 270 p.

7 ANEXOS

7.1 CIRCULAR 2007

CIRCULAR Nº /2007

Comunicamos a todos os funcionários que a partir desta data serão implementados critérios para utilização de Internet e acesso a rede de computadores de acordo com listado abaixo:

1. Atendendo legislação vigente encaminharemos a todos os funcionários termo de compromisso para acesso a rede;

2. A solicitação para criação de e-mail e conta de acesso ao sistema para funcionários será feito pelo Setor de Recursos Humanos de acordo com formulário próprio.

3. A solicitação de cancelamento de e-mail de funcionário desligado será feito pelo Setor de Recursos Humanos, em nenhuma hipótese após o desligamento do funcionário o e-mail institucional será redirecionado para e-mail particular.

4. A senhas de acesso à qualquer sistema da Empresa (rede, e-mail, banco de dados) deverão ser mantidas em confidencialidade, sendo o usuário o responsável pelo uso indevido do login.

5. O Suporte irá proceder vistoria em todas as estações de trabalho no período de 17 à 30/08. Após esta data serão aplicadas as penalidades de acordo com o Termo de Compromisso.

Brasília-DF, 16 de agosto de 2007

Departamento Alfa

7.2 TERMO DE COMPROMISSO

TERMO DE COMPROMISSO

Declaro que não utilizarei a rede de computadores e suas funções/disponibilidades para qualquer finalidade ilegal ou proibida por este termo de compromisso, bem como concordo em respeitar todas as leis e regulamentos locais, estaduais, federais e internacionais aplicáveis, sendo exclusivamente responsável por todas as ações ou omissões ilegais ou proibidas realizadas através da rede de computadores e suas funções/disponibilidades, feitas de minha senha de acesso.

Para tanto, estou ciente de que é expressamente proibido acessar:

- Sites de jogos on-line
- Radio on-line
- Bate papo de qualquer espécie
- Sites de relacionamento
- Sites de conteúdo pornográfico, discriminatório:

Proibido utilizar o e-mail Empresa:

- Endereço eletrônico (e-mail) fornecido pela empresa em proveito pessoal, bem como usar a rede de computadores e os cadastros para enviar pesquisas, concursos, pirâmides, correntes, lixo eletrônico, spam ou quaisquer mensagens periódicas ou não-solicitadas (comerciais ou não);
- Para difamar, abusar, perturbar a tranqüilidade alheia, perseguir, ameaçar ou de qualquer outra forma violar direitos de terceiros;
- Para publicar, distribuir ou divulgar quaisquer materiais ou informações inadequadas, profanas, difamatórias, transgressoras, obscenas, indecentes ou ilegais;
- Para anunciar ou oferecer para venda ou compra de bens ou serviços, com qualquer finalidade comercial;
- Para transmitir ou carregar qualquer material que contenha vírus, “cavalos-de-tróia”, “bombas-relógio” ou quaisquer programas prejudiciais ou nocivos;

- Para interferir ou desordenar redes conectadas à rede de computadores desta empresa ou violar regulamentos, normas ou procedimentos referentes a tais redes.

Utilização dos recursos de rede:

- Os drives “U” – drive do usuário, T – Temporário e Z – Rede, deverão ser usados para gravar arquivos de interesse da instituição, sendo proibido gravar qualquer arquivo pessoal, seja de imagens, arquivos de músicas e etc.
- Nas estações de trabalho, o usuário não poderá instalar nenhum tipo de programa, software e hardware sem o prévio conhecimento e anuência do SUPORTE.
- O usuário principal da estação de trabalho é responsável por informar ao SUPORTE qualquer anormalidade em sua estação de trabalho.
- Qualquer mudança de localização, instalação e qualquer outro tipo de ocorrência que influencie no funcionamento dos recursos de informática deverão ser comunicados ao SUPORTE.

Declaro ainda ter conhecimento que os servidores da Empresa são monitorados permitindo assim mapeamento de todos os acessos efetuados na rede.

Estou ciente de que a transgressão de quaisquer normas acima descritas consistirá em falta grave, podendo resultar na ruptura do Contrato de Trabalho motivadamente.

Como medida de segurança para a empresa, autorizo o acesso à caixa-postal do meu OUTLOOK EXPRESS para a verificação do teor dos e-mails recebidos e enviados, bem como o monitoramento da minha estação de trabalho.

Brasília-DF, 16 de agosto de 2007

7.3 QUESTIONÁRIO FECHADO

1- Qual sua idade?

☐ Abaixo de 20 ☐ Entre 21 a 30 ☐ Entre 31 a 40 ☐ Entre 41 a 50 ☐ Acima de 51

2- Qual sua formação acadêmica?

☐ 1º Grau
☐ 2º Grau
☐ Graduação
☐ Pós-Graduação
☐ Mestrado
☐ Doutorado

☐ Incompleto
☐ Cursando
☐ Completo

3- Seu trabalho está relacionado à informática?

☐ Não ☐ Sim, diretamente ☐ Sim, indiretamente

4- Já fez algum curso de informática?

☐ Não ☐ Sim. Ano de conclusão ☐

Se sim, foi financiado pela empresa?

☐ Sim ☐ Não

5- Você conhece as políticas de segurança da empresa?

☐ Sim ☐ Não

6- Quando você recebe um e-mail que contém um SPAM, o que acontece?

☐ Meu computador é infectado por um vírus
☐ Os outros computadores são infectados por um vírus
☐ Não sei
☐ Não acontece nada
☐ A rede e os servidores são infectados por um vírus

7- Para imprimir um documento que está aberto no Microsoft Word, qual dessas opções você mais utiliza?

☐ Pressionar no teclado CTRL + P
☐ Clicar com o mouse no desenho da impressora
☐ Selecionar com o mouse a opção do menu ARQUIVO, IMPRIMIR
☐ Chama alguém do suporte para me ajudar

8- Para ler suas mensagens de sua conta de e-mail externo (particular), você:

☐ Usa o webmail
☐ Solicita a configuração do e-mail no computador de trabalho
☐ Pede orientações do suporte da empresa
☐ Não acessa e-mail externo

9- Quando há um problema em outro departamento, você:

- ☐ Não faço nada. Os funcionários do departamento cuidarão do problema
- ☐ Vou até o departamento e pergunto em que posso ajudar
- ☐ Vou até o departamento e ofereço ajuda dentro das minhas limitações
- ☐ Vou até o departamento ajudar a solucionar o problema
- ☐ Nenhuma dessas opções

10- Quando você recebe um arquivo em anexo ao e-mail, você é capaz de identificar qual a extensão do arquivo recebido?

☐ Sim ☐ Não ☐ Não. O antivírus fará isto

Se sim, quais dessas extensões podem conter vírus?

☐ .scr ☐ .jpg ☐ .bat ☐ .exe ☐ .doc

11- Você já participou de algum treinamento sobre segurança promovido pela empresa?

☐ Sim ☐ Não

12- Quando você tem problemas (qualquer um) em seu computador de trabalho:

- ☐ Tenta arrumar sozinho, se não resolver chama o suporte
- ☐ Pergunta para o colega ao lado, se não resolver chama o suporte
- ☐ Chama o suporte diretamente

Ao chamar o suporter, você:

- ☐ Chama um funcionário específico do suporte para atender
- ☐ Chama qualquer funcionário do suporte para atender

13- Marque as atividades que você mais gosta de fazer:

- ☐ Ler
- ☐ Praticar Esportes
- ☐ Jogar xadrez
- ☐ Falar em público
- ☐ Ler mapas e plantas
- ☐ Trabalhar em equipe
- ☐ Revisar suas ações
- ☐ Socializar-se
- ☐ Visitar uma exposição
- ☐ Escutar música
- ☐ Trabalhar com planilha
- ☐ Relaxar
- ☐ Dançar
- ☐ Matar charadas ou desafios
- ☐ Fornecer feedback
- ☐ Escrever

Nome:

Nome Fantasia:

7.4 ENTREVISTA HERMES

PESQUISADOR:
No questionário você colocou que conhece as políticas de segurança da empresa. Poderia me dizer quais são?

HERMES:
enumerando:
os usuários não podem logar em + de 1 pc por vez
é proibido o acesso a sites de bate papo e afins
assim como sites pornográficos
os acessos dos usuários é relatado
os usuários de um setor tem acesso somente as pastas da rede que correspondem a seus serviços

PESQUISADOR:
E você considera que essas políticas ajudam ou atrapalham seu trabalho?

HERMES:
o "meu" trabalho em particular não interfere em nada

PESQUISADOR:
e você cumpre essas políticas?

HERMES:
80% as vezes eu diria

PESQUISADOR:
e os outros 20%?

HERMES:
como dizer..."escapoliu"

PESQUISADOR:
sei!
então existe uma necessidade de "burlar" as políticas as vezes?
ou seja, as vezes as políticas atrapalham o desempenho!

HERMES:
necessidade não, eu diria vontade

PESQUISADOR:
digamos que faz parte...

HERMES:
são os "5 minutinhos" de lazer no trabalho

PESQUISADOR:

necessários... mas se existe monitoramento, você não acha que isso pode te prejudicar?

HERMES:
desde que não seja constante ou repetitivo ou com grande duração eu acho que não

PESQUISADOR:
então essas políticas que censuram podem prejudicar o desempenho?

HERMES:
se o trabalho desenvolvido for muito estressante, isso nao impede de ter um minuto de relax e aí sim com o tempo pode a vir prejudicar o desempenho

PESQUISADOR:
Você acha que faltou algo, como palestras de esclarecimentos, no momento da implantação?

HERMES:
com certeza

PESQUISADOR:
e como foram as repercussões dessas medidas?

HERMES:
gerou uma insatisfação generalizada, mais nada que causasse moção dos funcionários

PESQUISADOR:
Afinal, foram políticas de segurança ou controle de acesso? Você foi informado o que estava acontecendo e por quê?

HERMES:
foi colocado como política de segurança
fomos informados somente no momento da implantação

PESQUISADOR:
Você recebeu alguma instrução, informação que seria monitorado?

HERMES:
sim

PESQUISADOR:
Me parece que as regras implantadas não mudaram sua forma de trabalhar
Você considera que essas regras irão ajudar na segurança ou irão apenas monitorar os usuários que não trabalham?

HERMES:
acho que irão provocar mais insatisfação do que melhoria no trabalho, parece realmente ter o intuito de inibir e monitorar e não de otimizar

PESQUISADOR:
ok!
muito obrigado pela contribuição e desculpe ter atrapalhado seu descanso!

7.5 ENTREVISTA HERA

PESQUISADOR:
No questionário você colocou que conhece as políticas de segurança da empresa, certo?

HERA:
certo

PESQUISADOR:
Você poderia dizer quais são?

HERA:
veja bem
alguns sites são bloqueados
não pode usar o e-mail da instituição com fins particulares
as pastas na rede também não podem ser usadas para este mesmo fim
que mais?!

PESQUISADOR:
entendo!

HERA:
não pode instalar programas que não sejam autorizados pela empresa
É ISSO!!!
ou não

PESQUISADOR:
E você considera que essas políticas ajudam ou atrapalham seu trabalho?

HERA:
bem acho que podem atrapalhar um pouco
na questão das pesquisas na Internet
as facilidades de utilizar algumas ferramentas
etc. tal

PESQUISADOR:
e você cumpre essas políticas?

HERA:
estou me adequando
praticamente sim

PESQUISADOR:
como essas políticas foram colocas para você? houve uma palestra?

HERA:
não
na verdade foram impostas
não houve nenhum tipo de levantamento

das nossas reais necessidades
nem nada
apenas comunicaram perante circular

PESQUISADOR:
e você acha que se fosse colocado de outra forma iria mudar alguma coisa?

HERA:
de repente o impacto ou até mesmo a maneira em que você enxerga as coisas
se fosse comunicado, explicado a real necessidade dessas normas
dar motivos para tais mudanças, pois o que parece é que tudo isso é feito como uma penalidade
a conscientização seria diferente

PESQUISADOR:
Mas houve um período de adaptação ou era proibido mas não era bloqueado, certo?

HERA:
aqui para nosso departamento
mas não houve a preocupação com o que os funcionários iriam pensar ou até mesmo uma orientação de como deveria ser o correto!
pelo menos foi o que percebi

PESQUISADOR:
Então o problema foi a falta de orientação e não no bloqueio?

HERA:
sim
totalmente
porque a empresa tem sim que se preocupar com a segurança de suas informações
se existem normas elas tem que serem seguidas, por mais que incomodem...

PESQUISADOR:
Você colocou no questionário que seria capaz de identificar um e-mail com vírus correto?

HERA:
pelo menos esses que aparecem por aqui sim
ou pelo menos sei o que é um e-mail suspeito

PESQUISADOR:
e também respondeu que não teve nenhuma treinamento ou palestra sobre segurança promovido pela empresa, certo?

HERA:
certíssimo

PESQUISADOR:
Então como aprendeu a fazer isso?

HERA:

conversas entre a galera
ou informações lidas na Internet

PESQUISADOR:
Os cursos que a empresas lhe pagou eram sobre segurança?

HERA:
ela nunca me pagou nenhum curso

PESQUISADOR:
Mesmo como foi colocada as normas de segurança, você considera válidas? ou sempre dá vontade de encontrar uma forma de burlar o sistema?

HERA:
bem, não conheço muito sobre esse tipo de forma, então, para evitar problemas no trabalho prefiro tentar seguir as orientações

PESQUISADOR:
agradeço sua participação

HERA:
disponha!!!

7.6 ENTREVISTA DIONE

PESQUISADOR:
No questionário você colocou que conhece as políticas de segurança da empresa. Poderia me dizer quais são?

ARES:
Acesso restrito a alguns sites. Especificamente aqueles com conteúdo pornográfico, sites de relacionamento, compartilhamento de vídeos ou arquivos, etc.

PESQUISADOR:
entendo!
E você considera que essas políticas ajudam ou atrapalham seu trabalho?

ARES:
Há pontos positivos e negativos. Como positivos eu ressaltaria o fato de que ao proibir o acesso a estas páginas o que a instituição objetiva é maior foco no trabalho e maior produtividade. Como ponto negativo eu ressalto que a política não deixa claro exatamente quais sites podem ser acessados. Concordo com o veto aos sites acima. Mas há alguns acesso que, mesmo se caracterizando como pessoais, contribuem para o conforto do indivíduo e, desde que feitos moderamente, em nada perturbam o bom andamento do trabalho. Então, como forma de melhorar a política eu sugeriria explicitar melhor a questão dos acessos proibidos e adotar algum instrumento que permita maior tolerância. Assim procedendo eu diria que contribuiria mais do que atrapalharia o meu trabalho.

PESQUISADOR:
Então as políticas de segurança foram impostas e não houve nenhum tipo de explicação?

ARES:
Exatamente. Não fomos chamados a opinar. Algum tipo de consulta é interessante. Sem "democratismos" (excesso de democracia). Mas acho que ouvir a opinião dos funcionários por meio de um formulário em que ele explicite os acessos de trabalho e pessoais que têm mais relevância seria necessário. A partir dele poder-se-ia então formular uma política de segurança.

PESQUISADOR:
"contribuem para o conforto do indivíduo" seria uma forma de ter o funcionário do lado da empresa?

ARES:
O exercício profissional hoje não pode ser mais encarado como uma linha de produção, exceto para aquelas funções que realmente trabalham como tal. O ideal seria que ele tivesse que comparecer fisicamente ao trabalho e realizar muitas tarefas a partir de outros locais que não o de trabalho (escritório pessoal, residência, em trânsito, etc.). Assim ele poderia administrar melhor o seu tempo entre o trabalho e seus afazeres e interesses pessoais. Infelizmente esta não é a relação de trabalho que nos é colocada. Então a informática, e seu uso, pode contribuir para esta compatibilização, isto é, entre trabalho e afazeres e vida pessoal. É neste sentido que eu utilizei a expressão "conforto do indivíduo".

PESQUISADOR:
Então podemos dizer que se as políticas se segurança fossem colocadas de outra forma a aceitação seria diferente?
De forma participativa dos funcionários!

ARES:
Bem, tenho que inferir o que você quis dizer com "outra forma" e também o que eu quero dizer com "aceitação diferente". Então, vamos lá.
continuarei a responder a questão acima

ENTREVISTA DIONE

PESQUISADOR:
de outra forma = com a participação dos funcionários

ARES:
Então, vamos lá. Por "outra forma" eu entendo com consulta, ou seja, exatamente o que você disse, participação dos funcionários.

PESQUISADOR:
aceitação diferente = melhor assimilado pelo corpo funcional

ARES:
Correto. Hoje acho que ela está sendo reativa (deveria ser pro-ativa). Virou objeto de brincadeiras. Mas não pode ser assim né?

PESQUISADOR:
o objetivo é detectar os focos do problema!

ARES:
Pra mim o foco do problema está na baixa democracia do processo de formulação da política. Consultas amplas são fundamentais.

PESQUISADOR:
Você colocou no questionário que seria capaz de identificar um e-mail com vírus correto? e também respondeu que não teve nenhuma treinamento ou palestra sobre segurança promovido pela empresa, certo?

ARES:
Sim, correto. E-mail com vírus geralmente é algo genérico e também com um anexo. Pedem que você o cliquem. Realmente, não fui treinado para este reconhecimento. A prática faz isto pra maioria das pessoas.

PESQUISADOR:
Existe algo relativo nas políticas de segurança?
Sobre os e-mails, SPAM...

ARES:
Defina melhor "relativo".

PESQUISADOR:
Nas políticas de segurança existe alguma orientação sobre abertura de email, SPAM?

ARES:
Se existe eu não tomei conhecimento. Pode ter sido por omissão da minha parte, se isto ocorreu a atitude não foi dolosa.

PESQUISADOR:
vc não leu o termo de compromisso?
mas assinou?

ARES:
Lembro-me de ter assinado um documento. Lembro da interdição de certos acessos, aqueles que mencionei na resposta à primeira pergunta. Não me lembro do conteúdo do restante. Mas creio que uma política não se implanta assim, com base num documento escrito e assinado em circunstâncias e momentos muito específicos. Ela precisar ser disseminada para ser bem aceita.

PESQUISADOR:
Entendo... faltou orientação no momento da implantação.

ARES:
E disseminação durante a sua vigência.....

PESQUISADOR:
e isso acabou gerando insatisfação do corpo funcional?

ARES:
Não apenas este fator específico, ou seja, baixa orientação e inexistência de disseminação. Como ela não é democrática desde o seu início, a probabilidade de boa aceitação é baixíssima. Logo, o corpo funcional fica insatisfeito.

PESQUISADOR:
muito obrigado pela participação

ARES:
Satisfação!

7.7 ENTREVISTA BOREAS

PESQUISADOR:
No questionário você colocou que conhece as políticas de segurança da empresa. Poderia me dizer quais são?

BOREAS:
Bloqueio de site
o não acesso a músicas
MSN

PESQUISADOR:
entendo!
E você considera que essas políticas ajudam ou atrapalham seu trabalho?

BOREAS:
em meu trabalho, especificamente
atrapalha
dentro do que eu uso e da consciência que eu tenho
essa forma de proibição
pra mim... é equivocada

PESQUISADOR:
Entendo!
e você cumpre essas políticas?

BOREAS:
hoje sim
antes não
mas o que eu acessava, antes
não era nada grave
não baixava
nada e nem ia em bate papo

PESQUISADOR:
entendo!
de que forma essas políticas foram colocas para você? houve uma palestra?

BOREAS:
não
proibiu e ponto... chegou uma cartinha lá e assinei
O suporte que deu algumas orientações.

PESQUISADOR:
e você acha que se fosse colocado de outra forma iria mudar alguma coisa?

BOREAS:
talvez... o sentimento das pessoas... no aspecto de aceitação, sim... tudo que vem de forma educada, explicativa, penso que a resposta é mais pro positivo do que pro negativo

PESQUISADOR:
ou seja, seria a mesma coisa colocada de forma diferente?

BOREAS:
isso
a importância da coisa, não foi revelada, e sim foi passado como uma proibição e ponto

PESQUISADOR:
Então não foi explicado o motivo dos bloqueios?

BOREAS:
não
só assinamos o termo

PESQUISADOR:
Mas sendo uma política de segurança imagino que o motivo é a segurança?
foi isso que você colocou no inicio da conversa!

BOREAS:
mas onde estava escrito isso? sei que é importante ante o dep. que trabalho. Caso contrário... não saberia

PESQUISADOR:
entendi... faltou informação... mas considerando que são as políticas de segurança não justifica?

BOREAS:
eu não sou muito entendida do assunto (computador) blz??
mas eu trabalho com uma galera que saca e de vez enquanto, troca figurinha
então, sem querer eu participo dessas informações trocadas.
então, somente aí, soube que era por segurança, entende???
porque foi falado de forma extra oficial, e no dep., nem todas estavam na sala no momento
portanto, vendo de forma macro, a informação não me chegou dessa maneira
agora
em se tratando do meu conhecimento.
do que eu tive acesso
eu acredito, que o que eu utilizava, não era prejudicial
por exemplo...
de repente, está também dentro do assunto "conhecimento"
fazer chegar a informação, entende?

PESQUISADOR:
entendo!
os fins não justificam os meios!
Então não houve uma preocupação em saber dos funcionários o que era importante... como passar essas políticas?

BOREAS:
eu não vi dessa forma... pra mim, realmente não houve

pra mim não
no meu ponto de vista...
não houve tal preocupação

PESQUISADOR:
podemos dizer então que o problema foi a falta de comunicação e não o bloqueio?
ou os dois?

BOREAS:
a falta de informação pesa mais.... mesmo assim, acredito que a maioria não tenha conhecimento que essa medida tomada pela empresa, seja para efeito de segurança. O aspecto levantado é a preocupação com quem está usando o mecanismo de trabalho para outra finalidade, foi dessa forma que foi passada.

PESQUISADOR:
Então podemos dizer que os bloqueios só serviram para gerar insatisfação no corpo funcional?

BOREAS:
sim

PESQUISADOR:
e a forma de amenizar essa situação seria?

BOREAS:
uma explicação de quem tem conhecimento tanto para os usuários quanto para a empresa. A conscientização tem que vir também dele, pois nem eles sabem o porque da proibição.
uma palestra, como você disse antes
aberta a perguntas
para o entendimento de todos

PESQUISADOR:
ok!
MUITO OBRIGADO!

BOREAS:
espero ter ajudado.

7.8 ENTREVISTA ARTEMIS

PESQUISADOR:
No questionário você colocou que conhece as políticas de segurança da empresa. Poderia me dizer quais são?

ARTEMIS:
sim, não acessar sites que possam comprometer a integridade das informações da entidade, como exemplos, sites de relacionamentos.

PESQUISADOR:
E você considera que essas políticas ajudam ou atrapalham seu trabalho?

ARTEMIS:
Particularmente sou totalmente favorável à adoção de integridade da informações de qualquer entidades, concordo plenamente com ações adotadas.

PESQUISADOR:
Então considera correto as políticas de segurança adotadas pela empresa?

ARTEMIS:
Sim estão corretas.
Inclusive neste momento, não sei se estou interferindo negativamente neste processo.

PESQUISADOR:
Como foi a implantação dessas políticas?

ARTEMIS:
Para o setor foi extremamente tranqüilo

PESQUISADOR:
Bom, segundo o conceito que você colocou não estamos comprometendo a integridade das informações da empresa, certo? ou errado?

ARTEMIS:
Acredito que não

PESQUISADOR:
Então podemos dizer que o bate-papo, usado de forma correta pode ser útil para a empresa?

ARTEMIS:
Sim, muito positivo, já utilizei o MSN como ferramenta de trabalho e tinha um resultado muito eficaz, inclusive de customização.

PESQUISADOR:
Então vamos chegar a um consenso...
As políticas de segurança proíbem o uso, mas estamos comprovando que pode ser útil...
utilizando de forma correta as ferramentas disponíveis podemos ter produtividade
ou seja, as políticas de segurança teriam que ser revistas em alguns pontos. Certo?

ARTEMIS:
Correto, utilizado com critérios, passa a ser uma ferramenta de trabalho eficaz e com informações em tempo real.
Acredito que a política adotado pela entidade poderia ser revista, mas com critérios bem definidos, como por exemplo: Qual o resultado da adoção desta ferramenta para o conjunto total da entidade, esta atitude não poderia beneficiar somente alguns setores

PESQUISADOR:
Se houvesse a participação dos funcionários da definição das políticas de segurança teríamos um melhor aproveitamento?

ARTEMIS:
Sou totalmente favorável à abertura de trabalho em equipe, ainda mais, quando o trabalho vai beneficiar a entidade como um todo, trazendo resultados esperados

PESQUISADOR:
Você respondeu no questionário que não sabe o que é um SPAM e nem identificar um possível vírus que chega por e-mail.
você acha que falta treinamento neste sentido?

ARTEMIS:
Pois é, como hoje as pessoas de um modo geral estão totalmente adaptadas ao mundo virtual, fico achando que o problema pode estar direcionado, como no meu caso, mas acredito que informações vinda através de treinamento, sempre são oportunas.

PESQUISADOR:
Você acha que os bloqueios não atrapalham na produtividade dos funcionários?

ARTEMIS:
desculpe, não entendi

PESQUISADOR:
os bloqueios a sites

ARTEMIS:
Definitivamente não, os profissionais aqui estão para desenvolver o que lhe foi confiado e não para ficar navegando na Internet.

PESQUISADOR:
Entendo...
Mas mesmo naqueles 5 minutos de relaxamento?
Que acontece com a maioria...

ARTEMIS:
Também não vamos radicalizar, acredito no bom senso, acredito que no horário de almoço, o funcionário poderia ter alguns acessos, como por exemplo, e-mail particular

PESQUISADOR:
sei..

mas sem abusos!
certo?

ARTEMIS:
correto

PESQUISADOR:
Mas da forma que esta colocado as políticas de segurança isso não é possível. Você não acha que dessa forma, o ambiente de trabalho fica "chato"?
ou seja, o funcionário se sente insatisfeito

ARTEMIS:
Não, não acho, tá certo que eu particularmente posso acessar os sites que desejar em minha residência, muitos não tem esta opção, mas não acho chato não, como por exemplo, sou fumante, aqui quando é possível fumo 01 cigarro, mas já trabalhei em empresas da qual isto não era permitido e tive que me adaptar aos procedimentos da empresa

PESQUISADOR:
Ter um funcionário insatisfeito pode comprometer a produtividade?

ARTEMIS:
Sim, pode, pode inclusive trazer danos à entidade, mas não consigo ver que o não acesso à Internet possa trazer insatisfações

PESQUISADOR:
vamos pesquisar!
o intuito do trabalho é exatamente este!
muito obrigado pela participação!

ARTEMIS: por nada

7.9 ENTREVISTA EOS

PESQUISADOR:
No questionário vc colocou que não conhece as políticas de segurança da empresa. Por quê?

EOS:
porque a empresa não tem!

PESQUISADOR:
entendo... como vc vê as normas que foram implantadas pela empresa? Sobre o bloqueio de alguns sites, e-mails, etc.

EOS:
De certa maneira eu acho certo, mas não da maneira como foi imposto e feito.!!! Gerou muita insatisfação da galera!!! Não tem beneficio nenhum!

PESQUISADOR:
Entendo...

EOS:
Sites específicos deveriam ter sido bloqueados! Mas no geral não!

PESQUISADOR:
Então o problema é na forma que foi feito e não no bloqueio?

EOS:
Isso...De repente tentaram mudar da água pro vinho! Não dá certo, todo ser humano tem dificuldade de se adaptar, não pode ser assim! O bloqueio de sites como orkut e jogos é necessário, eu acho, mas bloquear geral, além de sites, quer bloquear tempo tmb! Esse tipo de coisa gera muita insatisfação, tenho certeza que não gera retorno nenhum pra empresa!

PESQUISADOR:
Vc colocou no questionário que seria capaz de identificar um e-mail com vírus correto? e também respondeu que não teve nenhuma treinamento ou palestra sobre segurança promovido pela empresa, certo?

EOS:
Desde novo me interessei por Internet, e li em algum lugar que 95% dos vírus tem a terminação .exe ou .scr, acho que é isso!!! e sempre comecei a observar esses falsos e-mail...gente mal informada e vacilona que cai nisso...
Eu uso mais a lógica das coisas!!!

PESQUISADOR:
interessante

EOS:
Poh nada a ver... CLIKE AKI EM GANHE DINHEIRO!!! tem nego ke cai ainda!!!

PESQUISADOR:

vc já viu algum caso no trabalho?
ou acha que os bloqueios colocados irão diminuir este tipo de e-mail?

EOS:
No e-mail do trabalho? ou no pessoal

PESQUISADOR:
sim com vírus e alguém abrindo? não vc, mas outras pessoas!

EOS:
Nesse empresa ou outras ke já estive

PESQUISADOR:
Na empresa

EOS:
Aki não! Nunca ouvi falar!

PESQUISADOR:
você acha que os bloqueios colocados irão diminuir este tipo de e-mail? ou os vírus?

EOS:
Acho que não! Eu acho que se o objetivo era esse...
Seria bem mais aceitável de repente organizar uma palestra sobre o assunto com os funcionários e alertar.

PESQUISADOR:
Na sua opinião qual é o objetivo dos bloqueios?

EOS:
Cortar o acesso da Internet dos funcionários!!! Aff...sei lá... Acho que a empresa quer que os funcionários produza mais, deve ser...mas só gerou insatisfação!!! Querendo ou não, sempre tem um pouquinho do dia que vc não faz nada!!!

PESQUISADOR:
Então podemos dizer que os bloqueios só serviram para gerar insatisfação no corpo funcional?

EOS:
SIM

PESQUISADOR:
Para finalizar: Mesmo como foi colocada as normas de segurança, você considera válidas?

EOS:
NÃO!!! ta certo que eles estão vendo o lado da empresa... mas ela foi muito Bruto e rápido

PESQUISADOR:
blz! muito obrigado pelas respostas!

7.10 ENTREVISTA PEON

PESQUISADOR:
No questionário você colocou que não conhece as políticas de segurança da empresa. Por quê?

PEON:
porque nunca me passaram informação a respeito, a não ser, aquelas que restringem o uso da Internet...

PESQUISADOR:
certo... como você vê as normas que foram implantadas pela empresa? Sobre o bloqueio de alguns sites, e-mails, etc.

PEON:
acho que essas "restrições" são necessárias, pois muitos passam o dia inteiro em sites que não tem nenhum relacionamento com o trabalho.

PESQUISADOR:
você acha que atrapalha seu rendimento no trabalho?

PEON:
o meu não.
ops, se o meu trabalho depende de outros....
e esses outros brincam.... daí é complicado

PESQUISADOR:
ou seja... foi correto as medidas adotadas?

PEON:
eu acho que nnnnn... sim..!!!!

PESQUISADOR:
Você respondeu que quando recebe um SPAM no e-mail, não acontece nada! Onde você aprendeu sobre isto?

PEON:
bom, eu coloquei que não porque acho que não
não aprendi, só achismo.

PESQUISADOR:
sei... você já recebeu algum treinamento sobre segurança, ou como proceder em casos de riscos, pela empresa?

PEON:
já recebi instruções em caso de vírus....

PESQUISADOR:
você divide esses conhecimentos com seus companheiros de departamento?

PEON:
Sim, se bem que não tem muito com quem dividir.

PESQUISADOR:
A implantação do termo de responsabilidade e acesso ao e-mail da empresa mudou algum rotina no seu trabalho?

PEON:
não

PESQUISADOR:
Você acha que faltou algo, como palestras para esclarecimentos, no momento da implantação?

PEON:
acho que sim, ficou muito nas entrelinhas

PESQUISADOR:
mas no contexto geral tem alguma repercussão?

PEON:
como assim?

PESQUISADOR:
mesmo sem os esclarecimentos?

PEON:
em qual sentido?

PESQUISADOR:
normalmente os atos de proibição pela empresa, causam uma certa revolta...
que podem refletir na rotina de trabalho

PEON:
ah claro, houve constrangimentos...

PESQUISADOR:
você colocou que gosta de música. Se houvesse uma rádio interna da empresa, você escutaria?

PEON:
claro.

PESQUISADOR:
Muito obrigado pela entrevista!

PEON:
ok

7.11 ENTREVISTA EQUIPE DELTA

PESQUISADOR
Nossa pesquisa é sobre segurança de redes com foco principal no fator humano.

EQUIPE DELTA
Ok

PESQUISADOR
Gostaria de saber quais os maiores problemas que a empresa já teve?

EQUIPE DELTA
Semana passada tivemos um problema de perda de informações devida à uma falha nas rotinas de backup

PESQUISADOR
Além desta mais alguma?

EQUIPE DELTA
Em outra situação ocorreu um desvio no sistema devido à problemas de controle de acesso. Esses foram os maiores problemas relacionados a segurança creio eu

PESQUISADOR
Algum problema com abertura de e-mails com vírus?
Usuários que sabem senhas de outros?
Sites de hackers?
ou afins?

EQUIPE DELTA
É claro que sempre acontecem problemas de infecção de vírus por conta de abertura de mensagens infectadas. Entretanto, não tivemos grandes problemas gerados por conta disto ou na sua eliminação

PESQUISADOR
Estes problemas poderiam ser evitados?

EQUIPE DELTA
Esta questão é interessante. Há uma tradição aqui em pessoas cederem senhas de suas contas para outras pessoas, isso devido ao fato de suas tarefas poderem ser substituídas, isto é serem realizadas por outra pessoa. Contudo, foi implementado recentemente um termo onde cada usuário se compromete a manter em privacidade suas senhas.

PESQUISADOR
ou seja, os usuários não eram responsáveis por seus logins antes do documento ?

EQUIPE DELTA
Não. Definitivamente essa era uma prática muito comum aqui, e essa foi a forma encontrada para resolver esse problema de segurança.

PESQUISADOR
então podemos dizer que é o início das políticas de segurança?

EQUIPE DELTA
Agora sendo eles responsáveis pensarão duas vezes antes de ceder suas senhas

PESQUISADOR
existe alguma previsão para implantar? ou será sempre como neste caso, corretivo?

EQUIPE DELTA
Obviamente uma política de segurança é algo muito mais complexo do que um termo de responsabilidade. Porém isso indica um início de preocupação em relação a segurança da informação por parte dos dirigentes da empresa.

EQUIPE DELTA
Ainda não existe previsão para o início de um projeto de política de segurança. Mas devido aos últimos problemas, outras medidas de segurança deverão ser implementadas.

PESQUISADOR
Vc conhece o perfil dos seus usuários?

EQUIPE DELTA
O que seria exatamente o perfil dos usuários?
Conhecimento técnico??

PESQUISADOR
Escolaridade. Conhecimentos em Informática. idade

EQUIPE DELTA
De alguns sim

PESQUISADOR
daqueles que já apresentaram problemas ?

EQUIPE DELTA
Problemas de segurança??
ou problemas técnicos??

PESQUISADOR
sim. problemas de segurança?

EQUIPE DELTA
Veja bem, os incidentes de segurança estão relacionados com grande parte dos usuários. Não haveria como traçar um perfil específico destes usuários.

PESQUISADOR
ou seja, usuário é usuário?

EQUIPE DELTA

Certo, usuário é usuário

PESQUISADOR
Qual o problema causado por usuário que lhe deu mais trabalho???

EQUIPE DELTA
Acredito que o problema causado por usuário que deu mais trabalha foi uma certa vez que foi preciso recuperar várias informações no disco rígido que foram apagadas indevidamente

PESQUISADOR
Este usuário tinha conhecimentos técnicos? E formação acadêmica?

EQUIPE DELTA
Não era provido de muitos conhecimentos técnicos. Sua formação era superior

PESQUISADOR
Quando um funcionário é contratado existe algum teste de capacitação em informática? Você acha isso importante?

EQUIPE DELTA
Não existe nada neste sentido. O que acontece bastante é um funcionário declarar em seu curriculum que possui conhecimentos em informática suficientes para certa função, porém após ser contratado não se constata isso. Conforme a evolução da tecnologia conhecimentos em informática hoje são uma necessidade fundamental, talvez este teste seja sim algo que poderia ser importante na contratação de um funcionário.

PESQUISADOR
Interessante. A evolução tecnologia acontece sempre. Qual o procedimento com os usuários hoje? Existe algum tipo de treinamento?
O EQUIPE DELTA faz palestras de prevenção e atualização?

EQUIPE DELTA
Também não. Na realidade essa é uma questão que se volta para a política de segurança. Este tipo de treinamento comumente realizado através de palestras e workshops devem ser contemplados na política de segurança. Sem uma política de segurança não há uma estrutura sólida para se implementar outros projeto de segurança.

PESQUISADOR
se as políticas de seguranças são tão importantes porque ainda não foram implantadas?

EQUIPE DELTA
Acredito que deva por ser uma medida que traria uma grande mudança na forma e no hábito de trabalho das pessoas além de envolver recursos financeiros. Isso aliado ao fato de ser uma medida preventiva, e conforme sabemos aqui no Brasil, em sua grande maioria, as coisas funcionam de forma apenas corretiva

PESQUISADOR
Verdade.
Então, seguindo esta linha, na empresa hoje não existe nenhum tipo de treinamento, palestra ou workshop sobre segurança?

EQUIPE DELTA
Não existe.

PESQUISADOR
Poderia explicar, em linhas gerais, como funciona a segurança da rede hoje baseado no hardware e software?
servidores, backups, antivirus, firewall , acesso a Internet etc
pode ser um visão geral
a segurança da sua rede!

EQUIPE DELTA
Backup - Servidor central que realiza o backup diário de todos os servidores da rede
Antivírus - Servidor de Antivírus que gerencia estações da rede (atualizações, infecções, testes, etc)
Firewall - A rede é segmentada em subredes e protegida por um Firewall que controla o acesso entre elas
Controle de Acesso - O acesso a Internet é realizada através de um Servidor Proxy que controla cada acesso de acordo com uma política de acesso
Senhas de acesso a rede - Política de gerenciamento de senhas que controlam o período de alteração e histórico de senhas

PESQUISADOR: Nos questionários, a maioria dos usuários, responderam que conhecem as políticas de segurança da empresa. A que fator se deve essa resposta, já que não existem políticas de segurança?

EQUIPE DELTA:
Isso se deve ao fato de que os usuários associaram o termo de utilização como uma política de segurança da empresa.

PESQUISADOR:
entendo!

PESQUISADOR:
Em entrevistas individuais foi verificado que as políticas de segurança que os funcionários se referem, são na verdade, o termo de compromisso e o bloqueio no acesso a Internet de determinados sites e serviços. Podemos considerar este termo e os bloqueios com parte da política de segurança?

EQUIPE DELTA:
Sim, este termo pode ser considerado como um início. Porém espero que efetivamente este início de lugar a uma política de segurança consolidada.

PESQUISADOR:
Alguns questionaram a forma que foi implantada essas regras.
Como aconteceu essa implantação?

EQUIPE DELTA:
Aconteceu de uma forma não muito convencional e eficaz. Simplesmente solicitaram aos usuários que tomassem o devido conhecimento e a partir de então o termo vigoraria.

PESQUISADOR:
Você acha que a empresa foi muito incisiva na implantação?
se não quiser responder alguma pergunta, por questões pessoais, pode dizer!

EQUIPE DELTA:
Sim. Desta forma gerou grandes duvidas para os usuários que de repente se viram obrigados a seguirem certas normas, e ainda sem existir nenhum tipo de treinamento, palestra, ou qualquer outra forma que pudesse ser possível o conhecimento sobre o assunto segurança da informação

PESQUISADOR:
então ainda existe a possibilidade de uma palestra com orientação aos funcionários?

EQUIPE DELTA:
Acredito e espero que isso venha a acontecer. Isso e um fator crucial na implantação de uma política de segurança bem sucedida.

PESQUISADOR:
Você acha que o bloqueio a determinados site prejudica o desempenho no trabalho?

EQUIPE DELTA:
Não entendi a proposta da pergunta. Quero dizer, como prejudicaria o desempenho no trabalho de um usuário o bloqueio de um site que ele supostamente não seria permitido acessar?

PESQUISADOR:
A trabalho dos usuários com os bloqueios...
Isso!

EQUIPE DELTA:
O bloqueio de fato não os prejudicariam no desempenho de suas tarefas.

PESQUISADOR:
qual é o real motivo do bloqueio, é a segurança ou evitar que funcionários percam tempo com outros coisas?

EQUIPE DELTA:
De fato o bloqueio contempla os dois casos. Tanto por motivos de segurança quanto para evitar a ociosidade no trabalho.

PESQUISADOR:
Houve uma confusão nos questionários sobre o que é um SPAM e como identificar a extensão de um vírus no e-mail. Você acha que falta um canal de comunicação entre usuário e EQUIPE DELTA? Evitando assim alguns problemas e desgastes?

EQUIPE DELTA:
Sim, acho isso essencial. Este canal de comunicação seria contemplado nas palestras e treinamentos realizados na política de segurança.

PESQUISADOR:
Existe algum projeto em andamento para diminuir essa barreira?

EQUIPE DELTA:
Não. Como dito anteriormente, a política de segurança serve como uma estrutura sólida para a implantação de projetos desta natureza.

PESQUISADOR:
muito obrigado pelo tempo e pelas respondas.