UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
DEPARTAMENTO ACADÊMICO DE INFORMÁTICA
ESPECIALIZAÇÃO EM REDES DE COMPUTADORES

LUCAS RAFAEL WASCHBURGER

SEGURANÇA DA INFORMAÇÃO - CONHECIMENTOS NECESSÁRIOS PARA AS EMPRESAS ATUAIS

TRABALHO DE CONCLUSÃO DE CURSO

PATO BRANCO
2015

LUCAS RAFAEL WASCHBURGER

SEGURANÇA DA INFORMAÇÃO - CONHECIMENTOS NECESSÁRIOS PARA AS EMPRESAS ATUAIS.

Trabalho de Conclusão de Curso, apresentado ao II Curso de Especialização em Redes de Computadores – Configuração e Gerenciamento de Servidores e Equipamentos de Redes, da Universidade Tecnológica Federal do Paraná, câmpus Pato Branco, como requisito parcial para obtenção do título de Especialista.

Orientador: Prof. Christiam Carlos Souza Mendes.

PATO BRANCO
2015

TERMO DE APROVAÇÃO

Segurança da Informação - Conhecimentos Necessários para as Empresas Atuais

por

Lucas Rafael Waschburger

Esta monografia foi apresentada às 20h30min do dia 16 de novembro de 2015, como requisito parcial para obtenção do título de ESPECIALISTA, no II Curso de Especialização em Redes de Computadores – Configuração e Gerenciamento de Servidores e Equipamentos de Redes, da Universidade Tecnológica Federal do Paraná, Câmpus Pato Branco. O acadêmico foi arguido pela Banca Examinadora composta pelos professores abaixo assinados. Após deliberação, a Banca Examinadora considerou o trabalho **aprovado**.

Banca Examinadora

Prof. M.Sc. Christian Carlos Souza Mendes
Orientador / UTFPR-CT

Prof. Dr. Fábio Favarim
UTFPR-PB

Prof. Dr. Éden Ricardo Doscïatti
UTFPR-PB

Prof. Dr. Fábio Favarim
Coordenador do II Curso de Especialização
em Redes de Computadores

RESUMO

WASCHBURGER, Lucas Rafael. Segurança da Informação - Conhecimentos Necessários para as Empresas Atuais. 2015. 39 f. Monografia de Trabalho de Conclusão de Curso (II Curso de Especialização em Redes de Computadores), Departamento Acadêmico de Informática, Universidade Tecnológica Federal do Paraná, Campus Pato Branco. Pato Branco, 2015.

O presente trabalho buscou abordar os sistemas de informação quanto a segurança básica necessária nas organizações. Nota-se que, em contatos com empresas atuais, principalmente as pequenas e médias, a grande maioria não tem noção do risco que correm estando conectadas a grande rede, nem o valor real da informação que ali armazenam, buscou-se então, principalmente sua importância na proteção de dados e informações. Teve por métodos revisão bibliográfica do tema por autores e publicações, com procedimentos descritivos e abordagem qualitativa e indutiva.

PALAVRAS CHAVE: Proteção, Necessidade, Segurança.

ABSTRACT

WASCHBURGER, Lucas Rafael. Information Security - Necessary Knowledge for the Current Business. 2015. 39 f. Monografia de Trabalho de Conclusão de Curso (II Curso de Especialização em Redes de Computadores), Departamento Acadêmico de Informática, Universidade Tecnológica Federal do Paraná, Câmpus Pato Branco. Pato Branco, 2015.

This work sought to address the information systems as the basic security necessary in organizations. Note that, in contacts with today's enterprises, especially small and medium, the vast majority have no idea of the risk they face being connected to large network, or the real value of the information that there store, we sought to then, especially its importance on data protection and information. Had by methods bibliographic review by authors and publishers, with descriptive procedures and qualitative and inductive approach.

KEYWORDS: Protection, Need, Safety.

LISTA DE SIGLAS, ABREVIATURAS E ACRÔNIMOS

ABEP	Associação Brasileira de Estudos Populacionais
ABNT	Associação Brasileira de Normas Técnicas
ANATEL	Agência Nacional de Telecomunicações
CB	Comitês Brasileiros
CE	Comissões de Estudos
CET	Comissões de Estudo Especiais Temporárias
COBIT	*Control Objectives For Information end Relatet Technology*
CSS	*Cascading Style Sheets*
DNS	Domain Name System
e-MAIL	*electronic-mail*
HTTP	*HyperText Transfer Protocol*
IBOPE	Instituto Brasileiro de Opinião Pública e Estatística
IDS	*Intrusion Detection System*
IEC	*International Engineering Consortium*
IIA	*Institute of Internal Auditors*
ISACA	*Information Systems Audit and Control Association*
ISO	*International Organization for Standardization*
NBR	Norma Brasileira aprovada pela ABNT
ONS	Organismos de Normalização Setorial
PDTI	Plano Diretor de Tecnologia da Informação
SQL	*Structured Query Language*
TCU	Tribunal de Contas da União
TI	Tecnologia da Informação
WI-FI	*Wireless Fidelity*
XSS	*Cross-site scripting*

LISTA DE QUADROS

SUMÁRIO

1 INTRODUÇÃO

Com o advento da globalização, a informação passou a se disseminar de forma mais rápida. Desta forma, a necessidade de controlar e auditar os recursos, principalmente financeiros, das áreas de Tecnologia da Informação e da Comunicação se tornou algo vital para as empresas, uma vez que a informação interfere diretamente no desenvolvimento da estratégia e na tomada de decisões, passando a ser um dos ativos mais valiosos dentro da organização.

A informação é um ativo muito valioso para as organizações e dependendo da situação pode estar comprometida no que diz respeito à ausência de controles e processos de segurança adequados. Assim, toda a empresa deve utilizar sistemas de informação integrados e os mesmos devem ser confiáveis para evitar a exposição da empresa a riscos prejudiciais ao negócio, além de emitir relatórios sobre a situação atual da organização aos *stakeholders*, segundo Baruque e Santos (2010) são as “partes interessadas” de um negócio, projeto, etc. De maneira abrangente, podemos dizer que os *stakeholders* são aquelas pessoas ou instituições que possuem algum tipo de envolvimento profissional ou pessoal com a empresa (investidores, clientes, funcionários, fornecedores, credores, acionistas, usuários, parceiros, etc.) e as pessoas que podem ser afetadas de alguma forma pelos resultados da operação da empresa.

O trabalho em questão visa demonstrar às organizações um apanhado geral de segurança da informação e como se proteger de possíveis crimes cibernéticos que possam interferir na saúde organizacional.

1.1 OBJETIVOS

1.1.1 OBJETIVO GERAL

Apresentar uma sinopse geral sobre conceitos básicos de segurança da informação

1.1.2 OBJETIVOS ESPECÍFICOS

- Analisar referências de melhores práticas em segurança da informação.
- Identificar controles de TI para mitigar os riscos identificados.

1.2 JUSTIFICATIVAS

A preocupação com a segurança da informação nas organizações reflete nos objetivos de negócio a serem atingidos.

O ambiente de TI, em conjunto com a informação nele armazenada, são um dos principais ativos dentro de uma organização. A ABNT NBR ISO/IEC 27002 é uma referência de excelência para uma implantação eficaz da segurança da informação.

1.3 METODOLOGIA

Após o entendimento do ambiente de TI da instituição, adotou-se como estratégia a avaliação dos riscos de TI e posteriormente, a identificação da existência de controles de TI que mitiguem tais riscos encontrados. A pesquisa visa demonstrar a realidade dos fatos através de metodologia científica, por isso, seu objetivo principal é descobrir quais as soluções e práticas diante das premissas apresentadas através dos métodos científicos. Para tanto, o presente trabalho utilizará a pesquisa descritiva.

Segundo Gil (2002) este tipo de pesquisa visa analisar os fenômenos que envolvem determinado tema, a fim de compreender as suas variáveis, este método é marcado pela análise de coleta de dados.

Para tanto, será realizada pesquisa bibliográfica e documental, através da seleção de diversos materiais para leitura analítica (livros, artigos, teses, monografias, leis e documentos)

O presente trabalho utilizará esse tipo de pesquisa para dar suporte a tipologia que será realizada. Ainda, quanto ao procedimento será utilizado pesquisa bibliográfica.

Esse trabalho caracteriza-se como pesquisa bibliográfica porque utilizará referências teóricas de livros, artigos e autores especializados na área, através dos conhecimentos desses autores, conhecer, explicar e debater o tema para alcançar os objetivos do trabalho.

Vergara (2004, p. 46) afirma que a pesquisa bibliográfica, “*é o estudo sistematizado desenvolvido com base em material publicado em livros, revistas, jornais, redes eletrônicas, isto é, material acessível ao público em geral”.*

2 REFERENCIAL TEÓRICO

2.1 O QUE É GOVERNANÇA?

Baruque e Santos (2010), afirmam que governança é o conjunto de responsabilidades e práticas exercidas pela diretoria e pela gerência executiva com o intuito de fornecer uma direção estratégica à empresa, garantindo que seus objetivos sejam alcançados e seus riscos gerenciados de forma correta, verificando que seus recursos sejam usados com transparência, ética e responsabilidade.

Para os autores supracitados, o processo de governança nas empresas visa responder a quatro perguntas básicas, são elas:

1. Se a empresa está fazendo as coisas certas;
2. Se a empresa está atuando de forma correta;
3. Se o uso dos recursos é eficaz e eficiente;
4. Se os objetivos estabelecidos são alcançados.

Baruque e Santos (2010) citam as três principais áreas do conhecimento que podem contribuir diretamente para uma boa governança, os quais são ilustrados na Figura 1. Gestão, Auditoria e TI (Tecnologia da Informação).

Figura 1 - Os três pilares da Governança
Fonte: Baruque e Santos (2010)

Para Baruque e Santos (2010):

> Cada uma dessas áreas tem um objetivo definido dentro da governança:
> 1. Gestão – estabelece um sistema de controle gerencial, bem como um ambiente que promova o alcance dos objetivos do negócio.
> 2. Auditoria – avalia de forma independente a adequação e a eficácia dos controles estabelecidos pela gerência/diretoria.
> 3. Tecnologia da Informação – apoia e capacita a execução dos controles do nível estratégico ao operacional. (BARUQUE; SANTOS, 2010 p.13)

2.2 PLANO DIRETOR DE TI (PDTI)

Segundo Baruque e Santos (2010), o plano diretor de TI possui estratégias contidas no plano estratégico da organização que serão utilizados para alinhar a TI com os objetivos da organização. Ou seja, os objetivos da TI são criados a partir dos objetivos da organização.

Ainda segundo Baruque e Santos (2010), o PDTI é um documento de alto nível, elaborado pela diretoria de TI juntamente com partes interessadas no alcance dos objetivos estratégicos e deve conter informações pouco detalhadas, mas abrangentes.

Conclui-se, então, que um PDTI deve responder às seguintes questões:

- O que será feito?
- Quem fará?
- Quando fará?
- Por que fará?
- Onde fará?
- Como fará?
- Quanto custará?

Seguindo a linha de raciocínio de Baruque e Santos (2010), o PDTI deve responder as questões de forma menos detalhada, porém, suficiente para que seja possível a criação detalhada dos controles nas políticas e procedimentos.

2.3 DEFINIÇÃO DE INFORMAÇÃO

Como afirma Oliveira (2002), a informação é tudo aquilo que, diminuindo o nosso grau de incerteza, ou indefinição, nos potencializa a racionalidade do processo de decisão, isto é, de administração e gestão.

Já para Amaral e Varajão (2007), informação é aquele conjunto de dados que, quando provido de forma e tempo apropriado, melhora o conhecimento da pessoa que o recebe, ficando ela mais capacitada a desenvolver determinada atividade ou a tomar determinada decisão.

2.4 DEFINIÇÃO DE SISTEMA DE INFORMAÇÃO

Segundo Oliveira (2002), sistema de informação é um conjunto de meios físicos e lógicos, humanos, financeiros, organizacionais e consumíveis diversos, que de uma forma racional interagem entre eles, se integram e se combinam com vista à produção, memorização e distribuição/consulta de informação, objetivando satisfazer determinadas necessidades de gestão.

Conforme Amaral e Varajão (2007), sistema de informação é um sistema que reúne, guarda, processa e faculta informação relevante para a organização de modo que a informação é acessível e útil para aqueles que a querem utilizar, incluindo gestores, funcionários, clientes, etc.

Conclui-se então com a afirmação de Neto e Solonca (2007), que os sistemas de informação adquiriram uma relevância essencial para a sobrevivência da maioria das organizações modernas, já que, sem computadores e redes de comunicação, a prestação de serviços de informação pode se tornar inviável. Ainda concluem que, atualmente, não existem mais empresas que não dependam da tecnologia da informação, num maior ou menor grau.

2.5 DEFINIÇÃO DE SEGURANÇA DA INFORMAÇÃO

A ABNT NBR ISO/IEC 27002 (2005), define segurança da informação como sendo a proteção contra vários tipos de ameaças, garantindo a continuidade e minimizando o risco do negócio.

Ainda, segundo a ABNT NBR ISO/IEC 27002 (2005), a segurança da informação é adquirida a partir da implantação de um conjunto de controles apropriados, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de software e hardware. Estes controles precisam ser estabelecidos, implantados, monitorados, analisados criticamente e melhorados, onde necessário, para garantir que os objetivos do negócio e de segurança da organização sejam atingidos.

2.6 NECESSIDADE DA SEGURANÇA DA INFORMAÇÃO

Conforme descrito na ABNT NBR ISO/IEC 27002 (2005), muitos sistemas de informação não foram projetados para serem seguros. A segurança da informação que pode ser obtida por meios técnicos é limitada e deve ser amparada por uma gestão e por procedimentos adequados. A identificação de controles a serem implantados requer um planejamento cuidadoso e uma atenção aos detalhes.

Para Neto e Solonca (2007), a crescente utilização de soluções informatizadas nas distintas áreas de serviços exige maior exposição dos valores e das informações, além de níveis de segurança adequados. O avanço da tecnologia da informação, migrando de um ambiente centralizado para um ambiente distribuído, interligando redes internas e externas, adicionada à revolução da Internet, modificou a forma de se fazer negócios. Isto fez com que as empresas se preocupassem mais com o controle de acesso às suas informações bem como a proteção dos ataques, tanto internos quanto externos.

Ainda para Neto e Solonca (2007), com o advento dos computadores pessoais e das redes de computadores que são capazes de conectar o mundo inteiro, os aspectos de segurança atingiram tal complexidade que há a necessidade de desenvolvimento de equipes cada vez mais especializadas para a sua gerência.

Paralelamente, os sistemas de informação também adquiriram uma suma importância para a sobrevivência da maioria das organizações modernas, uma vez que, sem computadores e redes de comunicação, a prestação de serviços de informação pode se tornar impraticável.

Um exemplo prático da afirmação acima é citado por Neto e Solonca (2007), dizendo que um banco não trabalha exatamente com dinheiro, mas com

informações financeiras relacionadas com valores seus e de seus clientes. A maior parte destes dados é de natureza sigilosa, por força de determinação legal ou por se tratar de informações de natureza pessoal, que inspecionam ou mostram a vida econômica dos clientes, os quais podem vir a sofrer danos, caso elas sejam levadas a público.

Ainda concluem que, independente do setor da economia em que a empresa atue, as informações estão relacionadas com seu processo de produção e de negócio, políticas estratégicas, marketing, cadastro de clientes, etc. Não interessa o meio físico em que as informações estão armazenadas, elas são de valor incalculável não só para a empresa que as gerou, como também para seus concorrentes. Em último caso, mesmo que as informações não sejam sigilosas, na maioria das vezes elas estão relacionadas às atividades diárias da empresa que, sem elas, poderia ter complicações.

Na visão da ISACA (2010), a auditoria de TI é responsável por fazer uma revisão e avaliação dos riscos do ambiente de trabalho dos sistemas de informação que suportam os processos de negócio. A atividade da auditoria de TI tem como intuito ajudar a organização por meio da identificação e avaliação de exposições ao risco que sejam significativas, bem como contribuir para o avanço dos mecanismos de gestão de risco e de controle dos sistemas de informação.

No ponto de vista do IIA (2005), a auditoria de TI tem que aferir a capacidade dos controles dos sistemas de informação para resguardar a organização contra as ameaças mais relevantes e deve fornecer evidência de que os riscos residuais são pouco prováveis de causar danos significativos à organização e às suas partes interessadas, os *stakeholders*.

Segundo Neto e Solonca (2007), os tipos de auditoria mais comuns são classificados quanto à forma de abordagem, ao órgão fiscalizador e à área envolvida.

No Quadro 1, estão inseridas as classificações dos tipos de auditoria.

Classificação	**Tipos de auditoria**	**Descrição**
Quanto à forma de abordagem	Auditoria horizontal	Auditoria com tema específico, realizada em várias entidades ou serviços paralelamente.
	Auditoria orientada	Focaliza uma atividade específica qualquer ou atividades com fortes indícios de fraudes ou erros.

Quanto ao órgão fiscalizador	Auditoria interna	Auditoria realizada por um departamento interno, responsável pela verificação e avaliação dos sistemas e procedimentos internos de uma entidade. Um de seus objetivos é reduzir a probabilidade de fraudes, erros, práticas ineficientes ou ineficazes. Este serviço deve ser independente e prestar contas diretamente à classe executiva da corporação.
	Auditoria externa	Auditoria realizada por uma empresa externa e independente da entidade que está sendo fiscalizada, com o objetivo de emitir um parecer sobre a gestão de recursos da entidade, sua situação financeira, a legalidade e regularidade de suas operações.
	Auditoria articulada	Trabalho conjunto de auditorias internas e externas, devido à superposição de responsabilidades dos órgãos fiscalizadores, caracterizado pelo uso comum de recursos e comunicação recíproca dos resultados.
Quanto à área envolvida	Auditoria de programas de governo	Acompanhamento, exame e avaliação da execução de programas e projetos governamentais. Auditoria do planejamento estratégico - verifica se os principais objetivos da entidade são atingidos e se as políticas e estratégias são respeitadas.
	Auditoria administrativa	Engloba o plano da organização, seus procedimentos, diretrizes e documentos de suporte à tomada de decisão.
	Auditoria contábil	É relativa à fidedignidade das contas da instituição. Esta auditoria, consequentemente, tem como finalidade fornecer alguma garantia de que as operações e o acesso aos ativos se efetuem de acordo com as devidas autorizações.
	Auditoria financeira	Conhecida também como auditoria das contas. Consiste na análise das contas, da situação financeira, da legalidade e regularidade das operações e aspectos contábeis, financeiros, orçamentários e patrimoniais, verificando se todas as operações foram corretamente autorizadas, liquidadas, ordenadas, pagas e registradas. Auditoria de legalidade - conhecida como auditoria de conformidade. Consiste na análise da legalidade e regularidade das atividades, funções, operações ou

		gestão de recursos, verificando se estão em conformidade com a legislação em vigor.
	Auditoria operacional	Incide em todos os níveis de gestão, nas fases de programação, execução e supervisão, sob a ótica da economia, eficiência e eficácia. Analisa também a execução das decisões tomadas e aprecia até que ponto os resultados pretendidos foram atingidos.
	Auditoria de sistemas informatizados	Tipo de auditoria essencialmente operacional, por meio da qual os auditores analisam os sistemas de informação, o ambiente computacional, a segurança de informações e o controle interno da entidade fiscalizada, identificando seus pontos fortes e deficiências.

Quadro 1 - Classificação dos tipos de auditoria
Fonte: Neto e Solonca (2007)

Para o desenvolvimento do modelo de auditoria deste trabalho, será utilizada a auditoria de sistemas informatizados que, conforme Neto e Solonca (2007), é um tipo de auditoria operacional, ou seja, analisa a gestão de recursos, focalizando os aspectos de eficiência, eficácia, confidencialidade, integridade, disponibilidade, conformidade e confiabilidade.

Neto e Solonca (2007) afirmam que dependendo da área que será averiguada, este tipo de auditoria pode compreender todo o ambiente de informática ou a organização do departamento de informática. Além disso, podem considerar os controles sobre bancos de dados, redes de comunicação e de computadores, além de controles sobre aplicativos.

Desta forma, sob o entendimento dos tipos de controles identificados por Neto e Solonca (2007), os autores também afirmam que a auditoria pode ser separada em duas grandes áreas:

- Auditoria de segurança de informações: este tipo de auditoria em ambientes informatizados decide a postura ou a situação da empresa em relação à segurança das informações. Ela avalia a política de segurança da informação e também os controles relacionados a aspectos de segurança e controles que influenciam o bom funcionamento dos sistemas da organização. Tais controles estão descritos a seguir:

  - Avaliação da política de segurança;

- Controles de acesso lógico;
- Controles de acesso físico;
- Controles ambientais;
- Plano de contingência e continuidade de serviços;
- Controles organizacionais;
- Controles de mudanças;
- Controle de operação dos sistemas;
- Controles sobre os bancos de dados;
- Controles sobre computadores;
- Controles sobre ambiente cliente-servidor.

- Auditoria de aplicativos: este tipo de auditoria está direcionado para a segurança e o controle de aplicativos específicos, incluindo aspectos que fazem parte da área que o aplicativo atende, como: orçamento, contabilidade, estoque, marketing, RH, etc. A auditoria de aplicativos compreende:
  - Controles sobre o desenvolvimento de sistemas e aplicativos;
  - Controles de entrada, processamento e saída de dados;
  - Controles sobre o conteúdo e funcionamento do aplicativo com relação à área por ele atendida.

2.7 AMEAÇAS

Na definição da ABNT NBR ISO/IEC 27002 (2005), é uma potencial causa de um incidente indesejado, que pode culminar em dano para um sistema ou organização.

Para Neto e Solonca (2007), as ameaças podem ser definidas como sendo agentes ou condições incidentes que comprometem as informações e seus ativos, por meio da exploração de vulnerabilidades.

2.8 VULNERABILIDADES

Na definição da ABNT NBR ISO/IEC 27002 (2005), é uma fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças.

Neto e Solonca (2007) acreditam que as vulnerabilidades podem ser definidas como fragilidades presentes ou associadas a ativos que manipulam e/ou processam informações, que podem ser exploradas por ameaças e deixam que a ocorrência de um incidente de segurança aconteça, comprometendo negativamente um ou mais princípios da segurança da informação: confidencialidade, integridade e disponibilidade.

Os autores ainda concluem que as vulnerabilidades por si só não provocam acidentes de segurança, uma vez que são elementos passivos. Porém, quando possuem um agente causador, como ameaças, esta condição favorável provoca danos ao ambiente.

As vulnerabilidades citadas por eles estão inseridas no Quadro 2:

Físicas	• Instalações prediais fora do padrão; • Salas de equipamentos mal planejadas; • A falta de extintores, detectores de fumaça e outros para combate a incêndio em sala com armários e fichários estratégicos; • Risco de explosões, vazamentos ou incêndio.
Naturais	• Os computadores são suscetíveis a desastres naturais, como incêndios, enchentes, terremotos, tempestades; • Outros, como falta de energia, o acúmulo de poeira, o aumento de umidade e de temperatura, etc.
Hardware	• Falha nos recursos tecnológicos (desgaste, obsolescência, má utilização) ou erros durante a instalação.
Software	• Erros na aquisição de softwares sem proteção ou na configuração podem ter como consequência uma maior quantidade de acessos indevidos, vazamentos de informações, perda de dados ou indisponibilidade do recurso quando necessário.
Mídias	• Discos, fitas, relatórios e impressos podem ser perdidos ou danificados. A radiação eletromagnética pode afetar diversos tipos de mídias magnéticas.
Comunicação	• Acessos de intrusos ou perda de comunicação.
Humanas	• Rotatividade de pessoal; • Falta de treinamento; • Compartilhamento de informações confidenciais na execução de rotinas de segurança; • Erros ou omissões; • Ameaça de bomba, sabotagens, distúrbios civis, greves, vandalismos, roubos, destruição da propriedade ou dados, invasões ou guerras.

Quadro 2 – Vulnerabilidades no ambiente de TI
Fonte: Neto e Solonca (2007)

2.9 RISCO

Na definição da ABNT NBR ISO/IEC 27002 (2005), é uma combinação da probabilidade de um evento e de suas consequências.

Na definição da ABNT NBR ISO/IEC 27005 (2008), é a possibilidade de uma determinada ameaça explorar vulnerabilidades de um ativo ou de um conjunto de ativos, desta maneira prejudicando a organização.

Ambas as definições estão corretas, porém a apresentada pela ABNT NBR ISO/IEC 27005 (2008), traz uma abordagem mais completa.

2.10 ACESSO A SERVIÇOS POR TECNOLOGIA MÓVEL

O Ibope, em pesquisa encomendada pela empresa Qualcomm, com dados de 2014, divulgada pela revista Exame, (EXAME, 2014), constatou que um total dos usuários que possuem smartphones utilizam algum meio de comunicação com a internet, seja por 3g/4g ou Wi-Fi fixa. Afirmou também que um ponto, o que leva a aquisição dos aparelhos, é a necessidade de estar *online* o tempo todo.

Essas restrições aos acessos provem por outros fatores também, tais como, culturais, medos por não conhecer o funcionamento, achar difícil os termos, insegurança, esses, entre outros, além da enorme crescente, são motivos que levam a população a não aderirem ainda mais a utilização de serviços por tecnologia móvel. Essas barreiras podem ser as mais complicadas para expandir ainda mais a utilização. A tecnologia permitiu o desenvolvimento de novos canais de distribuição pelas empresas de telecomunicação através da Internet, que hoje faz movimentar bilhões de reais em transações entre empresas e clientes, porém o receio ainda é perceptível.

Ainda assim, segundo pesquisa realizada por TELECO (2015), notamos enorme crescimento, como demonstra os dados coletados da Anatel (Agencia Nacional de Telecomunicações), indicando que o Brasil terminou agosto de 2015 com aproximadamente 280 milhões de celulares e está passando por melhorias na tecnologia para propiciar a disseminação da população de baixa renda.

2.10.1 Mobile Payment

Após a adaptação com caixas eletrônicos e do acesso via Internet, as instituições bancárias começaram a investir no autoatendimento por aparelhos celulares, que é denominado como *Mobile Banking* (Sistema de operações financeiras via celular) esse tipo de serviço está ganhando mais funções e novos

usuários. O Serviço de *Mobile Payment* serve de incentivo para pessoas que possui pouco tempo hábil para deslocamentos, assim poderá efetuar seus pagamentos via celular, sem precisar arcar com os custos de transporte e tempo para irem até agências bancárias.

As agências bancárias e as operadoras de celulares estão incessantemente na busca de atualizações tecnológicas e parcerias. Pelo motivo de que, se de um lado as operadoras poderão aumentar suas receitas com o acréscimo no tráfego de dados, os bancos terão o acréscimo em suas carteiras de clientes, e por tudo isso, serão muito rentáveis, porque vão estar fora das agências, diminuindo as filas, assim como os famosos custos bancários.

2.11 CONCEITO DE AUDITORIA

Segundo Carneiro (2004), o conceito de auditoria pode ser citado como um estudo crítico que tem o objetivo de avaliar a eficácia e eficiência de um departamento ou uma instituição.

Dito de outro modo, toda e qualquer auditoria é a atividade que consiste na emissão de uma opinião profissional sobre o objeto de análise, a fim de confirmar se cumpre adequadamente as condições que lhe são exigidas (CARNEIRO, 2004).

Para Neto e Solonca (2007), a auditoria é uma atividade que reúne a análise das operações, processos, sistemas e responsabilidades gerenciais de uma determinada entidade, com o intuito de validar sua conformidade com certos objetivos e políticas institucionais, regras, orçamentos, normas ou padrões.

2.11.1 COBIT 4.1

COBIT, sigla que vem da língua inglesa, *Control Objectives For Information end Relatet Technology,* traduzida para o português, Objetivo de Controle para Tecnologia da Informação e Áreas Relacionadas, trata-se de um agrupamento de boas práticas com objetivo de dar suporte a governança de TI.

Na visão da ISACA (2010), o COBIT 4.1 é o modelo globalmente aceito que assegura que a TI esteja alinhada com os objetivos do negócio e que seus recursos sejam utilizados de maneira responsável e os riscos gerenciados de forma adequada. O novo modelo representa um aprimoramento do COBIT 4.0 e pode ser

usado para aperfeiçoar o trabalho já realizado com versões anteriores. As atualizações do COBIT 4.1 incluem um aperfeiçoamento na mensuração de desempenho, melhorias nos objetivos de controle e melhor alinhamento dos objetivos de TI e negócios.

Segundo a ISACA (2010), o COBIT auxilia as organizações a diminuírem os riscos de TI, a aumentarem o valor obtido com a TI e a atenderem às regulamentações de controle. Por exemplo, o Banco Central do Brasil faz uso do COBIT como um guia para avaliação de bancos e instituições financeiras, o TCU (Tribunal de Contas da União) baseia-se no COBIT para seus programas de auditoria para avaliação de várias entidades nacionais. Esses e outros exemplos de utilização por órgãos de controle e supervisão tornam esta nova versão do COBIT uma ferramenta útil à todas organizações que precisam manter um nível adequado de governança em TI.

Baruque e Santos (2010) afirmam que devido ao fato de ser mais focado em objetivos de negócio, o conteúdo do COBIT é muito abrangente, mas pouco detalhado no que diz respeito a *como* os processos devem ser implantados. O COBIT contém muito sobre o *quê* deve ser feito e *para quê* deve ser feito e, por outro lado, contém pouco sobre o *como* deve ser feito. Dessa forma a utilização do COBIT ajudará a empresa a alinhar os objetivos do negócio aos objetivos da TI, sendo o elo entre o planejamento estratégico da empresa e o plano diretor de TI.

Objetivando um melhor entendimento de como o COBIT pode ajudar uma organização, Baruque e Santos (2010) oferecem um exemplo de uma empresa que possua em seu plano estratégico o seguinte objetivo: melhorar o alinhamento estratégico da TI com o negócio. Mesmo parecendo algo abstrato, segundo os autores, os objetivos estratégicos são assim, genéricos o suficiente para darem uma direção, mas não detalhados o suficiente para limitar as opções de quem precisa concretizá-los.

Ainda segundo os dois autores, no Egito antigo, autoridades providenciavam averiguações independentes nos registros de arrecadações de impostos. Na Grécia, eram realizadas inspeções nas contas de funcionários públicos através da comparação de gastos com autorizações de pagamentos. Já os nobres castelos medievais ingleses indicavam auditores que revisavam os registros contábeis e relatórios preparados pelos criados.

Purpura (2008), afirma que a auditoria de empresas começou com a legislação britânica decretada durante a revolução industrial, em meados do século XIX. Progressos na tecnologia industrial e de transporte fomentaram novas economias de escala, empresas maiores, o aparecimento de administradores profissionais e o crescimento da ocorrência de situações em que os donos de empresas não estavam presentes nas ações diárias da corporação. No início da auditoria, este serviço tinha que ser feito por acionistas que não eram administradores das empresas.

> Na época em que as informações eram armazenadas apenas em papel, a segurança era relativamente simples. Bastava trancar os documentos em algum lugar e restringir o acesso físico àquele local. Com as transformações tecnológicas e o uso de computadores de grande porte, a estrutura de segurança já ficou um pouco mais sofisticada, englobando controles lógicos, porém ainda concentrados. (TCU, 2012, p.7)

Singleton (2011) informa que auditores de TI vem realizando contribuições desde o começo da era de TI, quando empresas e órgãos governamentais passaram a utilizar o computador para aspectos financeiros.

Neto e Solonca (2007) afirmam que o bem mais precioso de uma empresa pode não ser o produzido pela sua linha de produção ou o serviço prestado, mas as informações relacionadas com este bem de consumo ou serviço. Ao longo da história, o ser humano sempre buscou o controle das informações que lhe eram relevantes de alguma forma. O que mudou desde então foram as formas de registros e armazenamento das informações. Se na pré-história e até mesmo nos primeiros milênios da idade antiga o principal meio de armazenamento e registro de informações era a memória humana, com o início dos primeiros alfabetos isto começou a mudar. Mas foram somente nos últimos dois séculos que as informações passaram a ter importância essencial para as organizações humanas.

Ainda para Neto e Solonca (2007), atualmente, não há organização humana que não seja altamente dependente da tecnologia de informações, em maior ou menor grau. E o grau de dependência agravou-se muito em função da tecnologia de informática, que possibilitou acumular grandes quantidades de informações em espaços restritos. O meio de registro é, ao mesmo tempo, meio de armazenamento, meio de acesso e meio de divulgação. Esta característica traz efeitos graves para as organizações, por facilitar os ataques de pessoas não autorizadas.

Complementa-se com a afirmação de Baruque e Santos (2010) que, a dependência da TI torna-se cada vez mais crítica, em uma economia baseada no conhecimento, onde as organizações usam a tecnologia para gerenciar, desenvolver e reportar sobre ativos intangíveis, tais como informação e conhecimento. O êxito da empresa só pode ser alcançado quando tais ativos são seguros, precisos, confiáveis e proporcionados no tempo certo à pessoa certa. Tal dependência da TI implica uma grande vulnerabilidade que é inerente aos ambientes complexos de TI. Ameaças, tais como erros e omissões, abusos, crimes cibernéticos, fraudes, bem como sistemas indisponíveis custam muito caro para qualquer organização.

Conclui-se então com a linha de raciocínio de Neto e Solonca (2007), que auditar é preciso porque o uso desapropriado dos sistemas informatizados pode impactar uma sociedade. Informação com pouca exatidão pode causar a alocação precipitada de recursos dentro das corporações e as fraudes podem ocorrer devido à falta de sistemas de controle. Assim, para assegurar que os investimentos feitos em tecnologia da informação voltem para a empresa na forma de lucros e identificação de menores gastos com a TI, é onde o auditor de sistemas informatizados irá atuar. De posse dos objetivos, normas ou padrões da corporação o auditor irá verificar se tudo está funcionando como deveria.

2.12 CRIAÇÃO DO MODELO DE SI COM BASE NA ABNT NBR ISO/IEC 27002

O principal referencial para o desenvolvimento do modelo de auditoria de segurança da informação deste trabalho serão as normas da ABNT NBR ISO/IEC 27002.

A Associação Brasileira de Normas Técnicas (ABNT) é um Fórum Nacional de Normalização. As Normas Brasileiras, cujo conteúdo é de responsabilidade dos Comitês Brasileiros (ABNT/CB), dos Organismos de Normalização Setorial (ABNT/ONS) e das Comissões de Estudo Especiais Temporárias (ABNT/CET), são elaboradas por Comissões de Estudo (CE), formadas por representantes dos setores envolvidos, delas fazendo parte: produtores, consumidores e neutros (universidades, laboratórios e outros) (ABNT, 2005).

A ABNT NBR ISO/IEC 17799 foi elaborada no Comitê Brasileiro de Computadores e Processamento de Dados (ABNT/CB-21), pela Comissão de

Estudo e Segurança Física em Instalações de Informática (CE-21:204.01). O projeto circulou em Consulta Nacional conforme Edital nº 03, de 31/03/2005, com o número de Projeto NBR ISO/IEC 17799. A partir de 2007, a nova edição da ISO/IEC 17799 foi incorporada ao novo esquema de numeração ISO/IEC 27002 (ABNT, 2005).

Neto e Solonca (2007) afirmam que a atividade de auditoria pode ser dividida em três fases:

- Planejamento;
- Execução (supervisão);
- Relatórios.

2.12.1 Fase De Planejamento

Segundo Neto e Solonca (2007), o planejamento desempenha o mesmo papel em variadas áreas, na vida pessoal, no desenvolvimento de um novo produto, entre outros. Dele, resulta um arranjo ordenado dos passos necessários à condução de determinado objetivo. Tudo que é feito de forma organizada está fadado ao sucesso.

O planejamento da auditoria abrange vários passos importantes. A obtenção de conhecimento em relação ao negócio e à organização, representa a etapa crítica deste processo, pois forma a base para a realização de outros procedimentos de auditoria. Ao planejar o seu trabalho, o auditor toma importantes decisões sobre a relevância e o risco de auditoria. Um produto importante do planejamento envolve a tomada de decisões preliminares sobre a estratégia a ser adotada.

Um aspecto muito importante na obtenção das informações relacionadas ao negócio do cliente é o ciclo de vida das informações. É baseado nestes fluxos que se avalia a segurança que está envolvida.

Sendo mais específico, é preciso realizar um inventário do ambiente computacional do cliente, com informações sobre hardware, sistemas operacionais, arquitetura computacional, metodologia usada no desenvolvimento de software e os sistemas que são ou não críticos.

2.12.2 Fase De Execução / Supervisão

Segundo Neto e Solonca (2007), seguinte a etapa do planejamento, vem a fase de execução / supervisão. Esta envolve o direcionamento dos trabalhos dos assistentes para alcançar os objetivos de auditoria e conferir se os objetivos de fato foram atingidos.

2.12.3 Fase De Relatórios

Neto e Solonca (2007) acreditam que as responsabilidades do auditor na conclusão dos trabalhos podem ser divididas em três categorias: conclusão do trabalho de campo, avaliação das descobertas e comunicação com o cliente.

Conclusão do trabalho em campo: Neto e Solonca (2007) afirmam que na conclusão do trabalho de campo, o auditor precisa ter certeza de que já realizou todas as entrevistas e coletou todos os dados necessários para analisar as evidências e, assim, desenvolver um parecer correto, que auxilie o cliente a melhorar o seu ambiente de TI aumentando a sua disponibilidade, o seu caráter confidencial e a sua integridade de dados.

Avaliação das descobertas: Neto e Solonca (2007) afirmam que ao avaliar o que foi verificado na auditoria, o auditor tem por objetivos determinar o tipo de parecer a ser emitido. Na conclusão da auditoria, é necessário que todas as constatações sejam resumidas e avaliadas.

Neto e Solonca (2007) concluem que a administração do ambiente de informática, por sua vez, pode tentar defender a sua posição, porém isto não deve interferir na avaliação de conformidade da norma de segurança, caso contrário, incorrerá no erro de ser complacente com muitas inconformidades e acabará sem ajudar o cliente como proposto. Nesta situação é imprescindível que haja uma formalização para não haver dúvidas sobre o caso. Isto gera segurança para todos os envolvidos, tanto no lado do cliente quanto no lado do auditor. No final, geralmente se chega a um acordo a respeito das alterações que devem ser feitas e o auditor pode então ter que emitir um parecer explicando a situação. A comunicação da opinião do auditor é feita por meio de seu parecer.

Comunicação com o cliente: Neto e Solonca (2007) argumentam a comunicação em qualquer período da auditoria, seja durante ou na conclusão dos

trabalhos, deve ser feita por um canal escolhido pelas partes envolvidas, ou seja, tanto pelo cliente, quanto pela empresa de auditoria. Tal prática evita distorções de fatos e atos, pois deve ser feita formalmente por escrito, com cópia para todas as pessoas envolvidas no trabalho dos dois lados e com cópia para o comitê de segurança da empresa, se for o caso. Ainda finalizam, dizendo que o relatório entregue à administração da empresa deve ser cuidadosamente elaborado, bem organizado e escrito em tom de críticas construtivas.

Segundo ABNT NBR ISO/IEC 27002 (2007), a análise de riscos deve identificar, quantificar e priorizar os riscos com base nos critérios de aceitação e objetivos da organização. O resultado das análises deve orientar e determinar prioridades e as ações adequadas para o gerenciamento de riscos, bem como os controles que serão implantados.

Ainda segundo a ABNT NBR ISO/IEC 27002 (2007), a análise de riscos precisa ser realizada periodicamente, para considerar as mudanças no ambiente de TI e no risco envolvido. Esta análise de riscos deve ser atingida de forma metódica, capaz de gerar resultados comparáveis e reproduzíveis.

A ABNT NBR ISO/IEC 27002 (2007) descreve que a análise de riscos no ambiente de TI deve ter um escopo bem definido para ser eficaz, além de incluir relacionamentos com análises/avaliações dos riscos de outras áreas, quando necessário. O escopo pode ser de toda a organização, parte dela, em apenas um sistema de informação específico, em componentes de um sistema específico ou em serviços onde isto seja praticável, realístico e útil.

2.12.4 Tipos De Controle

Segundo Baruque e Santos (2007), controle é a fiscalização efetuada sobre as atividades de pessoas, órgãos, departamentos ou sobre produtos, para que estes não se desviem das normas ou objetivos previamente estabelecidos. Existem três tipos de controles, listados no Quadro 3.

Preventivos	Usados para prevenir fraudes, erros ou vulnerabilidades. (senhas de acesso a algum sistema informatizado, por exemplo).

Detectivos	usados para detectar fraudes, erros, vulnerabilidades (por exemplo: Log de eventos de tentativas de acesso a um determinado recurso informatizado)
Corretivos	usados para corrigir erros ou reduzir impactos causados por algum sinistro (planos de contingência, por exemplo)

Quadro 3 – Descrição dos tipos de controles existentes
Fonte: Neto e Solonca (2007)

Ainda segundo Baruque e Santos (2007), um dos objetivos desses controles é, primeiramente, a manutenção do investimento feito pela corporação em sistemas informatizados, tendo em vista que os sistemas de informação interconectados de hoje desempenham um papel de suma importância no sucesso empresarial de um empreendimento. Esses controles objetivam também, evitar que algum dano venha a ocorrer. Não conseguindo impedir, é preciso fazer com que o impacto seja pequeno e, se mesmo assim, o impacto for grande, ter em mãos processos que ajudem na reconstrução do ambiente.

Muitos sistemas de informação não foram projetados para serem seguros. A segurança da informação que pode ser alcançada por meios técnicos é limitada e deve ser apoiada por uma gestão e por procedimentos adequados. A identificação de controles a serem implementados exige um planejamento cauteloso e uma atenção aos detalhes. A gestão da segurança da informação requer pelo menos a participação de todos os funcionários da organização. Em determinados casos, é possível que seja necessária também a participação de acionistas, fornecedores, terceiras partes, clientes e ou outras partes externas. Uma consultoria externa especializada pode ser também necessária (ABNT NBR ISO/IEC 27002, 2007).

A ABNT NBR ISO/IEC 27002 (2007), contém 11 seções de controles de segurança da informação, que juntas somam 39 categorias principais de segurança e uma seção introdutória que engloba a análise/avaliação e o tratamento de riscos.

Cada seção possui um número das principais categorias de segurança da informação. As 11 seções (acompanhadas com o respectivo número de categorias) são:

- Política de Segurança da Informação (1 categoria);
- Organizando a Segurança da Informação (2 categorias);

- Gestão de Ativos (2 categorias);
- Segurança em Recursos Humanos (3 categorias);
- Segurança Física e do Ambiente (2 categorias);
- Gestão das Operações e Comunicações (10 categorias);
- Controle de Acesso (7 categorias);
- Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação (6 categorias);
- Gestão de Incidentes de Segurança da Informação (2 categorias);
- Gestão da Continuidade do Negócio (1 categoria); e
- Conformidade (3 categorias).

A ordem das seções não define seu grau de importância. Dependendo das circunstâncias, todas as seções podem ser relevantes. Contudo, cada organização que faz uso desta norma deve detectar quais são as seções aplicáveis, o quão importante elas são e qual a sua aplicação para os processos específicos do negócio. Todos os parágrafos na ABNT NBR ISO/IEC 27002 também não estão ordenados por prioridade, a menos quando explicitado (ABNT NBR ISO/IEC 27002, 2007).

3 SITUAÇÕES QUE COMPROMETEM A SEGURANÇA DA INFORMAÇÃO

Empresas não sobrevivem sem tecnologia, e estas precisam estar conectadas para que atinjam seu benefício total. Sistemas conectados trazem benefícios para as organizações, porém também algumas preocupações quanto a segurança dos dados e informações que ali trafegam.

Criminosos virtuais estão a cada dia mais evoluídos, utilizando novas tecnologias e fazendo com que muitos ataques sejam realizados de forma automatizada, ou seja, sem a intervenção do mesmo, onde ataques são realizados pela máquina. Com isso, sistemas de proteção precisam ser mais complexos a ponto de trabalhar com grande volume de dados em massa, ataques contínuos, onde consigam separar os dados validos dos mal-intencionados.

Para tornar um ambiente mais seguro, se faz necessário a implantação de políticas de segurança através das quais poderão ser notadas ações que são verdadeiras ou tentativa de intrusão. Politicas bem definidas contemplando restrições de acessos são indispensáveis para se atingir os objetivos de segurança da informação.

3.1 E-MAILS FALSOS

Trocar informações entre redes, tais como textos imagens e arquivos, é algo necessário entre as organizações. Entre as principais ferramentas para troca de informações está o Correio Eletrônico, o qual possui como principal vantagem a facilidade de atingir um número grande de destinatários, em longas distâncias em pouquíssimo tempo.

O correio eletrônico, não deixa de ser uma ferramenta de trabalho dentro da organização e por isso, sua utilização deve ser considerada em políticas de segurança da informação na organização.

Como sendo o principal meio de comunicação entre empresas e pessoas, este meio de comunicação é visado como forma de disseminação de *malware* por criminosos virtuais. Conforme Microsoft (2015*), " Malware é um nome abreviado para "software malicioso". É qualquer tipo de software indesejado, instalado sem o seu devido consentimento. Vírus, worms e cavalos de tróia são exemplos de*

software mal-intencionado que com frequência são agrupados e chamados, coletivamente, de malware”(Microsoft,2015) .

Conforme Microsoft (2015), golpes por e-mail podem ser reconhecidos se uma mensagem contiver informações alarmistas que contenha algum tipo de ameaça de suspensão de serviços, promessas de renda com pouco ou nem um esforço, negócios em geral que parecem ser muito facilitadores para ser verídica a oferta, pedidos de doações a entidades caridosas depois de algum desastre que vira a ser notícia ou mensagens que contenham erros de ortografia e gramática.

3.2 CONTROLE DE SENHAS

Vulnerabilidade no cadastro de usuários em sistemas na *internet* propiciam a injeção de códigos maliciosos baseados em *scripts*. Com o código injetado, a cada seção do usuário, informações da seção do mesmo é enviada ao criminoso.

Com dados da seção da vítima, pode-se executar qualquer operação em seu nome, da qual ela tem acesso, aí a importância de controle de acesso bem definido, já dificultando ações mais perigosas.

3.3 SISTEMAS SEM TRATAMENTO DE SI

Correções em softwares feitas por programadores, inexperientes, ou até mesmo sistemas sendo projetados do zero, em alguns casos, tem pouca ou nem uma preocupação com segurança. Correções feitas sob pressão, sem tempo hábil para planejamento e estudo, podem abrir diversas vulnerabilidades em redes inteiras.

Sistemas de detecção de intrusão (IDS) foram projetados como mecanismos de proteção para aplicações com pouco ou nem um tratamento em segurança, sistemas que não validam informações de entradas e saídas, porém em grande sacada, vulnerabilidades são tratadas por sistemas de segurança após já terem sido exploradas por certas vezes em larga escala.

3.4 AUSÊNCIA DE POLÍTICAS, NORMAS E PROCEDIMENTOS.

Ausência de política de segurança ou política mal estabelecida ou desatualizada se torna uma falha de segurança. Devem ser definidas normas e procedimentos com o objetivo de impedir a interrupção dos serviços, furto ou vazamento de informações. A política deve ser construída de acordo com as necessidades do negócio.

De acordo com Freitas e Araujo (2008), a política de segurança deve ser revisada periodicamente, revisada a cada 6 meses, ou sempre que houverem mudanças de processos ou procedimentos que devam constar na mesma.

As informações acessadas, por qualquer que seja o sujeito, devem ser de alguma forma defendidos por uma política de segurança, a ausência desta, pode trazer eventos os quais exijam intervenção ou trazer vulnerabilidades.

3.5 FALTA DE GESTOR DE SEGURANÇA

"*Convêm que a política de segurança da informação tenha um gestor que tenha responsabilidade de gestão aprovada para desenvolvimento, análise crítica e avaliação da política de segurança da informação*". (ABNT ISO/IEC 27002, 2005. P. 9).

O gestor de segurança tem o papel de assegurar que a mesma esteja sendo cumprida por todas as áreas da organização.

3.6 CONSCIENTIZAÇÃO/TREINAMENTO DA EQUIPE

A política deverá ser descrita de forma clara, que não traga dúvida para os usuários. Todos os colaboradores da organização, inclusive fornecedores e terceiros deverão receber um treinamento para se adequar.

Para Freitas e Araujo (2008), é fundamental que os funcionários estejam preparados para a política, indispensável que sejam feitos treinamentos, palestras, avisos, guias de segurança, entre outros meios de comunicação que possam esclarecer todos os pontos.

3.7 ENGENHARIA SOCIAL

Mcforland, (2015), diz que muitos ataques pelas grandes redes, no caso os cíberataques, utilizada da engenharia social para buscar informações, ou seja, tenta persuadir um indivíduo na tentativa de injetar uma infecção ou buscar algum tipo de informação importante para o sucesso do ataque.

> "*A aplicação deliberada de técnicas enganosas concebidas para induzir alguém a divulgar informações ou executar ações que possam resultar na liberação dessas informações*" (MCFORLAND, 2015, P.2).

MCforland (2015), ainda informa que o ataque utiliza de várias formas para atingir a vítima, entre elas estão ***Sites*** estratégicos ou falsos para fornecer *malware,* ***e-mail*** da vítima, onde são encaminhados *links* direcionando para algum tipo de vírus, **telefone**, **Cara a cara**, **Correios**, embora pareça que não seja possível, ainda há registros de tentativas de ataques neste canal. O autor ainda cita que para amenizar o risco, pode ser considerado três formas mais importantes, **Conscientização continua das equipes**, **liberdade de comunicação** para todos fazerem questionamentos sobre suspeitas referente a engenharia social e outros tipos de golpes, **monitoramento e filtragem** dos meios de comunicação.

3.8 DESCARTE DE EQUIPAMENTOS E INFORMAÇÕES – VAZAMENTO DE INFORMAÇÕES

É comum o descarte de microcomputadores, celulares, tablets, correspondências documentos em geral, etc. dentro das organizações. Muitas empresas não se preocupam com os dados contidos nos descartes e acabam vazando informações.

Conforme Manual de Controle de segurança do banco itaÚ, (2010), mídias devem ser destruídas antes do descarte, documentos e cartas devem ser triturados e computadores e demais equipamentos sem mídias de armazenamento.

Vários criminosos cibernéticos conseguem sucesso em ataques apenas coletando informações de lixeiras de empresas, como anotações de senhas em blocos de anotações, informações confidenciais de clientes ou de próprios colaboradores, credenciais de acessos entre outros.

3.9 FALTA DE SEGREGAÇÃO DE FUNÇÕES

> “É um princípio da segurança usado para impedir que uma única pessoa possa acessar modificar ou usar ativos sem a devida autorização ou detecção, reduzindo os riscos de uso acidental ou deliberado destes ativos. Assegurar que estágios críticos de um processo, como a do administrador do sistema e do auditor de segurança, fiquem a cargo de dois ou mais indivíduos”. (BANCO ITAU, 2010 p.7).

Nota-se, em visitas empresariais, a utilização de usuários genéricos, onde vários colaboradores da empresa utilizam de determinado serviço, com as mesmas credenciais de acesso. Estas, muitas vezes com elevação de acesso, podendo ser executado tarefas com perfis de total liberdade, o que pode dificultar ou impedir que qualquer forma de auditoria consiga encontrar falhas em processos. Uma pessoa não deve ter autoridade completa sobre uma parcela significativa de qualquer processo, e a divisão de funções e perfis de acesso deve existir e ser auditado.

A ABNT ISO 27002 (2005) indica que se for difícil a segregação de funções, se faz necessário a existência de outros controles, como por exemplo a monitoração, auditoria e acompanhamento gerencial. Indica também que normalmente a dificuldade de segregação é encontrada por pequenas empresas.

3.10 FALHAS DE CONFIGURAÇÕES

Rohr (2014), afirma que falhas de segurança são normalmente aplicada em sistemas já inseguros. Indica que por exemplo que uma senha padrão foi esquecida de ser alterada, onde senhas padrões de equipamentos normalmente tem acesso irrestrito e total, um acesso indevido foi dado para indivíduo sem autorização, opções de segurança de equipamentos ou aplicativos não foram ajustadas devidamente.

O autor também assegura que software de usos cotidianos ou equipamentos em geral, a principal falha de configuração se refere a senha, onde a mesma foi esquecida de ser trocada, ou as políticas de senha de redes e softwares são fracas ao ponto de permitir senhas facilmente de ser quebradas. Já para provedores e demais servidores de serviços ligados diretamente ao acesso à internet, possibilitaria falhas de configurações mais complexas, abrindo brechas para ações dos criminosos, como por exemplo, permitindo acesso em roteadores de grande escala.

3.11 ATRIBUIR APENAS A ÁREA DE TECNOLOGIA À SEGURANÇA DA INFORMAÇÃO

Erros contínuos são identificado em organizações onde ligam diretamente a segurança de informação a área de TI da mesa, porém a segurança de informação deve ser alinhada entre todos os setores, sejam eles ligados mais ou menos a tecnologia para que haja sinergia entre as áreas e nem uma delas possa abrir vulnerabilidades se tratando em segurança da informação.

4 BOAS PRÁTICAS DE SEGURANÇA DA INFORMAÇÃO

Toda empresa que quer crescer no mercado, precisa estar conectada, utilizar da tecnologia e se atualizar constantemente para se tornar competitiva. Empresas que não utilizam qualquer meio de tecnologia ou conexão intranets ou internet são impulsionadas pela globalização a utilizar alguma forma de conexão.

> [...] empresas de todos os portes construíram redes conectadas à Internet para se comunicar com seus clientes e servir os dados que alimentam seus negócios. Essa coleta e digitalização de informações, aliada à vastidão e ao alcance das redes modernas, constitui uma oportunidade tentadora para ladrões: o roubo de dados. (INTEL, MCAFEE, 2015, P. 16).

Alves (2013) afirma que muitas empresas com necessidade de cortes no orçamento, acabaram deixando a segurança da informação um pouco de lado e isso se dá ao fato da falta de compreensão sobre as reais ameaças que enfrentam. O autor ainda comenta que para ter uma segurança da informação eficaz, é preciso mudar a maneira de pensar: não há mais espaço para apostar na sorte.

Edgar (2013) afirma que as empresas líderes não pensam nem um pouco em reduzir investimentos em área de segurança da informação, muito pelo contrário, investem mais e conseguem atingir resultados melhores.

> “É como se “joga” o “jogo”: alinhamento, liderança e profissionais treinados são fundamentais”. (EDGAR, 2013, P.6).

Segundo a ISO 27002 as para boas práticas de segurança da informação, é necessário se ter uma política de segurança sempre atualizada e auditada constantemente, esta deve ser atualizada sempre que houver mudança no processo ou em um período máximo de 6 meses. Ter um Gestor de segurança da informação com o papel de coordenador de segurança, este deve ser representado por membros de diferentes setores. Conscientizar colaboradores, fornecedores, terceiros, enfim, todos que fazem parte do quadro de recursos humanos da empresa, estes devem receber treinamentos, palestrar sobre segurança, explicações detalhadas das políticas da empresa, avisos diversos sobre o assunto e ter reciclagens periódicas, utilização consciente de aplicativos e serviços de tecnologia da organização, assim como qualquer documento com informações confidencias, seja ele impresso ou digitalizado, deve ser levado em conta na segurança da informação. As vulnerabilidades devem ser identificadas e tratadas, documentadas e consideradas em qualquer ação de melhoria ou incidentes. Plano

de continuidade do negócio deve ser bem definido, contingencias e todos os serviços críticos da organização devem ser mantidos em funcionamento. Planos de Backup devem existir e seguir os critérios de armazenamento externo, não adiantaria ter um backup na mesma sala de equipamentos, caso haja incidentes mais graves perde-se o backup e toda sua informação de origem. Backups devem ser mantidos o mais longe possível. Incidentes de segurança da informação assim como registros de auditoria, os logs, devem ser mantidos por período de tempo acordado para investigações futuras caso necessário. Políticas de credencias, senhas seguras devem ser utilizadas assim como a segregação de função.

Edgar, (2013) indica que a segurança da informação é um jogo de técnicas e estratégias avançadas. Que muda com frequência e o profissional deve acompanhar. Seguranças de outras décadas, ou até mesmo de anos passados, já não podem ser eficientes.

> [...] os líderes reconhecem que, para ter uma segurança eficaz, é preciso se transformar e adotar uma nova maneira de pensar. Eles estão cientes de que a própria sobrevivência do negócio exige a compreensão das ameaças de segurança, o preparo para enfrentá-las e respostas rápidas. (EDGAR, 2013, P.60).

Para Edgar (2013), como forma de melhorar o desempenho da segurança da informação, é necessário implantar uma estratégia abrangente de avaliação de riscos e adequar a eles os investimentos de segurança. Também é preciso compreender as informações do negócio entendendo os potenciais ali armazenados, buscando entender o que os concorrentes seriam capazes de fazer para chegar até esta informação. Entender que os requisitos de Segurança da Informação, e o negócio como um todo, passam por mudanças frequentes, todos os envolvidos precisam estar sincronizados. Pensamentos devem ser alinhados referente a segurança da informação, além de ser uma proteção, é também uma potente forma de criar valores para a empresa.

5 CONSIDERAÇÕES FINAIS

Atualmente todo negócio bem-sucedido depende da tecnologia da informação e da comunicação. Com isso, a informação passa a ser um dos ativos mais valiosos dentro da organização. Desta forma, podemos perceber que assim como qualquer outro ativo, a segurança da informação passa a ser uma atividade vital para garantir a proteção desse bem.

Para apoiar as organizações e os profissionais de TI, atrelados às ameaças internas e externas, as normas da ABNT NBR ISO/IEC 27002 são importantes referências para se conseguir atingir um nível adequado de segurança da informação dentro da organização. O modelo pode ser usado em qualquer outro tipo de negócio, independente do segmento que atue.

REFERÊNCIAS BIBLIOGRÁFICAS

ABNT, Associação Brasileira De Normas E Técnicas NBR ISO/IEC 27002, **Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação**. Rio de Janeiro: ABNT, 2005.

ABNT, Associação Brasileira De Normas e Técnicas NBR ISO/IEC 17799. **Tecnologia da informação - Técnicas de segurança - Código de prática para a gestão da segurança da informação.** Rio de Janeiro: ABNT, 2005.

ABNT, Associação Brasileira De Normas E Técnicas NBR ISO/IEC 27005. **Tecnologia da informação – Técnicas de segurança – Gestão de riscos de segurança da informação**. Rio de Janeiro: ABNT, 2008.

ALVES, Fernando; PWC. **Virando o jogo.** Disponível em <https://www.pwc.com.br/pt/estudos-pesquisas/assets/pesquisa-seguranca-inforrmacao-13e.pdf> Acesso em novembro de 2015

AMARAL, L. e Varajão, J. **Planeamento de Sistemas de Informação**. 4ª edição; Lisboa: Editora FCA, 2007.

ANATEL, **Agência Nacional de telecomunicações**. Disponível em: <http://www.anatel.com.br> Acesso em outubro de 2015.

BARUQUE, Lúcia Blondet; SANTOS, Luis Claudio dos. **Governança em Tecnologia da Informação**. Rio de Janeiro: Fundação CECIERJ, 2010.

CARNEIRO, Alberto. **Auditoria de Sistemas de Informação**. 2ª edição; Lisboa: Editora FCA, 2004.

EDGAR, R. P. D'Andrea; PWC. **Virando o jogo.** Disponível em <https://www.pwc.com.br/pt/estudos-pesquisas/assets/pesquisa-seguranca-inforrmacao-13e.pdf> Acesso em novembro de 2015

EXAME. **Gasto e vício de brasileiro em smartphone aumentaram em 2014**. 2014, Disponível em <http://exame.abril.com.br/tecnologia/noticias/gasto-e-vicio-de-brasileiro-em-smartphone-aumentaram-em-2014> Acesso em novembro de 2015

FREITAS, F; ARAUJO, M. **POLITICAS DE SEGURANÇA DA INFORMAÇÃO: Guia prático para elaboração e implementação.** 2. ed. Rio de Janeiro: Ciência Moderna LTDA, 2008

GIL, A. C. **Como elaborar projetos de pesquisa**. 4. ed. São Paulo:Atlas, 2002.

IDGNOW, Ciab 2011: **Bancos apostam em pagamentos e serviços no celular**. Disponível em: <http://idgnow.uol.com.br/internet/2011/06/17/ciab-2011-bancos-apostam-em-pagamentos-e- servicos-no-celular/ > Acesso em outubro de 2015

IIA - The Institute of Internal Auditors, **Global Technology Audit Guide: Information Technology Controls**. Florida: Inc. 2005.

ISACA, Information Systems Audit and Control Association. **ISACA Introduces Portuguese Edition of COBIT 4.1 (Portuguese)**. Disponível em < http://www.isaca.org/About-ISACA/Press-room/News-Releases/Portuguese/Pages/ISACA-Introduces-Portuguese-Edition-of-COBIT-4-1-Portuguese.aspx >. Acesso em setembro de 2015.

BANCO ITAU. **Manual de controles de segurança da informação para empresas de Gerenciamento Eletrônico de Documentos**. Disponível em: <http://www.itau.com.br/fornecedores/pdf/GerenciamentoDocumentos.pdf> Acesso em Novembro de 2015.

INTEL, security; MCAFEE. **Relatório do McAfee Labs sobre ameaças.** Intel Security; Mcafee, 2015.

MICROSOFT. **O que é malware?.** Disponível em <https://www.microsoft.com/pt-br/security/resources/malware-whatis.aspx> Acesso em novembro de 2015.

MCFORLAND, Charles. **Hackers Contra o Sistema Operacional Humano | Resumo Executivo**. Intel Security; Mcafee, 2015.

NETO, Abílio Bueno; SOLONCA, Davi. **Auditoria de Sistemas Informatizados**. 3ª edição; Palhoça: Unisul Virtual, 2007.

OLIVEIRA, Silvio Luís de. **Tratado de metodologia científica: projetos de pesquisas, TGI, TCC, monografias, dissertações e teses**. São Paulo: Pioneira Thomson Learning, 2002.

PURPURA, Philip P. **Security and Loss Prevention: An Introduction**. 5ª edição; Boston: Elsevier Butterworth-Heinemann, 2008.

SINGLETON, Tommie W. **Como o auditor de TI pode fazer contribuições substantivas para uma auditoria financeira**. 2011, Disponível em <http://www.isaca.org/Journal/archives/2011/Volume-1/Documents/jpdf11v1-how-the-IT-auditor-Portuguese.pdf> Acesso em novembro de 2015

ROHR, Altieres. **Como um hacker invade o computador?.** Disponível em <http://g1.globo.com/tecnologia/blog/seguranca-digital/post/pacotao-em-video-como-um-hacker-invade-o-computador.html> Acesso em Novembro de 2015

TCU, **Boas Práticas em Segurança da Informação**. 4. ed. Brasília: TCU, 2012.

TELECO, **Estatísticas de Celulares no Brasil.** Disponível em <http://www.teleco.com.br/ncel.asp> Acesso em novembro de 2015.

VERGARA, Sylvia Constant. **Projetos e relatórios de pesquisa em administração.** 5. ed. São Paulo: Atlas, 2004.