UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
DEPARTAMENTO ACADÊMICO DE ELETRÔNICA – DAELN
CURSO DE ESPECIALIZAÇÃO EM GESTÃO DA TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

LUCIANA NOGUEIRA COSTA

A IMPORTÂNCIA DE UMA POLÍTICA DINÂMICA DE SEGURANÇA DA INFORMAÇÃO EM UMA EMPRESA DE GRANDE PORTE

MONOGRAFIA DE ESPECIALIZAÇÃO

Curitiba - PR
2014

LUCIANA NOGUEIRA COSTA

A IMPORTÂNCIA DE UMA POLÍTICA DINÂMICA DE SEGURANÇA DA INFORMAÇÃO EM UMA EMPRESA DE GRANDE PORTE

Trabalho de Conclusão de Curso apresentado na Universidade Tecnológica Federal do Paraná como requisito básico para a conclusão do Curso de Especialização em Gestão da Tecnologia da Informação e Comunicação.

Orientador Prof. Eng. Dr. Roberto Candido

Curitiba – PR
2014

Ata de Aprovação da monografia

Agradecimentos

Agradeço a Deus, por ter me sustentado em todos os momentos e por ter me alcançado, através de seu filho Jesus, autor e consumador da minha fé.

Ao meu orientador, Prof. Eng. Dr. Roberto Candido, pela paciência, disponibilidade e todo suporte a mim dispensado.

Às pessoas que ao longo da vida se mostraram figuras incentivadoras e me fizeram acreditar no valor e na importância que a busca pelo conhecimento representa em nossas vidas.

E ao meu querido esposo, pela força, paciência e incentivo que recebi até hoje, em especial ao longo de todo este período.

RESUMO

COSTA, Luciana. A importância de uma política dinâmica de segurança da informação em uma empresa de grande porte. 2014. 69 f. Monografia (Especialização em Gestão da Tecnologia da Informação e Comunicação) – Programa de Pós-Graduação em Tecnologia, Universidade Tecnológica Federal do Paraná. Curitiba, 2014.

Este estudo tem como propósito verificar a importância das regras de segurança da informação e o tratamento dado por uma organização de grande porte. Para isso foram pesquisadas teorias a respeito do assunto. A metodologia para a pesquisa foi a técnica de estudo de caso. Foram coletados dados e informações a respeito da política de segurança da informação utilizada atualmente, e que permitiram traçar o cenário da organização e confrontar informações com relação à teoria e a prática da empresa. Mediante o contexto estudado, foi possível identificar pontos de fragilidade e sugerir melhorias. Observou-se que a questão da segurança da informação na empresa estudada pode ser refinada e abordada precisamente com todos os integrantes da organização para que haja melhora no cenário atual.

PALAVRAS CHAVE: importância, Política de Segurança da Informação, Fragilidade.

ABSTRACT

COSTA, Luciana. A importância de uma política dinâmica de segurança da informação em uma empresa de grande porte. 2014. 69 f. Monografia (Especialização em Gestão da Tecnologia da Informação e Comunicação) – Programa de Pós-Graduação em Tecnologia, Universidade Tecnológica Federal do Paraná. Curitiba, 2014.

This paper proposal is to verify the importance of information safety rules in a big company and how the organization deals with it. In order to write about it, some theories about it were studied. The method used was cases research. Data and information were collected about the information safety policy currently used, which drove the organization scenario composition and made possible to compare the theories with the daily routine. Being before the found scenario, it was possible to identify some weak points and suggest some better practices. It was observed that the information safety in the company case can be improved and talked through with all the employees, so that the scenario can become stronger.

Key words: Importance, Information safety policy, weakness

NOLISTA DE SIGLAS

ABNT – Associação Brasileira de Normas Técnicas

FOR – Formulário

IP – Internet Protocol

NBR – Norma Brasileira

PCO – Procedimento Corporativo

PDI – Programa de Desenvolvimento Individual

TI – Tecnologia da Informação

VPN – Virtual Private Network

VOIP – Voz sobre IP

LISTA DE TABELAS

LISTA DE GRÁFICOS

SUMÁRIO

1. INTRODUÇÃO

A comunicação possui um papel crucial na história de evolução do homem e no desenvolvimento da sociedade. É através da comunicação que os seres humanos e até mesmo os animais partilham diferentes informações entre si, isso torna o ato de comunicar uma atividade essencial para a vida em sociedade.

A troca mútua de informações auxilia na transformação das crenças, valores e comportamentos, pois o homem necessita se relacionar com o mundo e isto só é possível através da comunicação. Na esfera organizacional, a comunicação é uma ferramenta estratégica com objetivo de melhorar a imagem da empresa e os resultados obtidos.

Independente da maneira como a comunicação é realizada, se há comunicação, existe uma informação a ser transmitida. A informação, que é um dos mais valiosos bens de uma organização, seja qual for o ramo de atividade ou porte. Alguns segmentos naturalmente tornam-se alvo de pessoas mal intencionadas, ladrões cibernéticos ou às vezes, inofensivos curiosos, que podem comprometer o negócio da organização. O fato é que as organizações precisam tratar o assunto de acordo com a relevância que têm na companhia.

A segurança da informação não é assunto somente de tecnologia. Há um conjunto de fatores e forças que precisam estar em sincronia para que renda o efeito esperado pela alta administração.

Mesmo que a organização tenha uma política de segurança da informação, há necessidade de revisá-la periodicamente e adequá-la frente às mudanças culturais, de mercado, de pessoas e ao avanço tecnológico que a esfera corporativa enfrenta. Ressaltando que os processos de informação atualmente estão totalmente vinculados à tecnologia, diariamente surgem novas formas de ataques cibernéticos, novos equipamentos e soluções para roubo de dados, fraude entre outros.

Dispor de uma política abrangente e que minimize as vulnerabilidades da organização diminuirá as chances do mau uso das informações e tende a aumentar a proteção de dados da empresa. A política deve ser desenhada única e exclusivamente para cada empresa, levando em consideração cada particularidade da organização bem como as estratégias do negócio.

1.1 PROBLEMA DE PESQUISA

É importante que uma empresa de grande porte possua uma política de Segurança da Informação, a questão é, qual é o grau de importância que regras e normas dinâmicas e segurança da informação possui na organização?

Orientações quanto à utilização dos recursos e sistemas de informática são importantes para toda organização, seja qual for o porte ou ramo de atuação. A maneira como a empresa trata a existência ou não de uma política, depende, entre outros fatores, da cultura da organização e também dos níveis de informação que circulam nos escritórios e plantas.

Estudar qual é a importância de uma política dinâmica de segurança da informação em uma Empresa de Grande Porte é o objetivo deste trabalho, analisando as regras e procedimentos existentes na empresa. O intuito é identificar o nível de segurança que uma organização de grande porte necessita.

1.2 DELIMITAÇÃO DO PROBLEMA

O objeto deste trabalho é uma empresa de grande porte, do ramo de telecomunicações, denominada neste trabalho “Empresa Telecom Alfa”, estabelecida na cidade de Curitiba, PR. O cenário atual da organização (ano de 2014) é o utilizado para o desenvolvimento deste estudo.

Para desenvolvimento da pesquisa foram entrevistados colaboradores que atuam nos níveis tático e estratégico da organização e espera-se identificar qual é a visão que os mesmos possuem com relação ao assunto, seus hábitos e qual é a relevância que atribuem à temática.

1.3 JUSTIFICATIVA

A proteção de informações das organizações é um fator estratégico e de competitividade. Desta forma, é imprescindível que a Organização defina a filosofia de segurança da informação e a partir dela, crie as estruturas necessárias para sua consolidação, informando e orientando os colaboradores, clientes e parceiros como dela se utilizarem.

Para construir um conjunto de regras e normas que consolidam uma política de segurança da informação, é preciso identificar e conhecer os possíveis impactos que as vulnerabilidades apresentam à empresa. A política somente, não garante a irrefutável segurança da empresa, ela é um dos fatores que contribui para tal.

Mesmo existindo uma política de segurança da informação, deve ser analisado se, as regras e normas estão alinhadas ao negócio e se podem ser melhoradas. Deve-se buscar a manutenção periódica em função de novas tecnologias, novos aplicativos e constante evolução de recursos.

1.4 OBJETIVOS

1.4.1 OBJETIVO GERAL

- Estudar a importância de uma Política Dinâmica de Segurança da Informação em uma Organização de Grande Porte;

1.4.2 OBJETIVOS ESPECÍFICOS

- Desenvolver uma pesquisa bibliográfica sobre Segurança da Informação;
- Analisar o alinhamento da Política de Segurança da Informação com as estratégias competitivas numa organização de grande porte;
- Avaliar a efetividade da Política de Segurança da Informação existente numa organização de grande porte;
- Criar um conjunto de diretrizes para a criação de uma política dinâmica de Segurança da Informação em uma Organização de grande porte, atendendo a ABNT NBR ISSO 27002:2005
- Propor um código de conduta a colaboradores e parceiros, a partir de uma política dinâmica de segurança em TI.

2. FUNDAMENTAÇÃO TEÓRICA

2.1. O QUE É SEGURANÇA DA INFORMAÇÃO

O conhecimento proveniente do processo de transformação da informação serve comumente de base para tomada de decisão nas organizações. Esta informação, quando adequada, e se gera valor para o negócio, propicia à empresa maior agilidade, competitividade, previsibilidade de ações futuras e torna-se um diferencial.

A informação existe de diversas formas e pode ser transmitida de inúmeras maneiras. A questão é, seja qual for o teor, a informação sempre terá um ou mais interessados, por este motivo, mantê-la segura pode minimizar as chances de que chegue a pessoas indevidas. Especificamente na esfera organizacional, nota-se que a segurança da informação possui um papel relevante para o equilíbrio do negócio, pelo menos no que diz respeito a possíveis riscos.

Segundo a ABNT NBR ISSO/IEC 27002: 2005, a Segurança da Informação caracteriza-se pela proteção da informação de diversas ameaças. Esta proteção garante a continuidade do negócio, além de minimizar os riscos que estas ameaças representam. Para que haja segurança nas informações é necessário que se tenha uma série de ações que contribuam para o alcance deste fim.

A prática de segurança da informação deve se estender por toda a organização e sua gestão pode ser realizada por todos os colaboradores

Segundo a ABNT NBR ISO / IEC 27002: 2005, Segurança da Informação é *"a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio".*

Informações organizacionais devem ser gerenciadas com muita cautela, pois podem ser utilizadas indevidamente, gerando transtornos e comprometendo o negócio como um todo. Manter seguras as informações não as torna imunes de riscos, mas minimiza as chances de que as mesmas sejam corrompidas de alguma forma.

Para PEIXOTO (2006, p. 37), *"O termo segurança da informação pode ser designado como uma área do conhecimento que salvaguarda os chamados ativos da informação, contra acessos indevidos, modificações não autorizadas ou até mesmo sua não disponibilidade".*

Não há como garantir que as informações da organização estejam cem por cento seguras, mas há um conjunto de regras e normas que podem auxiliar nesta tarefa. As tentativas de acessos indevidos, exposição, compartilhamento, roubo de informações podem ser frustradas se a empresa fizer uso de uma política de segurança da informação.

2.2. PRINCÍPIOS DA SEGURANÇA DA INFORMAÇÃO

Segundo Campos (2077, p. 17) *“existem três princípios básicos, nos quais um sistema de segurança da informação de baseia. São eles: confidencialidade, integridade e disponibilidade.”*

Figura 1 – Pilares Segurança da Informação
Fonte: Elaboração própria - Adaptado

- **Confidencialidade**

O caráter confidencial remete que a informação só deve ser acessada por pessoas autorizadas.

- **Integridade**

Manter a informação íntegra e inviolável é a premissa deste princípio. Para DANTAS (2011, p 11), “*garantir a integridade é permitir que a informação não seja modificada, alterada ou destruída sem autorização, que ela seja legítima e permaneça consistente*”. Se ocorrer algo que altere a informação original, ocorre também a quebra deste princípio, consequentemente a segurança da informação é afetada.

- **Disponibilidade**

Este pilar trata da informação disponível às pessoas autorizadas sempre que necessário. Nota-se que, o fato de determinada informação não estar disponível a alguém não caracteriza indisponibilidade, na aplicabilidade deste princípio. Somente há quebra do princípio quando pessoas devidamente autorizadas não conseguirem acesso à informação, seja por problemas ordem técnica ou até mesmo por consequência de ações do próprio usuário.

2.3. A POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Para DANTAS (2001), o documento caracterizado por política de segurança contempla orientações, regras, valores, princípios a respeito de como atingir um padrão desejável para garantir a segurança da informação. Em outras palavras, são orientações com relação ao que é ou não permitido relacionado a segurança da informação. O objetivo é minimizar ao máximo a probabilidade de quebra de qualquer um dos três princípios da segurança da informação. O conteúdo tem de ser escrito e disposto de maneira dinâmica e clara.

De acordo com a NBR ISSO/IEC27002(2005), é recomendado que a política seja revisada periodicamente e de forma planejada ou quando ocorrerem mudanças significativas, para assegurar a sua continua pertinência, adequação e eficácia.

2.4. CULTURA ORGANIZACIONAL E SEGURANÇA DA INFORMAÇÃO

De acordo com CHIAVENATO (2000),

> *“A cultura organizacional representa a maneira tradicional e costumeira de pensar e fazer as coisas, que são compartilhadas por todos os membros de organização”. A cultura da empresa evidencia sua identidade, sua personalidade”.*

A cultura é única e tem raízes profundas na história de cada empresa, valores e conceitos de seus fundadores muitas vezes são incorporados às características da organização e mudá-las não é tarefa fácil, nem rápida.

Para SCHEIN (1991), um dos pioneiros no conceito de “Cultura Organizacional”, toda cultura possui três níveis, a seguir:

- **Artefatos, comportamentos e produtos**

Estão relacionados aos elementos tangíveis da cultura, como vestuário, linguagem, rituais, comemorações e etc. Estes artefatos são visíveis por todos no comportamento dos membros de uma cultura. Podem ser reconhecidos por quem não é parte da mesma cultura.

- **Normas e valores**

Dizem respeito às hierarquias de valores na cultura e códigos de conduta. São as maneiras que os membros da cultura representam para si e para os outros.

- **Assunções básicas**

Comportamentos e crenças com fortes raízes na mente e na programação dos indivíduos. Essas assunções constituem a essência da cultura, e geralmente são tão bem integradas na dinâmica da cultura que chegam a ser difíceis de serem detectados pelos membros da cultura.

Levando em consideração o grau de importância que a cultura organizacional possui, se houver necessidade de alterar esta cultura, os gestores têm de ser capazes de criar um novo contexto, no qual seja possível às pessoas agirem voluntariamente e de acordo com o que a empresa espera.

Trabalhar este conjunto de fatores com intuito de incorporar a ele a necessidade e a importância de se ter Segurança da Informação é uma tarefa difícil, mas que no longo prazo, pode garantir a sobrevivência de conceitos básicos sobre o assunto. Possibilitará também a continuidade das ações de segurança e diminuirá os riscos de que, com mudanças de gestão, algumas práticas sejam deixadas de lado.

2.5 IDENTIFICAÇÃO E ANÁLISE DE RISCOS

Para FONTES (2008), ameaça é qualquer evento capaz de prejudicar o andamento normal das atividades de uma organização. Já o risco, é a possibilidade dessa ameaça se concretizar.

Quando da busca por identificar os riscos aos quais a empresa está sujeita, é necessário levar em consideração os objetivos da companhia e suas estratégias de

negócio. Não há como atuar em algo sem que tenha sido identificado, tão pouco mensurado seu impacto para a organização.

Outro fator que deve ser levado em consideração diz respeito à legislação e regulamentação vigente. Os riscos estão relacionados a agentes diretos e indiretos à organização, desta maneira devem ser analisados todos os pontos e vieses que podem existir entre a empresa e parceiros, sejam eles fornecedores, clientes e prestadores de serviços. Atentar quanto ao sigilo de informações e cumprimento de normas e leis.

A análise de riscos tem por objetivo identificar as ameaças e quantificar os riscos inerentes à segurança da informação, além do desenvolvimento de um plano de ação (CARVALHO; SILVA; TORRES, 2003).

Uma vez identificados os riscos, faz-se necessário elaborar estratégias para atuar em cada ponto identificado, o nível de investimento e aprofundamento dependerá dos danos que podem ser causados à organização. A análise e avaliação dos riscos devem ser realizadas periodicamente.

Inúmeras são as variáveis que integram o conjunto Segurança da Informação, neste trabalho será abordado o quesito Política de Segurança da Informação, para aplicação em uma empresa de grande porte.

2.6 EMPRESA OBJETO DO ESTUDO

A organização, objeto deste estudo, atua no mercado nacional de telecomunicações. Possui atualmente em seu quadro funcional 600 colaboradores, entre efetivos, terceiros e estagiários.

A planta de Curitiba conta com o centro administrativo e a fábrica. Nos estados de São Paulo, Bahia, Rio Grande do Sul, Recife e Distrito Federal há escritórios de vendas. As informações corporativas são acessadas via Virtual Private Network (VPN) nos escritórios e pelos colaboradores que fazem uso de equipamentos da empresa, como *smartphones*, *lap tops*, *tablets* entre outros.

3. METODOLOGIA

Para o desenvolvimento deste trabalho, será realizada uma análise da política de segurança da informação existente na “Empresa Telecom Alfa”, bem como analisar o nível e a efetividade da segurança existente atualmente e o padrão que se pretende alcançar.

BONOMA (1985, p. 203) coloca que o "estudo de caso é uma descrição de uma situação gerencial". Desta forma, se desenvolverá um estudo de caso, de caráter exploratório e descritivo qualitativo, que utilizou como procedimentos técnicos as pesquisas explicativas realizadas, pesquisa bibliográfica e a análise documental.

Para coleta de dados, serão aplicados questionários com questões fechadas com os gestores das áreas. Será também estudada a possibilidade de aplicação de questionários a uma amostra de colaboradores, para auxiliar na identificação de vulnerabilidades. O questionário constitui perguntas fechadas, padronizadas e é um instrumento de pesquisa mais adequado à quantificação, pois propicia comparações com outros dados relacionados ao tema pesquisado.

3.1. PROPOSTA DE DESENVOLVIMENTOE CRONOGRAMA

O desenvolvimento deste trabalho será realizado utilizando como objeto de estudo uma empresa de grande porte, denominada no trabalho como “Empresa de Telecom Alfa”, atuante no ramo de telecomunicações. Estabelecida com sua industrial na cidade de Curitiba, possui escritórios nos estados São Paulo, Bahia, Rio Grande do Sul e Recife.

A organização conta com aproximadamente 600 colaboradores, entre funcionários efeitos, estagiários e terceirizados.

4. LEVANTAMENTO DE DADOS E ANÁLISE DOS RESULTADOS

4.1 SISTEMA DE GERENCIAMENTO DE DOCUMENTOS - COLABORADORES

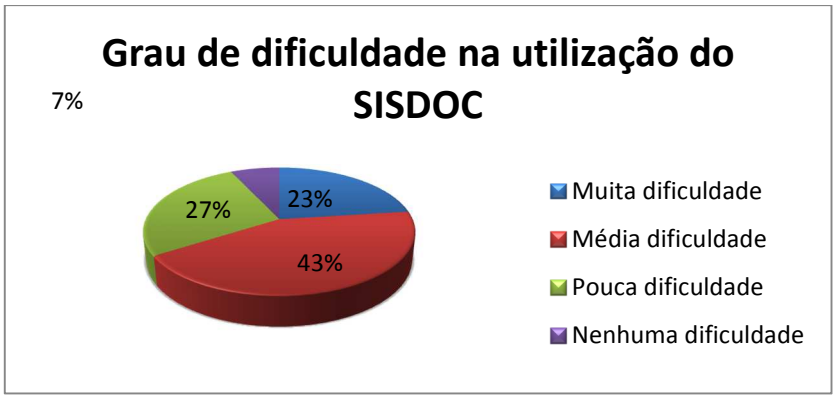
A empresa estudada possui regras e normas que disciplinam o uso da Tecnologia da Informação pelos colaboradores e parceiros, em um documento eletrônico chamado de SISDOC, que somente pode ser acessado com uso de um *login* devidamente registrado. Esta situação pode ser inibidora ao acesso às informações, motivo pelo qual, se buscou levantar o grau de dificuldade encontrada com 70 colaboradores administrativos sobre o uso do SISDOC.

A pesquisa foi realizada através do Googledocs, o formulário está disponível como APÊNDICE 1.Os colaboradores entrevistados integram áreas operacionais administrativas.

Através das respostas foi possível identificar que a maioria dos colaboradores possui certa dificuldade ao utilizar o sistema, conforme dados a seguir.

VOCÊ ENCONTRA DIFICULDADE QUANDO UTILIZA O SISDOC?	FREQUÊNCIA	PERCENTUAL
Muita dificuldade	16	23%
Média dificuldade	30	43%
Pouca dificuldade	19	27%
Nenhuma dificuldade	5	7%
Total	70	100%

Fonte: Elaboração Própria
Tabela 1: Grau de dificuldade

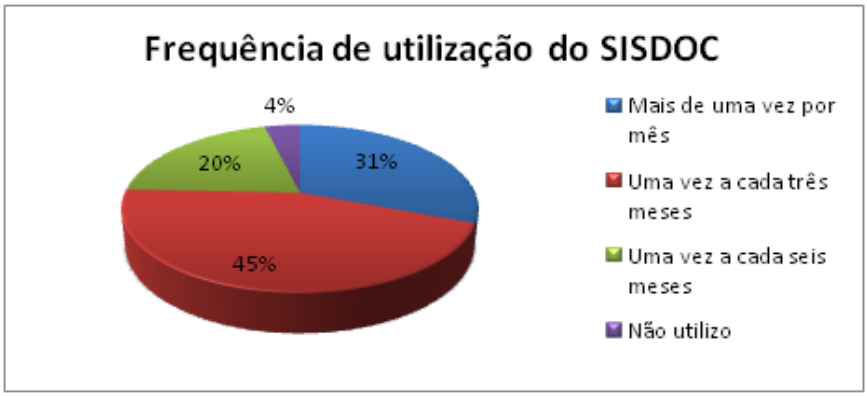


Fonte: Elaboração Própria
Gráfico 1 – Grau de dificuldade

A consulta continua a documentos da empresa é importante para seguirem-se as normas estabelecidas. No caso da TI esta consulta deve ser uma rotina, pois mudanças são extremamente rápidas. Por este motivo foi feito ao mesmo grupo de entrevistados a questão sobre qual a periodicidade de consulta as normas pertinentes, constatando-se que a maioria o faz a cada três meses.

COM QUE FREQUÊNCIA VOCÊ O UTILIZA?	FREQUÊNCIA	PERCENTUAL
Mais de uma vez por mês	17	24%
Uma vez a cada três meses	35	50%
Uma vez a cada seis meses	16	23%
Não utilizo	2	3%
Total	70	100%

Fonte: Elaboração Própria
Tabela 2: Frequência de utilização

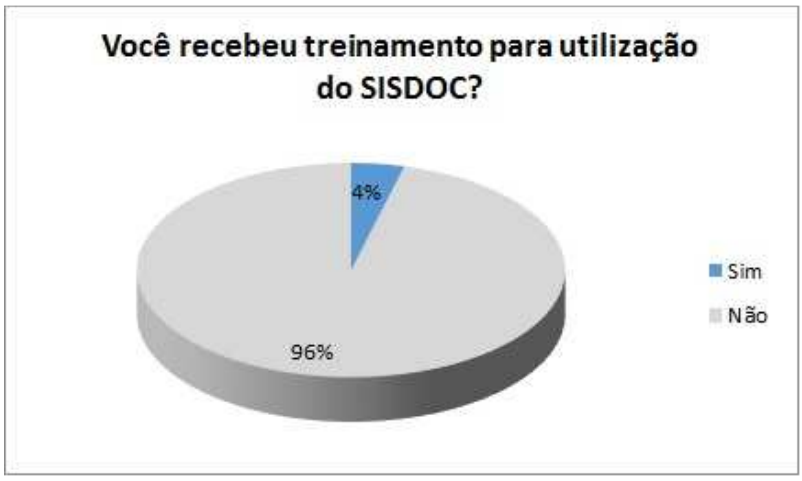


Fonte: Elaboração Própria
Gráfico 2 – Frequência de utilização

A correta utilização de ferramentas de TI exige treinamentos e capacitação contínua, desta forma verificar se os colaboradores tiveram treinamentos para uso do SISDOC, é importante para contexto da pesquisa. Desta entrevista observou-se que a maioria dos colaboradores não teve treinamento.

VOCÊ RECEBEU TREINAMENTO PARA UTILIZAÇÃO DO SISDOC?	FREQUÊNCIA	PERCENTUAL
Sim	3	4%
Não	67	96%
Total	70	100%

Fonte: Elaboração Própria
Tabela 3: Treinamento para utilização

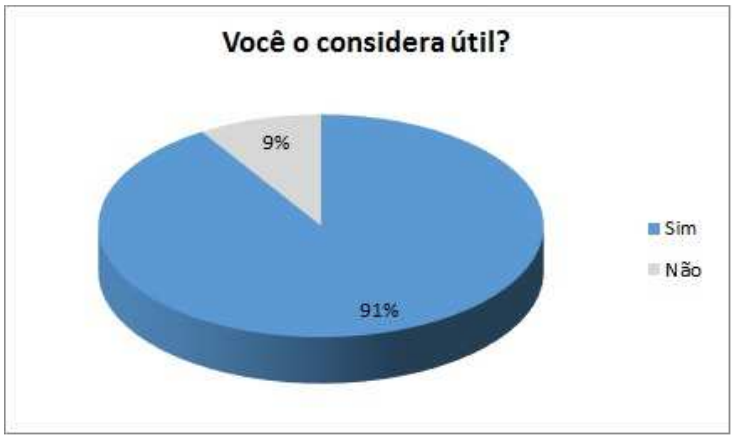


Fonte: Elaboração Própria
Gráfico 3 – Treinamento

Outra informação importante para a pesquisa é o entendimento se o SISDOC é realmente útil para os colaboradores, desta questão observou-se que 91% dos entrevistados assim o considera.

VOCÊ O CONSIDERA ÚTIL?	FREQUÊNCIA	PERCENTUAL
Sim	64	91%
Não	6	9%
Total	70	100%

Fonte: Elaboração Própria
Tabela 4: Utilidade do Sistema



Fonte: Elaboração Própria
Gráfico 4 – Utilidade do sistema

4.2 REGRAS E PROCEDIMENTOS INTERNOS - COLABORADORES

O SISDOC é o sistema que disponibiliza todos os Procedimentos Corporativos (PCOs) aos colaboradores, inclusive o de Segurança em TI, foco deste estudo.

Dos 130 colaboradores administrativos, foi realizada uma pesquisa, através do Googledocs, com 70 destes funcionários a respeito das práticas e utilização dos recursos de TI. As questões foram elaboradas tendo como base o PCO de Segurança em TI

O objetivo da pesquisa é identificar as práticas relacionadas aos recursos de Informática no dia a dia dos colaboradores.

O questionário foi elaborado com assuntos tratados no PCO, possui 10 questões, 9 de múltipla escolha e 1 questão cuja resposta deve ser dada no formato de tempo.

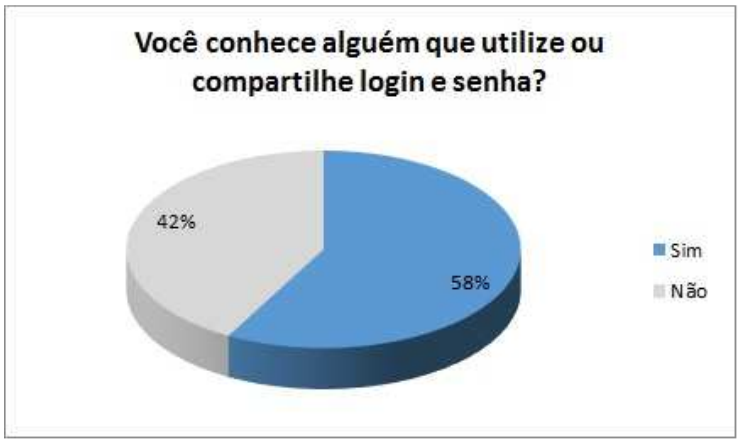
O procedimento está disponível como ANEXO 1e o questionário está disponível como APÊNDICE 2.

As questões foram elaboradas de maneira que as respostas fossem indiretas, ou seja, perguntando aos entrevistados se conhecem alguém que faça determinada ação pode evitar que o respondente se sinta exposto com suas respostas

O compartilhamento de *login* é extremamente perigoso ao colaborador e principalmente a empresa, pois esta prática abre portas para todo tipo de ingressos indevidos ao sistema. Desta forma o questionamento feito revelou que 50% conhecem alguém que já tenha feito este procedimento na empresa,

VOCÊ CONHECE ALGUÉM QUE UTILIZE OU COMPARTILHE LOGIN E SENHA?	FREQUÊNCIA	PERCENTUAL
Sim	41	58%
Não	29	42%
Total	70	100%

Fonte: Elaboração Própria
Tabela 5: Compartilhamento de *login* e senha



Fonte: Elaboração Própria
Gráfico 5: Compartilhamento de *login* e senha

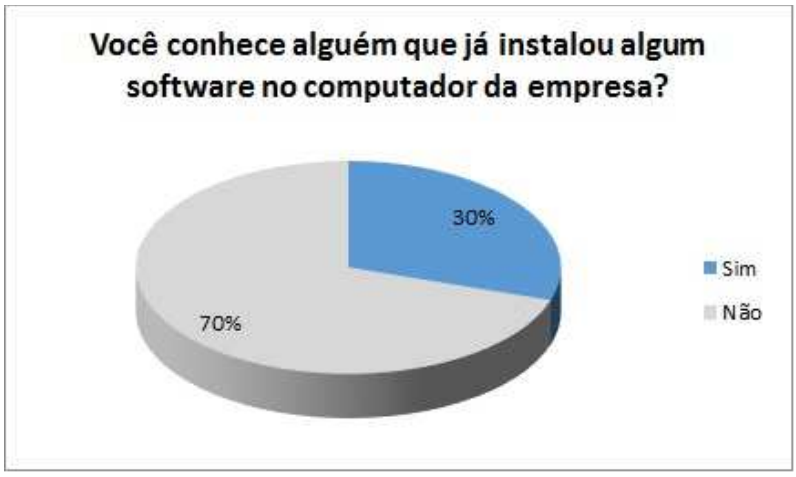
O Procedimento informa que senhas de acesso são pessoais e intransferíveis. Não devem ser compartilhadas, esta proibição é enfática no documento e no caso de infração à esta regra a pessoa que o fizer é sujeito a advertência ou outras medidas cabíveis.

A instalação de *software*s não autorizados pode ser um risco ao sistema da empresa, portanto o conhecimento desta prática é essências para os estudos realizados, desta questão 70% dos respondentes negam conhecer alguém que tenha realizado tal procedimento.

A instalação de *software*s não autorizados pode ser um risco ao sistema da empresa, portanto o conhecimento desta prática é essências para os estudos realizados, desta questão 70% dos respondentes negam conhecer alguém que tenha realizado tal procedimento.

VOCÊ CONHECE ALGUÉM QUE JÁ TENHA INSTALADO ALGUM SOFTWARE NO COMPUTADOR DA EMPRESA?	FREQUÊNCIA	PERCENTUAL
Sim	21	30%
Não	49	70%
Total	70	100%

Fonte: Elaboração Própria
Tabela 6: Instalação de *software*



Fonte: Elaboração Própria
Gráfico 6: Instalação de *software*

O uso de *e-mail* corporativo para fins pessoais é uma prática aceita pela corporação, embora deva existir limites do que é enviado, afinal a imagem corporativa está envolvida. Desta forma, com a entrevista observa-se que 90% dos entrevistados conhece alguém que utilize o *e-mail* da empresa para assuntos particulares.

VOCÊ CONHECE ALGUÉM QUE COSTUME UTILIZAR O E-MAIL DA EMPRESA PARA TRATAR DE ASSUNTOS PARTICULARES?	FREQUÊNCIA	PERCENTUAL
Sim	63	90%
Não	7	10%
Total	70	100%

Fonte: Elaboração Própria
Tabela 7: Utilização do *e-mail* da empresa para fins particulares

Fonte: Elaboração Própria
Gráfico 7: Utilização do *e-mail* da empresa para fins particulares

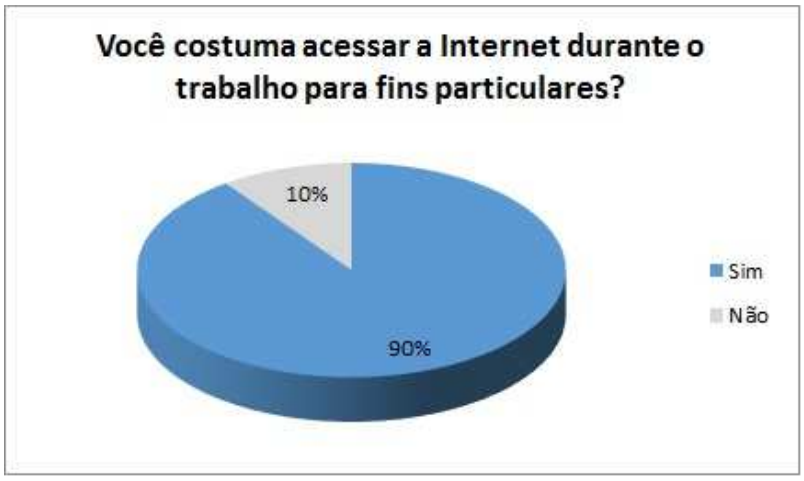
Não há proibição absoluta com relação à utilização do *e-mail* corporativo para fins particulares, desde que os colaboradores não reenviem *e-mail*s do tipo corrente, aviso de vírus, avisos da Microsoft/AOL/Symantec, criança desaparecida, entre outros.

Quanto à Internet, os colaboradores foram questionados se acessam a internet durante o expediente de trabalho para fins particulares e 90% dos respondentes afirmaram acessar a internet durante do trabalho. Este percentual corresponde a 63 dos entrevistados.

Não há segurança na efetividade das respostas, o assunto pode ser objeto de um novo estudo, que identifique e mensure o impacto que o acesso e permanência à internet pode causar no rendimento do colaborador e consequentemente, para a organização.

VOCÊ COSTUMA ACESSAR A INTERNET DURANTE O HORÁRIO DE TRABALHO PARA FINS PARTICULARES?	FREQUÊNCIA	PERCENTUAL
Sim	63	90%
Não	7	10%
Total	70	100%

Fonte: Elaboração Própria
Tabela 8: Acesso a internet para fins particulares



Fonte: Elaboração Própria
Gráfico 8: Acesso a internet para fins particulares

As regras quanto ao uso da internet não são proibitivas, a organização menciona que o acesso à internet deve ser realizado para fins corporativos, para o enriquecimento intelectual de seus colaboradores ou como ferramenta para busca de informações que venham contribuir para o desenvolvimento das atividades destes.

O uso para fins particulares é permitido, mediante o consentimento do responsável pelo setor, fica restrito à consulta de movimentação bancária e ao acesso ao *e-mail* pessoal, estando vedadas práticas abusivas tais como acesso ou a circulação de correntes, material pornográfico, difamatório ou ilegal entre outros.

A pesquisa apresentou uma questão aberta e refere-se ao tempo estimado que cada respondente permanece conectado à Internet durante o expediente. O tempo médio apurado foi 19,7 minutos.

Não há parâmetros que permitam avaliar se o tempo utilizado na Web afeta o desempenho das atividades, pois a empresa não possui regras com relação ao tempo que cada colaborador pode utilizar para acesso com fins particulares.

As informações corporativas têm alto nível de sigilo, e certamente não deve ser compartilhadas com o público externo, na entrevista a maioria dos respondentes afirma não conhecer ninguém que já tenha compartilhado informações internas com pessoas de fora da organização.

VOCÊ CONHECE ALGUÉM QUE JÁ TENHA COMPARTILHADO INFORMAÇÕES INTERNAS COM PESSOAS DE FORA DA EMPRESA?	FREQUENCIA	PERCENTUAL
Sim	14	20%
Não	56	80%
Total	70	100%

Fonte: Elaboração Própria
Tabela 9: Compartilhamento de informações internas

Fonte: Elaboração Própria
Gráfico 9: Compartilhamento de informações internas

A organização disponibiliza alguns *softwares* de comunicação instantânea, e acordo com a pesquisa, 85% dos entrevistados utiliza alguma das ferramentas disponibilizadas.

VOCÊ UTILIZA ALGUM SOFTWARE DE COMUNICAÇÃO INSTANTÂNEA?	FREQUENCIA	PERCENTUAL
Sim	60	85%
Não	10	15%
Total	70	100%

Fonte: Elaboração Própria
Tabela 10: Utilização *software* de comunicação instantânea

Fonte: Elaboração Própria
Gráfico 10: Utilização *software* de comunicação instantânea

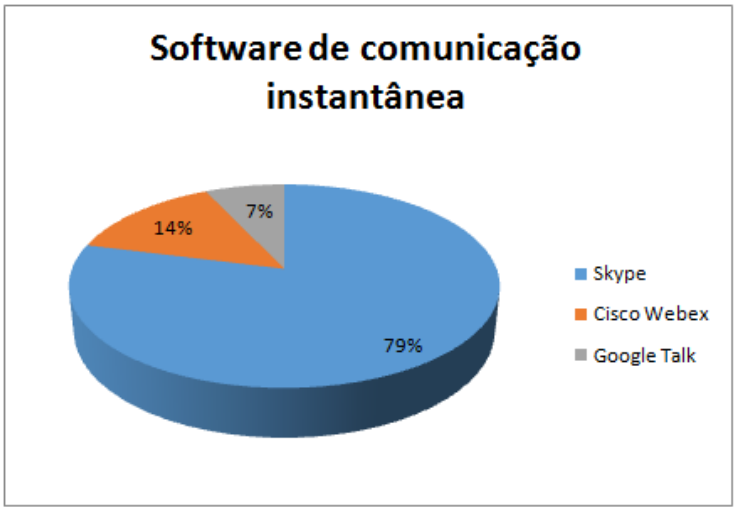
Foi evidenciado que o *software* mais utilizado é o Skype, com 55 entrevistados, o que representa 79% dos respondentes. Na sequência, com 14% e 7% o Cisco Webex e Google Talk respectivamente.

QUAL? (SOFTWARE DE COMUNICAÇÃO INSTANTÂNEA VOCÊ UTILIZA)?	FREQUENCIA	PERCENTUAL
Skype(1)	55	79%
Cisco Webex(2)	10	14%
Google Talk(3)	5	7%
Total	70	100%

Fonte: Elaboração Própria
NOTAS:

(1) O Skype é um *software* que permite comunicação através da web em distintas regiões do mundo. É possível realizar chamadas gratuitas de voz, enviar mensagens de chat e compartilhar arquivos com outras pessoas. O acesso pode ser feito através de um aparelho celular, computador ou em uma TVcom o Skype instalado.
(2) Cisco Webex é um aplicativo que permite a realização de apresentações, compartilhamento de documentos, demonstração de aplicativos, controle de desktop remoto ou oferece a possibilidade de que o usuário entregue o controle para permitir que outra pessoa se apresente.
(3) Google Talk é um serviço de mensagens instantâneas e de VoIP, baseado em um protocolo aberto, chamado Jabber. Permite a realização de chamadas, envio de mensagens instantâneas, transferência de arquivos e mensagens de voz.

Tabela 11: *Software* utilizado

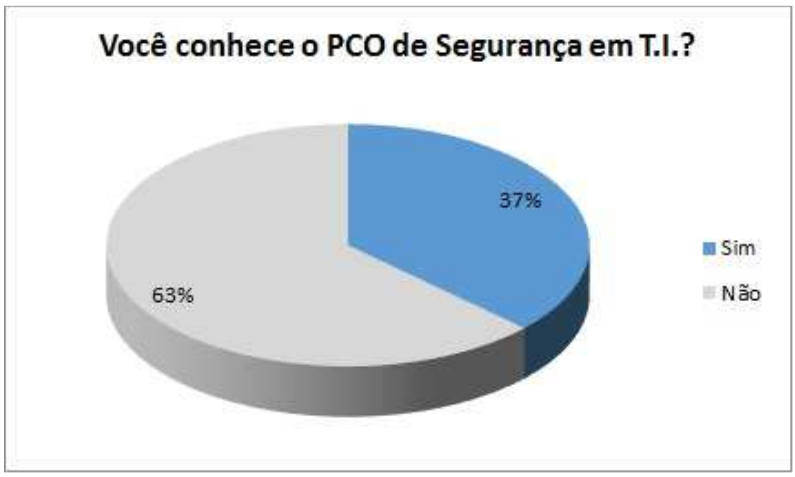


Fonte: Elaboração Própria
Gráfico11: Software utilizado

Para que o Procedimento Corporativo de Segurança de TI seja realmente eficiente e eficaz e é preciso que os usuários o conheçam com profundidade de detalhes. Desta forma a questão formulada buscou saber se os entrevistados o conheciam, e 63% alegaram completo desconhecimento.

VOCÊ CONHECE O PROCEDIMENTO CORPORATIVO DE SEGURANÇA EM TI?	FREQUENCIA	PERCENTUAL
Sim	26	37%
Não	44	63%
Total	70	100%

Fonte: Elaboração Própria
Tabela 12: Conhecimento do PCO de segurança em TI



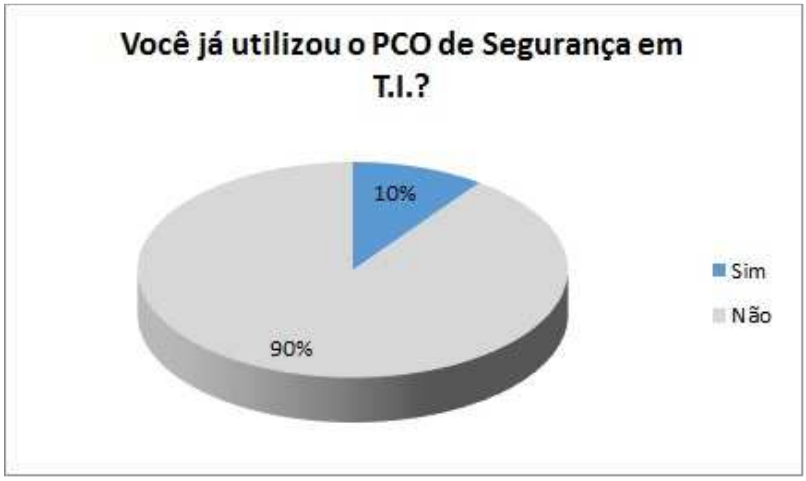
Fonte: Elaboração Própria
Gráfico 12: Conhecimento do PCO de segurança em TI

O procedimento possui um item que trata a respeito da divulgação do documento. De acordo com as regras internas, o procedimento deve ser divulgado aos colaboradores através do “SISDOC”.

A situação que se desenha, durante a pesquisa é curiosa, pois percebe-se que os procedimentos não são efetivamente usados, conforme comprova a questão abaixo, onde 90% dos entrevistados reconhece não utilizá-lo.

VOCÊ JÁ UTILIZOU O PROCEDIMENTO CORPORATIVO DE SEGURANÇA EM TI?	FREQUENCIA	PERCENTUAL
Sim	7	10%
Não	63	90%
Total	70	100%

Fonte: Elaboração Própria
Tabela 13: Utilização do PCO de segurança em TI

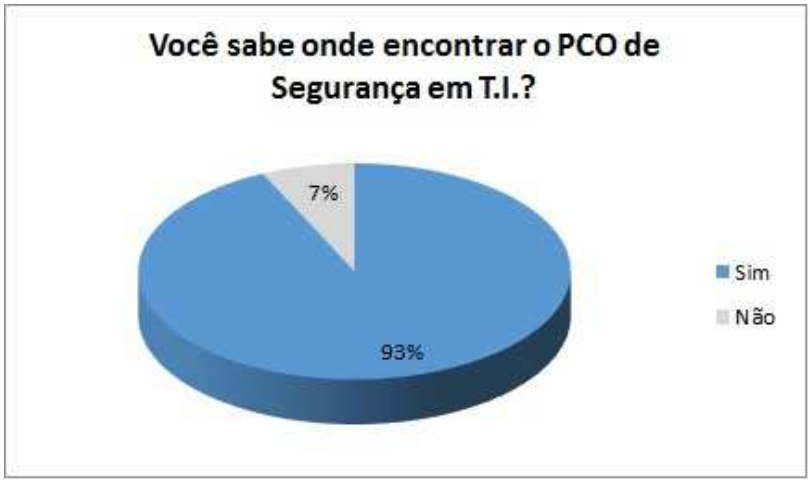


Fonte: Elaboração Própria
Gráfico 13: Utilização do PCO de segurança em TI

A falta do uso dos PCOs, poderia estar vinculado ao desconhecimento de onde encontrá-lo, o que motivou a realização da próxima pergunta, que indicou exatamente o contrário, pois todos sabem onde eles estão, segundo 93% dos respondentes.

VOCÊ SABE ONDE ENCONTRAR O PCO DE SEGURANÇA EM TI?	FREQUENCIA	PERCENTUAL
Sim	65	93%
Não	5	7%
Total	70	100%

Fonte: Elaboração Própria
Tabela 14: Localização do PCO de segurança em TI



Fonte: Elaboração Própria
Gráfico 14: Localização do PCO de segurança em TI

4.3 GESTORES - PRÁTICAS E USO DOS RECURSOS DE TI

A segunda fase do processo de busca de informações foi de gerar uma pesquisa junto aos gestores da empresa, e observar qual o ponto de vista do grupo sobre a Gestão de TI e posteriormente confrontar resultados com o que foi obtido com os colaboradores.

Dentre os 30 gestores existentes na organização, 25 responderam a um questionário elaborado com base no Procedimento de Segurança de TIA quantidade de respondentes representa 83% dos gestores.

O questionário aplicado possui questões de múltipla escolha e foram elaboradas abordando tópicos presentes na Política de Segurança da Informação da empresa.

Para a maioria das questões foi estipulado um critério de pontuação, no qual o intervalo varia de 1 a 5 pontos, sendo:

- 1 para quando o gestor discordar totalmente da afirmação da questão;

- 2 para quando discordar parcialmente;
- 3 para quando não concordar nem discordar;
- 4 para quando concordar parcialmente e
- 5 para quando concordar totalmente.

A primeira questão levantada junto aos Gestores trata-se do tempo que estão vinculados a organização e observou-se que a maioria possui de 11 a 15 anos e nenhum possui menos de 5 anos. Esta questão permite imaginar que todos devem conhecer com detalhes o que acontece internamente aos seus setores gerenciais.

TEMPO DE EMPRESA	FREQUÊNCIA	PERCENTUAL
De 0 a 5 anos	0	0%
De 6 a 10 anos	7	28%
De 11 a 15 anos	13	52%
De 16 a 20 anos	4	16%
Mais de 20 anos	1	4%
Total	25	100%

Fonte: Elaboração Própria
Tabela 15: Tempo de empresa

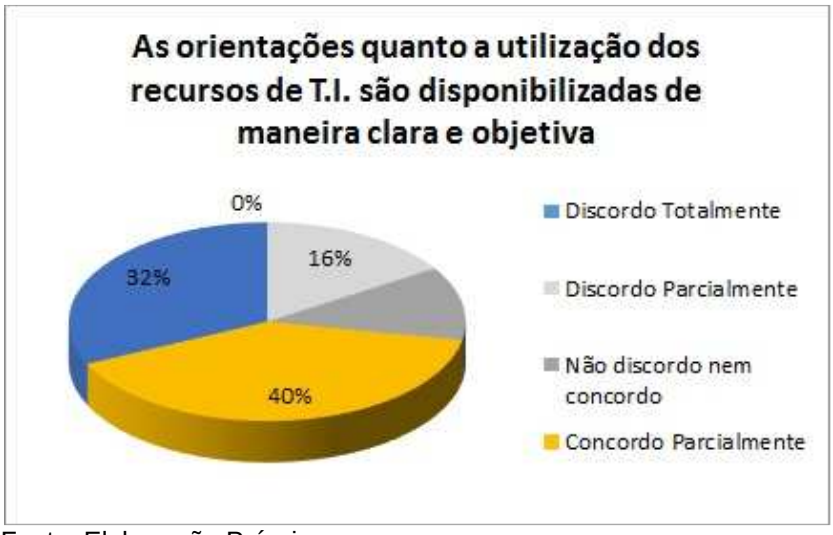
Fonte: Elaboração Própria
Gráfico 15 – Tempo de empresa

Um bom sistema de TI corporativo implica necessariamente em investimentos constantes em equipamentos, *software*s, treinamentos, etc. Para tanto os Gestores

foram questionados a respeito dos recursos de TI se são, em seu entendimento, disponibilizados de maneira clara e objetiva, 40% concorda parcialmente.

AS ORIENTAÇÕES QUANTO A UTILIZAÇÃO DOS RECURSOS DE TI SÃO DISPONIBILIZADAS AOS COLABORADORES DE MANEIRA CLARA E OBJETIVA	FREQUÊNCIA	PERCENTUAL
Discordo Totalmente	0	0%
Discordo Parcialmente	4	16%
Não discordo nem concordo	3	12%
Concordo Parcialmente	10	40%
Concordo Totalmente	8	32%
Total	25	100%

Fonte: Elaboração Própria
Tabela 16: Orientações sobre os recursos de TI

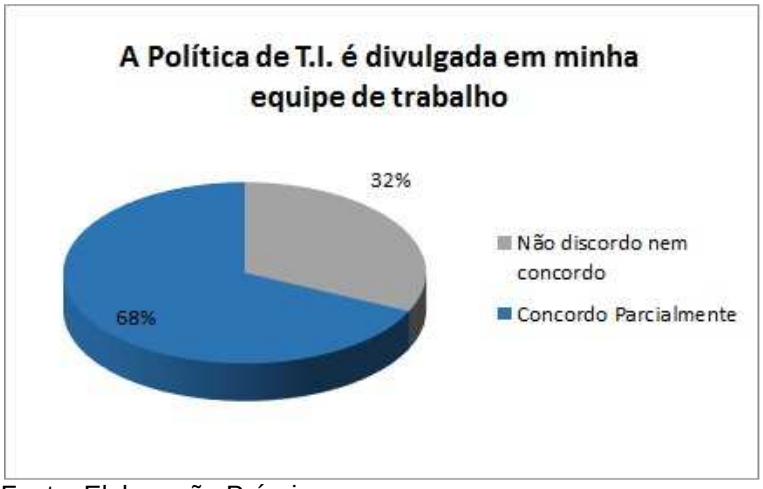


Fonte: Elaboração Própria
Gráfico 16 – Orientações sobre os recursos de TI

A próxima indagação feita aos gestores trata sobre a forma de divulgação da Política de TI aos colaboradores, que segundo os gestores é feita continuamente segundo 68% dos participantes.

A POLÍTICA DE SEFURANÇA DE TI É AMPLAMENTE DIVULGADA EM MINHA EQUIP DE TRABALHO	FREQUÊNCIA	PERCENTUAL
Discordo Totalmente	0	0%
Discordo Parcialmente	0	0%
Não discordo nem concordo	8	32%
Concordo Parcialmente	17	68%
Concordo Totalmente	0	0%
Total	25	100%

Fonte: Elaboração Própria
Tabela 17: Divulgação da política de TI nas equipes de trabalho

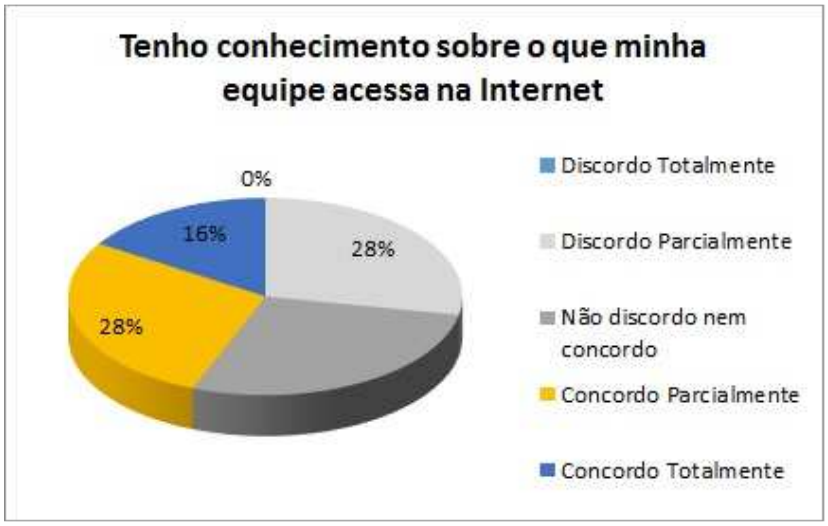


Fonte: Elaboração Própria
Gráfico 17 – Divulgação da política de TI nas equipes de trabalho

Em seguida, quando questionados a respeito da Internet, 28% dos gestores discorda parcialmente de que tenham conhecimento a respeito do que seus funcionários acessem na Internet, 28% não concorda nem discorda e 28% concorda parcialmente. Apenas 16% concorda totalmente.

TENHO CONHECIMENTO DO QUE MEUS FUNCIONÁRIOS ACESSAM NA INTERNET	FREQUÊNCIA	PERCENTUAL
Discordo Totalmente	0	0%
Discordo Parcialmente	7	28%
Não discordo nem concordo	7	28%
Concordo Parcialmente	7	28%
Concordo Totalmente	4	16%
Total	25	100%

Fonte: Elaboração Própria
Tabela 18: Acesso a internet



Fonte: Elaboração Própria
Gráfico 18 – Acesso a internet

Uma questão que é fundamental nos encaminhamentos de uma política de TI, deve ser a disponibilidade de equipamentos e recursos para atendimento das demandas da equipe, segundo 60% dos entrevistados, os equipamentos e recursos de TI atendem às necessidades de trabalho das equipes.

OS EQUIPAMENTOS E RECURSOS DE TI SÃO ADEQUADOS ÀS NECESSIDADES DE MINHA EQUIPE	FREQUÊNCIA	PERCENTUAL
Discordo Totalmente	0	0%
Discordo Parcialmente	10	15%
Não discordo nem concordo	10	15%
Concordo Parcialmente	21	30%
Concordo Totalmente	28	40%
Total	70	100%

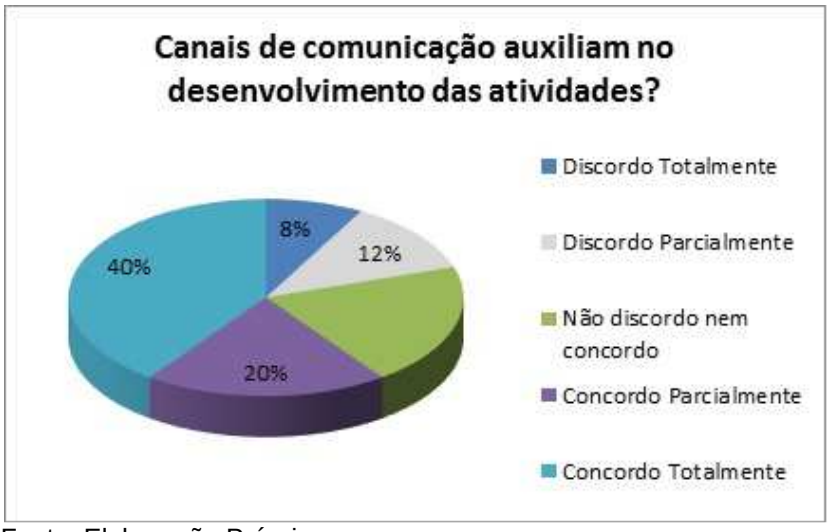
Fonte: Elaboração Própria
Tabela 19: Equipamentos e recursos de TI

Fonte: Elaboração Própria
Gráfico 19: Recursos e equipamentos de TI

A próxima questão feita aos gestores buscou levantar o entendimento dos mesmos se os canais de comunicação disponibilizados pela empresa realmente auxiliam o desenvolvimento das atividades cotidianas dos colaboradores, do que 40% dos entrevistados manifestaram-se em acordo com a afirmativa.

OS CANAIS DE COMUNICAÇÃO DISPONIBILIZADOS PELA ÁREA DE TI AUXILIAM NO DESENVOLVIMENTO DAS ATIVIDADES	FREQUÊNCIA	PERCENTUAL
Discordo Totalmente	2	8%
Discordo Parcialmente	3	12%
Não discordo nem concordo	5	20%
Concordo Parcialmente	5	20%
Concordo Totalmente	10	40%
Total	25	100%

Fonte: Elaboração Própria
Tabela 20: Canais de comunicação

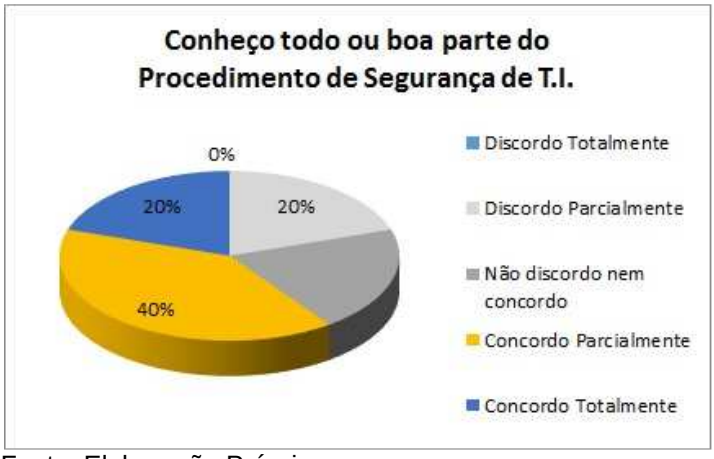


Fonte: Elaboração Própria
Gráfico 20: Canais de comunicação

Seguindo a pesquisa com gestores, a próxima questão levantada buscou saber se estes têm conhecimento do Procedimento de Segurança em TI, e 40% deles foram afirmativos na resposta.

CONHEÇO TODO OU BOA PARTE DO PROCEDIMENTO DE SEGURANÇA DE TI	FREQUÊNCIA	PERCENTUAL
Discordo Totalmente	0	0%
Discordo Parcialmente	5	20%
Não discordo nem concordo	5	20%
Concordo Parcialmente	10	40%
Concordo Totalmente	5	20%
Total	25	100%

Fonte: Elaboração Própria
Tabela 21: Conhecimento sobre o procedimento de segurança de TI

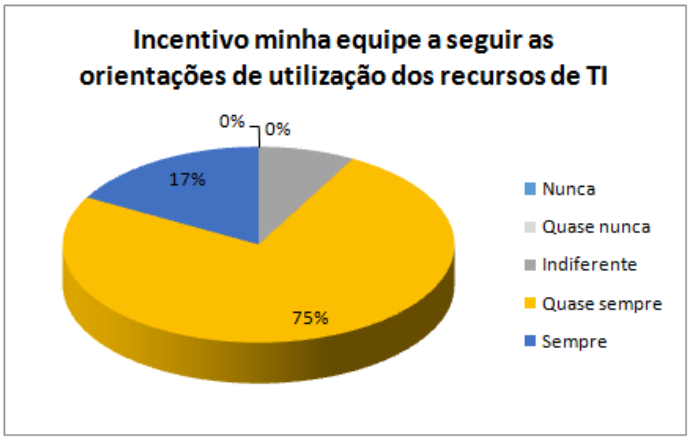


Fonte: Elaboração Própria
Gráfico 21: Conhecimento sobre o procedimento de segurança de TI

Quando questionados se incentivam suas equipes e seguirem as orientações de utilização dos recursos de TI, a maioria dos gestores (65%) afirmou que quase sempre incentiva, gestores imparciais correspondem a 8% e 15% afirmaram sempre incentivar suas equipes de trabalho.

INCENTIVO MINHA EQUIPE A SEGUIR AS ORIENTAÇÕES QUANTO A UTILIZAÇÃO DOS RECURSOS DE TI	FREQUENCIA	PERCENTUAL
Nunca	0	0%
Quase nunca	0	0%
Indiferente	2	8%
Quase sempre	19	75%
Sempre	4	17%
Total	25	100%

Fonte: Elaboração Própria
Tabela 22: Incentivo à utilização dos recursos de TI



Fonte: Elaboração Própria Gráfico 22 – Incentivo à utilização dos recursos de TI
Gráfico 22: Incentivo à utilização dos recursos de TI

4.4 DIAGNÓSTICO

Os questionários aplicados em dois grupos diferentes da organização permitiram ter uma visão global do entendimento das questões de Segurança em TI, por parte de Gestores e de Colaboradores. Este confronto de respostas, devidamente estruturado, permite observar que existem pontos convergentes e divergentes no entendimento da pauta, portanto, objeto das próximas avaliações.

4.4.1 ACESSO AO SISDOC E PCO DE SEGURANÇA DE TI

4.4.1.1 VISÃO DO COLABORADOR

Como resultado da entrevista feita com os colaboradores foi possível observar alguns pontos negativos quanto a utilização de recursos de TI, para a maioria dos respondentes:

- Possui certa dificuldade ao acessar o sistema de documentos (43% possui média dificuldade);
- Acessa com pouca frequência (50% acessa a cada três meses);
- Alega não ter recebido treinamento para utilização;
- Não conhece o Procedimento de Segurança de TI;
- Nunca utilizou o SISDOC.

Por outro lado, de maneira positiva, a maioria dos colaboradores afirmou:

- Saber onde encontrar o PCO de Segurança de TI e
- Considera o PCO útil.

De acordo com as informações levantadas, pode-se afirmar que, do ponto de vista dos colaboradores não existe um processo formal de orientações quanto ao uso do SISDOC.

4.4.1.2 VISÃO DOS GESTORES

No entendimento dos gestores sobre o assunto, a maioria (40%) concorda parcialmente que as orientações são disponibilizadas de maneira clara e objetiva e 32% concordam totalmente com esta afirmação.

4.4.1.3 CONFRONTO DE INFORMAÇÕES (COLABORADOR X GESTOR)

Percebe-se que, não há concordância entre o entendimento dos gestores e os hábitos de utilização dos colaboradores.

Dos gestores entrevistados, a maioria concorda parcialmente que a Política de Segurança de TI é amplamente divulgada em suas equipes de trabalho, mesmo que esta firmação não seja total, este dado conflita com a constatação de que a maioria dos colaboradores entrevistados não conhece, nem nunca utilizou o procedimento. Nota-se que apenas 5% dos gestores afirma conhecer todo ou boa parte do Procedimento de Segurança de TI, em contrapartida a maioria afirma incentivar suas equipes a seguirem as orientações do procedimento.

Esta divergência pode evidenciar algumas situações que devem ser tratadas mais a fundo, como uso indevido das ferramentas, não cumprimento de normas, riscos de perda de informação;.

4.4.2 EQUIPAMENTOS E RECURSOS DE TI

Quando mencionado “recursos de TI” entenda-se *Software*s de Comunicação Instantânea. Estes “recursos” foram restritos aos *software*s para abordar o item do qual menciona o procedimento.

4.4.2.1 VISÃO DO COLABORADOR

Quanto aos canais de comunicação disponibilizados pela empresa, 85% dos respondentes os utiliza. Dos *software*s disponibilizados, 79% dos entrevistados utilizam o Skype, com 14% de utilização o Cisco Webex e 7% utiliza o Google Talk. Para a maioria dos gestores os canais de comunicação auxiliam no desenvolvimento das atividades do dia a dia.

4.4.2.2 VISÃO DOS GESTORES

A maioria dos gestores concorda totalmente que os equipamentos e recursos de TI atendem às necessidades de trabalho de suas equipes.

4.4.2.3 CONFRONTO DE INFORMAÇÕES (COLABORADOR X GESTOR)

Observa-se que de maneira geral há concordância quanto à utilização, por parte dos colaboradores, dos recursos disponibilizados pela empresa que atendem às necessidades das equipes de trabalho. Desta forma a pesquisa reforça o que acontece realmente na empresa, sem necessidade de novas recomendações eventuais.

4.4.3 COMPARTILHAMENTO DE LOGIN E SENHA

O objetivo da abordagem deste tópico é identificar se as regras de utilização de *login* e senha são cumpridas, de acordo com o que determina o PCO de Segurança de TI

4.4.3.1 VISÃO DO COLABORADOR

Mais de 50% dos colaboradores respondentes conhece alguém que já tenha compartilhado algum *login* de acesso. Esta prática é proibida e infringe uma determinação da organização.

4.4.3.2 VISÃO DOS GESTORES

De acordo com o que o Procedimento menciona a respeito do compartilhamento de *logins,* observa-se que os gestores sabem que é proibido, no seu entendimento esta prática não é realizada.

4.4.3.3 CONFRONTO DE INFORMAÇÕES (COLABORADOR X GESTOR)

Percebe-se que há um conflito quanto à prática e a recomendação de não compartilhar *logins* de acesso. Para os gestores, esta prática não é realizada, porém observa-se que ocorre sim, na informalidade. Esta situação contraditória demonstra que este quesito precisa ser tratado urgentemente de forma a uniformizar entendimentos e encerrar o compartilhamento de *login*.

4.4.4 INSTALAÇÃO DE SOFTWARE

O intuito de abordar este tópico é identificar quais são os hábitos dos colaboradores e o entendimento dos gestores no que diz respeito á instalação de *software*s nos equipamentos da organização.

4.4.4.1 VISÃO DO COLABORADOR

A maioria dos colaboradores afirma que não conhece alguém que já tenha instalado algum *software* no computador da empresa. A organização proíbe e a orientação é que, sempre que haja necessidade de instalação, esta deve ser

comunicada ao departamento de TI, que procederá para tal caso constate a necessidade do mesmo.

4.4.4.2 VISÃO DOS GESTORES

A maioria dos gestores concorda que os equipamentos e recursos de TI atendem às necessidades de suas equipes de trabalho.

O entendimento dos gestores neste quesito conota que a recomendação do Procedimento é seguida e que esta prática não deve e não é adotada pelos funcionários.

4.4.4.3 CONFRONTO DE INFORMAÇÕES (COLABORADOR X GESTOR)

Desta forma, não são necessárias recomendações de procedimentos futuros neste quesito.

4.4.5 UTILIZAÇÃO E-MAIL DA EMPRESA

A organização trata deste assunto de maneira breve em seu Procedimento, o objetivo de abordá-lo neste trabalho é identificar se o colaborador utiliza o recurso de maneira procedimento.

4.4.5.1 VISÃO DO COLABORADOR

De acordo com a pesquisa, a maioria dos colaboradores (90% dos respondentes) utiliza o *e-mail* corporativo para assuntos particulares.

Não há restrição total quanto à utilização do *e-mail* corporativo para fins particulares, desde que os colaboradores não reenviem *e-mail*s do tipo corrente, aviso de vírus, avisos da Microsoft/AOL/Symantec, criança desaparecida, entre outros.

4.4.5.2 VISÃO DOS GESTORES

Como a organização não proíbe a utilização do *e-mail* da empresa para fins particulares no entendimento dos gestores esta prática pode ser realizada, porém

conforme o procedimento, desde que os colaboradores não reenviem *e-mail*s do tipo corrente, aviso de vírus, avisos da Microsoft/AOL/Symantec, criança desaparecida, entre outros.

4.4.5.3 CONFRONTO DE INFORMAÇÕES (COLABORADOR X GESTOR)

Mais uma vez a uniformidade de entendimento descarta a necessidade de aprofundar o estudo neste quesito.

4.4.6 UTILIZAÇÃO DA INTERNET

O acesso à Internet não é proibido na empresa Alfa Telecom, há algumas orientações quanto ao assunto. O intuito de abordar este tópico é identificar se há um entendimento entre as práticas dos colaboradores e a visão dos gestores sobreo tema.

4.4.6.1 VISÃO DO COLABORADOR

A maioria dos colaboradores acessa a Internet durante o horário de trabalho, o tempo médio estimado não passa de 20 minutos por dia. A empresa mão proíbe a utilização da rede, porém o tempo de utilização não será analisado.

4.4.6.2 VISÃO DOS GESTORES

Observa-se que não há um monitoramento minucioso, por parte dos gestores, acerca do que seus colaboradores acessam.

Quando questionados se os gestores têm conhecimento do que seus colaboradores acessam na Internet, houve empate no percentual das respostas. Dos respondentes, 28% discorda parcialmente e 28% não concorda nem discorda de que tem conhecimento da utilização da Internet por suas equipes de trabalho.

4.4.6.3 CONFRONTO DE INFORMAÇÕES (COLABORADOR X GESTOR)

Tanto gestores quanto colaboradores não estão seguindo o que determina o Procedimento da organização quanto ao uso da Internet. A empresa estipula que pode-se acessar a web para fins particulares, desde que haja consentimento do responsável pelo setor, e que o acesso seja limitado a consultas bancárias e acessos ao *e-mail* pessoal.

Percebe-se que não há um acompanhamento da utilização da Internet, esta “falta de controle” pode se configurar em um problema para a organização. Desta forma, é preciso que se elabore uma série de estudos para avaliar quais recomendações são cabíveis neste item.

4.4.7 SIGILO DAS INFORMAÇÕES DA EMPRESA

O sigilo com relação às informações organizacionais foi abordado com intuito de identificar se estão sendo tratadas com coerência dentro da organização.

4.4.7.1 VISÃO DO COLABORADOR

A maioria dos respondentes (80% dos respondentes) afirma não conhecer ninguém que já tenha compartilhado informações internas com pessoas de fora da organização. De acordo com os respondentes, esta prática não é comum na empresa.

4.4.7.2 VISÃO DOS GESTORES

No entendimento dos gestores, informações internas não devem ser repassadas a terceiros. Esta é a conduta que os gestores esperam de suas equipes de trabalho.

4.4.7.3 CONFRONTO DE INFORMAÇÕES (COLABORADOR X GESTOR)

Informações organizacionais, não devem ser compartilhadas sem que sejam analisadas por um gestor. Mesmo que pareçam inofensivas, se utilizadas de maneira inadequada podem comprometer o negócio da organização.

Há um entendimento entre colaboradores e gestores neste quesito.

5. CONCLUSÕES FINAIS

Esta pesquisa revelou que existem pontos extremamente críticos na gestão da segurança de TI em grandes corporações, que podem ser extensivas a qualquer outro tipo de empresa.

5.1 SISDOC E PCO DE SEGURANÇA DE TI

O texto do Procedimento de Segurança da Informação da empresa Alfa Telecom poderia ficar mais claro se mencionasse que o objetivo do documento é orientar os colaboradores quanto a seus direitos e obrigações no que diz respeito ao uso de recursos da empresa.

Tendo em vista o fato de os colaboradores afirmarem que possuem dificuldades ao acessar o SISDOC, acessarem com pouca frequência e a maioria não ter recebido instruções, sugere-se que seja desenvolvido um treinamento para uso da ferramenta.

A organização possui o Programa de Desenvolvimento Individual (PDI), que consiste numa programação anual de cursos que cada colaborador deve realizar. A definição destes cursos é realizada em conjunto com o colaborador e seu superior imediato e devem ser incluídos no programa treinamentos que facilitem e capacitem o funcionário para o desempenho das atividades na organização. Existem alguns cursos que são recomendados a todos os funcionários e o treinamento a respeito da utilização do SISDOC pode ser incluído no PDI de todos.

Juntamente com o treinamento, é possível criar uma campanha de conscientização quanto à importância da utilização do Procedimento de Segurança da Informação, bem como os demais documentos que tratam do assunto. Para esta campanha, pode ser utilizada a TV Corporativa, que é uma espécie de “mural eletrônico” e que disponibiliza o dia todo informações da empresa e atualidades de maneira geral. Os aparelhos de TV estão localizados na copa e no refeitório.

Além da TV Corporativa é possível que a campanha seja enviada por *e-mail* aos funcionários ou até mesmo com folders, com as orientações.

Com o incentivo partindo dos gestores, pode-se mudar o cenário atual.

5.2 EQUIPAMENTOS E RECURSOS DE TI

Observa-se que a utilização de *software*s de comunicação instantânea tem sido benéfica no desempenho das atividades da organização. Neste quesito não há necessidade de alterar o modo como o qual a organização tem trabalhado, o que se pode fazer é destacar aos colaboradores a importância de se utilizar com bom senso, para evitar eventuais problemas para a empresa.

Atualmente a maioria dos colaboradores utiliza o Skype como meio de comunicação, além de alguns setores utilizarem o Webex para reuniões com clientes e parceiros. Para as reuniões observa-se que reduz o gasto com telefonia, viagens e estadia.

5.3 COMPARTILHAMENTO DE LOGIN E SENHA

O compartilhamento de senhas de acesso é absolutamente não recomendado, ocorre que, em alguns momentos a empresa não dispõe do número de licenças necessário para que este requisito seja cumprido. Para que esta prática não ocorra, deve-se ser realizado um levantamento da quantidade de licenças necessárias e incluí-las no orçamento de TI, para que a demanda seja atendida em sua totalidade.

As senhas de acesso aos sistemas utilizados na empresa devem ser trocadas a cada 3 meses ou com a periodicidade definida pela TI para cada *software*.

5.4 INSTALAÇÃO DE SOFTWARE

É proibida, a instalação de *software* de qualquer natureza e alterar configurações dos programas instalados, porém algumas permissões de acesso não impedem tais alterações. Não há bloqueio por *login*. Todos os usuários podem fazê-lo. Para auxiliar no cumprimento desta regra, pode-se bloquear *downloads* por *login*, alterando regras de segurança ou utilizando um firewall (nível de aplicação) e bloquear extensões de programas que não devem copiados.

5.5 UTILIZAÇÃO E-MAIL DA EMPRESA

As diretrizes da empresa não proíbem a utilização do *e-mail* corporativo para fins particulares, neste ponto também sugere-se que o bom senso seja instigado aos colaboradores para que não haja práticas abusivas do recurso da empresa.

O assunto pode ser abordado pelos gestores nas reuniões mensais que são realizadas com as equipes, pela proximidade existente entre gestores e suas equipes de trabalho, espera-se que haja efeito de conscientização.

É possível também o envio de *e-mail*s aos funcionários e até mesmo com folhetos ou ainda utilizando a TV Corporativa, com chamadas que tratem do assunto.

5.6 UTILIZAÇÃO DA INTERNET

Com relação à utilização da Internet, no dia-a-dia nota-se que o uso para fins pessoais não fica restrito à consulta de movimentação bancária e ao acesso ao *e-mail* pessoal, conforme descrito no procedimento. Mesmo que no procedimento a regra seja uma, na prática é possível acessar outros conteúdos.

A execução de jogos, músicas ou rádios on-line, é proibida, na prática a execução não é bloqueada. Levando em consideração que o uso deliberado da internet implica em maior exposição a ataques e arquivos maliciosos, para que haja maior efetividade nesta restrição seria necessário bloquear este tipo de ação, por *login* por exemplo.

Já que a organização não proíbe na prática a utilização da Internet, o uso consciente deve ser instigado nos colaboradores. É internet é uma ferramenta extremamente ágil e abrangente, como a política da empresa não é proibitiva conscientizar seus funcionários pode ser mais efetivo, mas há outras opções, como utilizar o *e-mail* da empresa, a TV Corporativa.

5.7 SIGILO DAS INFORMAÇÕES DA EMPRESA

Apesar de não ter sido identificado ponto de falha neste quesito, sugere-se que os colaboradores sejam sempre “lembrados” à respeito do assunto, através do gestores em reuniões, com campanhas de conscientização quanto à conduta que a empresa espera por parte de seus colaboradores e até mesmo através da TV Corporativa, com lembretes sobre o assunto.

5.8 OUTRAS SUGESTÕES DE MELHORIA

Outro documento brevemente analisado é o PCO que trata das regras de acesso à rede corporativa. O procedimento é disponibilizado no sistema de Gerenciamento de Documentos e pode ser visualizado no Anexo 2.

A publicação data de 05/04/2010 e a validade é indicada até 05/04/2012. O documento está em sistema com o status “vigente” em 28/08/2014.

Há um problema de falta de atualização e revisão periódica. Sabe-se, de acordo com a NBR ISSO/IEC27002(2005), que a política (entenda-se também PCOs), seja revisada periodicamente e de forma planejada, ou ainda quando ocorrerem mudanças significativas, com intuito de assegurar sua contínua pertinência, adequação e eficácia.

Levando em consideração o rápido avanço tecnológico e as constantes mudanças que o ambiente corporativo e sociedade enfrentam, não há como conceber que em 4 anos não houve mudança alguma no cenário e na tecnologia utilizada pela organização ou que não foi necessária nenhuma alteração nas regras.

No item Regras de Acesso são tratadas as definições de SOLICITANTE e APROVADOR. Já no item Regras Uso e de Acesso, informa das regras para o uso e gerenciamento dos diretórios da rede. Este procedimento cita mais dois documentos com conteúdo relacionado, um deles é o FOR000091 (Formulário 000091). O FOR000091 é um fluxograma do processo de atribuição de um acesso e o documento FOR000092 é o mapeamento de todos os diretórios existentes na rede.

Observou-se que em alguns pontos há redundância de informação. Se para cada procedimento existirem pelo menos mais dois documentos relacionados, corre-se o risco de que um documento seja lido e outro não. Neste caso, sugere-se que as informações sejam dispostas em apenas um documento, para evitar que o colaborador procure por um documento e não procure por outro.

Foi possível observar que a empresa Alfa Telecom possui em suas diretrizes os princípios da Segurança da Informação, porém há o que ser melhorado afim de que não haja quebra destes princípios.

7. REFERÊNCIAS BIBLIOGRÁFICAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISSO/IEC 27002**: Tecnologia da Informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação. Rio de Janeiro: ABNT, 2005. 120 p.

FONTES, Edson Luiz Gonçalves, **Praticando a Segurança da Informação**. 1 Ed. Rio de Janeiro: Brasport, 2008.

DANTAS, Marcus Leal, Segurança da informação: uma abordagem focada em gestão de riscos. – Olinda: Livro Rápido, 2011.

PONTES, Edison, **Políticas e normas para segurança da informação**. / Edison Fontes – Rio de Janeiro: Brasport, 2012.

RODRIGUEZ, Martius V. / FERRANTE, Agustin J., **Tecnologia da Informação e Gestão Empresarial**. – Rio de Janeiro: E-Papers, 2000.

MARCIANO, João Luiz / MAMEDE, Lima Marques, **O enfoque social da segurança da informação** / SciElo Brasil – 89 -98; 2006-12.
Disponível em <www.scielo.org> Acesso em: 17 jul. 2014.

DENISON, Daniel, **A força da cultura organizacional nas empresas globais** [recurso eletrônico]: como conduzir mudanças de impacto e alinha estratégia e cultura / Tradução Edson EdsonFurmankiewics – Rio de Janeiro: Elsevier, 2012.

MANOEL, Sérgio da Silva, **Governança de Segurança da informação**, Rio de Janeiro: Brasport, 2014.

PÁDUA, Elisabete Matallo Marchesini de, **Metodologia da pesquisa: Abordagem teórico-prática**, Campinas, SP: Papirus, 2004.

RECIPRHOCAL. **Cultura segundo Edgar Schein**. Disponível em <http://www.reciprhocal.com.br/?p=172> Acesso em: 19 ago .2014.

SUPPORT SKYPE. **O que é O Skype?** Disponível em <https://support.skype.com/pt/faq/FA6/o-que-e-o-skype> Acesso em 01 out. 2014.

WEBEX. **Aplicativos de reunião WebEx para empresas e grandes negócios**. Disponível em <http://www.webex.com.br/webex-for-enterprise.html> Acesso em 01 out. 2014.

SOUZA, Diego dos Santos, **Disciplina: Práticas e Modelos de Segurança**. Universidade Estácio de Sá – Rio de Janeiro – 2012. Disponível em <http://pt.slideshare.net/diegosouzapc/avaliao-aula-2-estcio-diegodossantossouza> > Acesso em 30 set.2014.

CUNHA, André Luiz / PEISCHL, Roberto Bittencourt. **O valor das informações para as empresas e a importância da segurança da informação**. Disponível em <http://pt.slideshare.net/acunha_sp/o-valor-das-informaes-para-as-empresas-e-a-importancia-da-seguranca-da-informacao> Acesso em 26 out. 2014.

APÊNDICE 1 – QUESTIONÁRIO SISDOC

SISDOC

Este questionário tem como finalidade identificar a funcionalidade do SisDoc no desempenho de suas atividades diárias.
Seu nome e e-mail não serão registrados, contamos com sua colaboração para responder todas as perguntas.

1 - Qual é seu grau de dificuldade quando utiliza o SisDoc?

- Muita dificuldade
- Média dificuldade
- Pouca dificuldade
- Nenhuma dificuldade

2 - Com que frequência você o utiliza?

- Mais de uma vez por mês
- Uma vez a cada três meses
- Uma vez a cada 6 meses
- Não utilizo

3 - Você recebeu treinamento para utilização?

- Sim
- Não

4 - Você o considera útil?

- Sim
- Não

4.1 - Por que?

Enviar

100% concluído.

Nunca envie senhas em Formulários Google.

APÊNDICE 2 – QUESTIONÁRIO PRÁTICAS E UTILIZAÇÃO DOS RECURSOS DE TI

Práticas e utilização dos recursos de T.I.

Este questionário tem por finalidade identificar as práticas relacionadas aos recursos de Informática no dia a dia dos colaboradores.
Você não será identificado. Contamos com sua participação.

1. Você conhece alguém que utilize ou compartilhe login e senha?

- Sim
- Não

2. Você conhece alguém que já tenha instalado algum software no computador da empresa?

- Sim
- Não

3. Conhece alguém que costume utilizar o e-mail da empresa para tratar de assuntos particulares?

- Sim
- Não

4. Você costuma acessar a Internet durante o horário de trabalho para fins particulares?

- Sim
- Não

5. Em geral, quanto tempo por dia você permanece conectado à Internet?

--:--

Exemplo. 11h

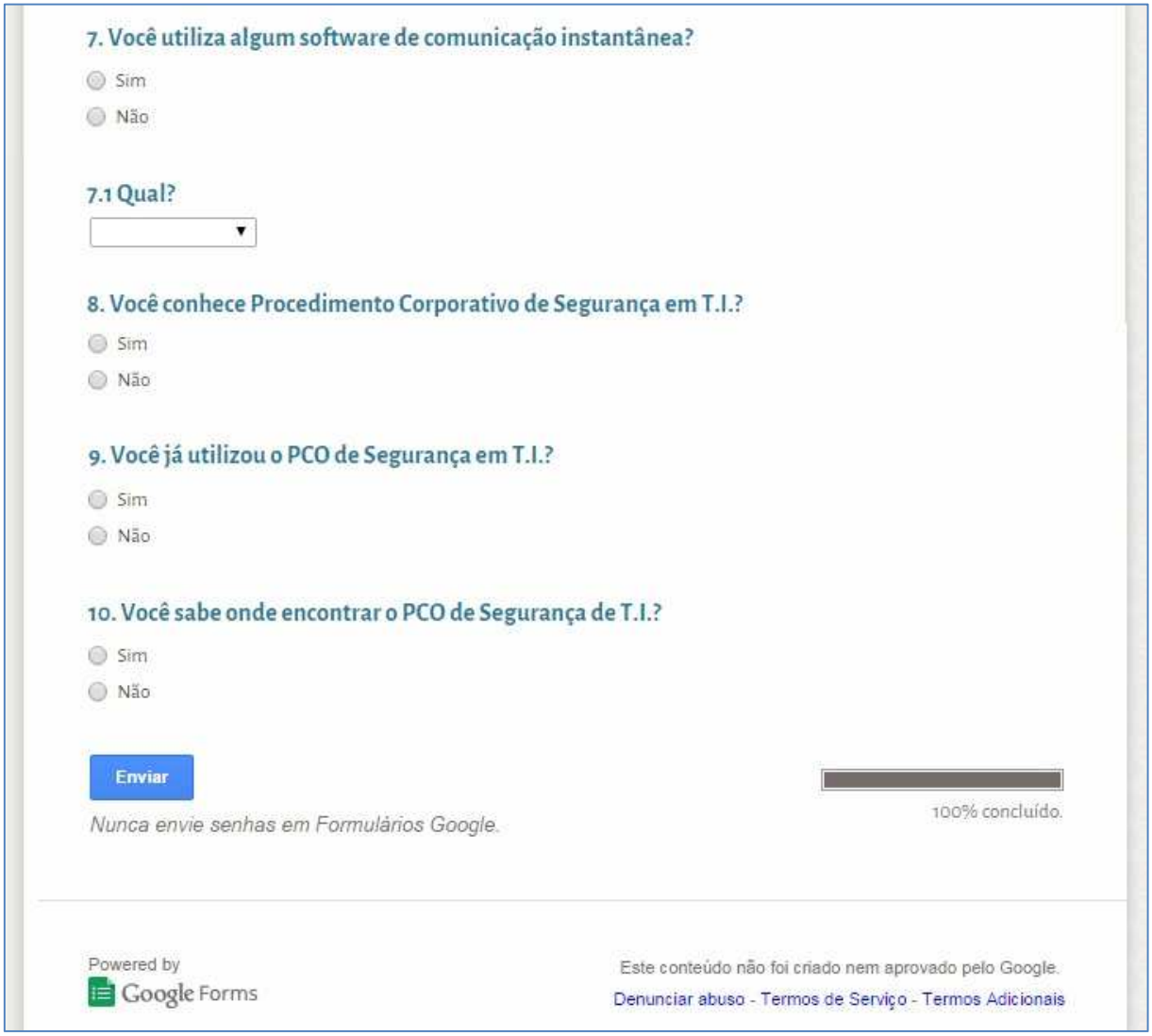
6. Você conhece alguém que já tenha compartilhado informações internas com pessoas de fora da empresa?

- Sim
- Não

CONTINUA

CONTINUAÇÃO

APÊNDICE 2 – QUESTIONÁRIO PRÁTICAS E UTILIZAÇÃO DOS RECURSOS DE TI



7. Você utiliza algum software de comunicação instantânea?

- Sim
- Não

7.1 Qual?

8. Você conhece Procedimento Corporativo de Segurança em T.I.?

- Sim
- Não

9. Você já utilizou o PCO de Segurança em T.I.?

- Sim
- Não

10. Você sabe onde encontrar o PCO de Segurança de T.I.?

- Sim
- Não

Enviar

100% concluído.

Nunca envie senhas em Formulários Google.

Powered by Google Forms

Este conteúdo não foi criado nem aprovado pelo Google.

Denunciar abuso - Termos de Serviço - Termos Adicionais

APÊNDICE 3 – QUESTIONÁRIO RECURSOS DE TI – GESTORES

TELA 1

Recursos de T.I. - Gestores

Este questionário tem como objetivo identificar se é e como é trabalhada a utilização dos recursos de T.I. em sua equipe de trabalho.

Sua opinião é fundamental para que possamos realizar este diagnóstico.

Continuar »

TELA 2

Recursos de T.I. - Gestores

Esclarecimentos

Todas as questões deste formulário são compostas de uma afirmação genérica que tem por objetivo constatar as práticas comumente adotadas com sua equipe de trabalho no dia a dia.

Fizemos algumas simulações e o tempo de resposta não passou de 10 minutos.

« Voltar Continuar »

TELA 3

Recursos de T.I. - Gestores

*Obrigatório

Para as questões com resposta em forma de escala, considere:

(1) Discordo Totalmente
(2) Discordo Parcialmente
(3) Não discordo nem concordo
(4) Concordo Parcialmente
(5) Concordo totalmente

Tempo de empresa *

- [ ] De 0 a 5 anos
- [ ] De 6 a 10 anos
- [ ] De 11 a 15 anos
- [ ] De 16 a 20 anos
- [ ] Mais de 20 anos

As orientações quanto à utilização dos recursos de T.I. são disponibilizadas aos colaboradores de maneira clara e objetiva. *

	1	2	3	4	5	
Discordo Totalmente	○	○	○	○	○	Concordo Totalmente

A Política de Segurança de T.I. é amplamente divulgada em minha equipe de trabalho. *

	1	2	3	4	5	
Discordo Totalmente	○	○	○	○	○	Concordo Totalmente

Tenho conhecimento do que meus funcionários acessam na Internet. *

	1	2	3	4	5	
Nunca	○	○	○	○	○	Sempre

« Voltar Continuar »

Powered by Google Forms

Este conteúdo não foi criado nem aprovado pelo Google.
Denunciar abuso - Termos de Serviço - Termos Adicionais

TELA 4

Recursos de T.I. - Gestores

*Obrigatório

Para as questões com resposta em forma de escala, considere:

(1) Discordo Totalmente
(2) Discordo Parcialmente
(3) Não discordo nem concordo
(4) Concordo Parcialmente
(5) Concordo totalmente

Os equipamentos e recursos de T.I. são adequados às necessidades de minha equipe. *

	1	2	3	4	5	
Concordo Totalmente	○	○	○	○	○	Discordo Totalmente

Os canais de comunicação disponibilizados pela área de T.I. auxiliam no desenvolvimento das atividades. *

	1	2	3	4	5	
Concordo Totalmente	○	○	○	○	○	Discordo Totalmente

Conheço todo ou boa parte do Procedimento de Segurança de T.I. *

	1	2	3	4	5	
Concordo Totalmente	○	○	○	○	○	Discordo totalmente

Incentivo minha equipe a seguir as orientações quanto à utilização dos recursos de T.I. *

	1	2	3	4	5	
Nunca	○	○	○	○	○	Sempre

« Voltar Enviar

Nunca envie senhas em Formulários Google.

Powered by Google Forms

Este conteúdo não foi criado nem aprovado pelo Google.
Denunciar abuso - Termos de Serviço - Termos Adicionais

TELA 5

Recursos de T.I. - Gestores

Obrigada pela colaboração!

Suas respostas são muito importantes.

Enviar outra resposta

Este formulário foi criado com o Formulários Google.
Criar seu próprio formulário

Google Forms

ANEXOS

ANEXO 1 – PCO – Procedimento Corporativo de Segurança em TI

PCO000070-01

PROCEDIMENTO CORPORATIVO DE SEGURANÇA EM TI

Elaborador:	Verificador:	Aprovador:

1. OBJETIVO

Melhorar a aspectos de segurança das informações da Furukawa.

Prevenção de instalação de softwares indevidos nas máquinas da Furukawa

Permissões de utilização da Internet e Email corporativo

2. DEFINIÇÕES

- TI – Tecnologia da Informação
- As informações criadas, armazenadas ou disponibilizadas em sistemas de computadores da empresa ou de terceiros que trabalham em suas dependências, são de propriedade da Furukawa.
- Os recursos e facilidades de informática, tais como acessos à rede, internet, sistemas de colaboração e mensagens eletrônicas, dentre outros, são recursos da Empresa, portanto devem ser utilizados somente para atividades profissionais.

3. AUTONOMIA DO DEPARTAMENTO DE TI

- O departamento de TI possui total autonomia para atuar sobre os equipamentos de propriedade da empresa, sem prévio aviso, no que se refere aos seguintes tópicos:
- Realização de auditoria local ou remota.
- Definição de perfis de usuários cujos privilégios não permitam a realização de atividades tidas como prejudiciais ao hardware e software ou à rede da empresa como um todo;
- A instalação e configuração de softwares de monitoramento;
- A desinstalação de quaisquer softwares considerados prejudiciais à rede, ou ainda softwares não autorizados, ilegais e/ou não licenciados;
- Excluir arquivos pessoais ou proibidos por direitos autorais (ex. livros eletrônicos, músicas, Filmes...)
- O credenciamento e descredenciamento de usuários;

4. DIRETRIZES QUANTO À UTILIZAÇÃO DA INTERNET

- A Internet deve ser utilizada para fins corporativos, o enriquecimento intelectual de seus colaboradores ou como ferramenta para busca de informações que venham contribuir para o desenvolvimento das atividades destes.
- O uso para fins pessoais, mediante o consentimento do responsável pelo setor, fica restrito à consulta de movimentação bancária e ao acesso ao e-mail pessoal, estando vedadas práticas abusivas tais como o acesso ou a circulação de correntes, material pornográfico, difamatório ou ilegal entre outros.
- Softwares liberados para comunicação:

- Skype
- Windows Live Messenger
- Google Talk
- Cisco Webex

5. A REALIZAÇÃO DE DOWNLOAD

- A realização de downloads exige banda de navegação do servidor e, se realizado em demasia, congestiona o tráfego e torna a navegação para os demais usuários mais demorada. A realização de downloads deve ser vista com muito cuidado e feita somente em casos de extrema necessidade.

6. EXECUÇÃO DE JOGOS E RÁDIOS ON-LINE

- É terminantemente proibida a execução de jogos, músicas ou rádios on-line, visto que esta prática congestiona a banda de internet, dificultando a execução de serviços que necessitam deste recurso.

7. E-MAIL CORPORATIVO

- Desconfiar de todos os e-mails com assuntos estranhos ao ambiente de trabalho. Não reenviar e-mails do tipo corrente, aviso de vírus, avisos da Microsoft/AOL/Symantec, criança desaparecida, entre outros.
- Evitar enviar anexos acima de 10 Mbytes.

8. SENHAS DE ACESSO

- A senha de acesso é pessoal, intransferível, cabendo ao seu titular total responsabilidade quanto seu sigilo. Não devem ser escritas e/ou armazenadas em locais de fácil acesso.
- Devem conter no mínimo 8 caracteres alfanuméricos, não relacionados ao próprio nome, apelido, data de nascimento e outras referências óbvias.
- Devem ser trocadas a cada 3 meses ou sempre que necessário.
- O compartilhamento de senhas de acesso é absolutamente proibido e o titular que divulgar sua senha a outrem responderá pelas infrações por esse cometidas, estando passível de advertência ou outras medidas cabíveis. Caso o usuário desconfie que sua senha não seja mais segura, deve trocá-la imediatamente. No caso de perda de senha, abrir chamado junto ao HELP DESK.
- Os logins devem ser padronizados e extrapolados para todos os sistemas da XXXXX . A área de cadastro de usuários deverá ser instruída para tal fim e o usuário deverá carregar o login por toda sua vida na XXXXX

  EXEMPLO:

  João de Freitas

Login = jfreitas (para o Oracle, Tedesco, Internet Expense, ISOSystem etc.).

E-mail = jfreitas@xxxxx.com.br

9. A INSTALAÇÃO DE SOFTWARES

- Qualquer software que, por necessidade do serviço, necessitar ser instalado, deverá ser comunicado ao departamento de TI, que procederá a instalação caso constate a necessidade do mesmo. **Fica proibida, sob qualquer pretexto, a instalação de software de qualquer natureza e alterar configurações dos programas instalados.**
- O departamento de TI poderá utilizar da autonomia citada no item 4 deste instrumento para desinstalar, sem aviso prévio, todo e qualquer software sem licença de uso, em atendimento à lei do software (Lei 9.609/98).

10. QUANTO AOS EQUIPAMENTOS (HARDWARE)

- Os computadores e periféricos conectados à rede de dados da empresa são instalados de acordo com as configurações definidas pelo Departamento de Tecnologia da Informática e disponibilizados aos funcionários como ferramentas de trabalho.
- Fica proibida, sob qualquer pretexto:
  - Abrir os equipamentos
  - Mudar os equipamentos de local, exceto portáteis

11. PENALIDADES

- O usuário que infringir qualquer uma das diretrizes de segurança expostas neste instrumento estará passível às penalidades a serem definidas de acordo com a gravidade da ocorrência, podendo envolver advertência, suspensão, rescisão contratual por justa causa ou outras medidas cabíveis conforme legislação vigente (sem prévio aviso).

12. EQUIPE DE SEGURANÇA DA INFORMAÇÃO

- Os servidores relacionados a seguir são diretamente responsáveis pela implantação deste procedimento:
  - Gestor de TI;
  - Gestor do Jurídico
  - Gestor de Recursos Humanos

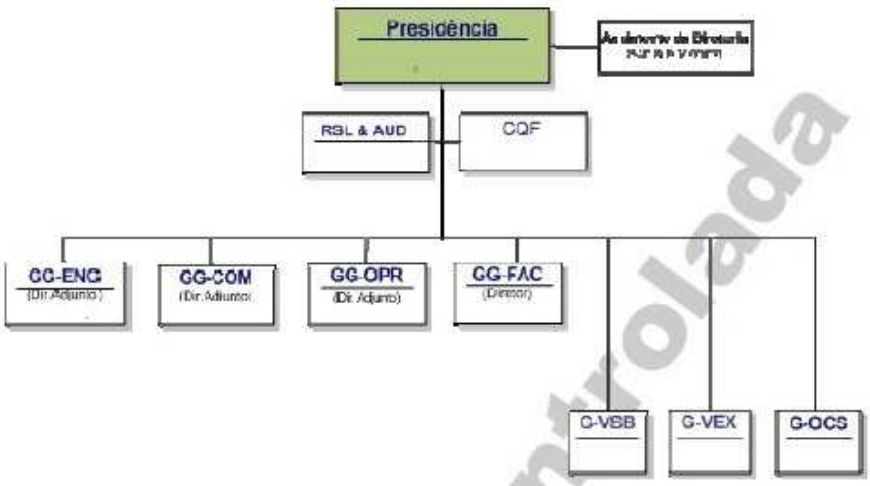
13. FLUXO DE APROVAÇÕES DE CHAMADOS DE TI PELOS SUBORDINADOS DIRETOS À PRESIDÊNCIA

- As aprovações de chamados de TI abertos pelos subordinados direto à presidência ficam designadas para o Gerente de TI (sr. FULANO) como aprovador nível 1.

PCO000070-01

PROCEDIMENTO CORPORATIVO DE SEGURANÇA EM TI

Elaborador: **Verificador:** **Aprovador:**



14. DIVULGAÇÃO

- Este procedimento deve ser divulgado aos colaboradores através do ISOSystem.

15. VIGÊNCIA E VALIDADE

- O presente procedimento passa a vigorar a partir da data de sua homologação e publicação, sendo válida por tempo indeterminado podendo ser alterada conforme necessidades previamente detectadas.
- Este procedimento é válido para todos os colaboradores, prestadores de serviço, fornecedores, clientes, quaisquer terceiros e/ou visitantes que utilizem a infraestrutura de TI da XXXXXX .

ANEXO 2 – Procedimento Corporativo Rede Corporativa – Regras de Acesso

LOGO DA EMPRESA	Categoria: PROCEDIMENTO CORPORATIVO		Nº: PCO000059
	Assunto: REDE CORPORATIVA Regras de Acesso		Versão: 03
	Data de publicação: 05-04-10	Data de validade: 05-04-12	Data do cancelamento: -O-

A revisão deste procedimento atende a metodologia do PDCA (Plan-Do-Check-Act).

1. OBJETIVO

Estabelecer as condições para acesso a rede corporativa da xxxxx .

2. CAMPO DE APLICAÇÃO

Todas as áreas, conforme organograma da empresa.

3. DOCUMENTOS DE REFERÊNCIA

Formulário **FOR000091** [REDE CORPORATIVA Solicitação de Acesso] e **FOR000092** [DIRETÓRIOS Catálogo].

4. DEFINIÇÕES

Rede Corporativa. Rede privada que permite o compartilhamento dos recursos de hardware e softwares instalados [incluso os diretórios de rede].

Sistemas Corporativos. São considerados sistemas corporativos o **e-Business suíte da Oracle,** os sistemas **complementares,** os sistemas **WEB,** os softwares de **colaboração** e os **diretórios**.

e-Business suíte da Oracle. Sistema automatizado e integrado de informações de dados e processos de uma corporação.

Sistemas Complementares. Sistemas secundários que gravitam em torno do sistema Oracle. Exemplos: Forponto, Orbium, Sispro, Sygno, Trade, XRT entre outros.

Sistemas WEB. Sistemas desenvolvidos em plataforma WEB.

Software de colaboração. Softwares corporativos para comunicação, segurança e aplicativos de microinformática. Exemplos: VPN, Office, Autocad, MS Project, Correio Eletrônico, Visio entre outros.

Diretórios. O diretório é uma estrutura utilizada para organizar arquivos em computador. O arquivo é um agrupamento de registros que contém informações específicas de uma área e são registrados em discos rígidos.

Remedy User. Software da BrT/Oi que controla as solicitações dos usuários da xxxxx .

Perfil de acesso do usuário. Responsabilidades que o usuário possui levando-se em consideração as premissas de sua função.

Usuário APROVADOR. É o superior imediato do usuário SOLICITANTE (ver organograma).

Usuário SOLICITANTE. É aquele que precisa que uma necessidade seja atendida.

Backup. Cópia de segurança.

5. DIRETRIZES

REDE CORPORATIVA Regras de Acesso

5.1 O Usuário APROVADOR aprova ou não a solicitação do Usuário SOLICITANTE.

5.1.1 O Usuário SOLICITANTE detecta necessidades próprias **ou** relativas a usuários admitidos, demitidos ou transferidos.

5.1.2 O Usuário SOLICITANTE, no caso dos **funcionários admitidos** ou **transferidos**, deve ser da área onde o novo funcionário será alocado.

5.1.3 O Usuário SOLICITANTE, no caso dos **funcionários demitidos**, deve ser da área de RHU.

5.2 O responsável de cada contrato define, quando aplicável, a necessidade de **inclusão ou exclusão de terceiros** à rede corporativa da xxxxx [o responsável de contrato funcionará como o Usuário SOLICITANTE neste caso].

5.3 As liberações de acesso e de responsabilidades serão controladas através do REMEDY USER da BrT/Oi.

5.4 As solicitacões de acesso ou de responsabilidades devem ser feitas através do ramal 4321 ou do e-mail help desk@xxxxx.com.br

Elaborador: XXXXX	Verificador: XXXXX	Aprovador: XXXXX

Este documento é válido por 2 dias a partir da data de impressão. Eliminar o mesmo após o uso.