Faculdade de Tecnologia SENAC

Segurança da Informação nas Empresas
Uso efetivo de segurança da informação em equipes e departamentos de T.I.

Clécio Oliveira Pinto
Diego Fonseca Elcain
Raphael Moreno

Goiânia 2014

Segurança da Informação nas Empresas
Uso efetivo de segurança da informação em equipes e departamentos de T.I.

Clécio Oliveira Pinto[1], Diego Elcain[1], Raphael Moreno[1]

[1]Pós-Graduação em Segurança e Integração de Redes de Computadores em Ambientes Corporativos – Faculdade de Tecnologia SENAC – Goiânia, GO – Brasil

Contato[at]clecioooliveira.com, diego[at]cuidadodigital.com.br, raphaelserrinha12[at]hotmail.com

Abstract. *The purpose of this research is to reflect on the Information Security through data collection extracted through a form used in technical goianas companies. The data collected will be used to demonstrate the applicability in organizations when it comes to Information Security. After the collection and transformation of data into information, indexes will be presented applicability of ISO/IEC/NBR 27002.*

Resumo. *A proposta da presente pesquisa é fazer uma reflexão sobre a segurança de informação mediante a coleta de dados extraídos através de um formulário técnico aplicado nas empresas goianas. Os dados coletados servirão para demonstrar a aplicabilidade nas organizações em se tratando da segurança da informação. Após a coleta e transformação dos dados em informações, serão apresentados índices de aplicabilidade da ISO/IEC/NBR 27002.*

1. INTRODUÇÃO

A cada ano o mercado de Segurança Digital vem crescendo, isso devido à informação se tornar cada vez mais vulnerável. As necessidades de se manter competitivo com eficiência nos processos de negócios fizeram com que a informação se tornasse um dos principais ativos das organizações, o qual precisa ser protegido a todo custo de qualquer eventualidade.

A infraestrutura de TI antes era vista como um dos pilares de suporte das empresas, mas com toda evolução e a necessidade de manter segura a informação, a segurança tornou um fator prioritário na tomada de decisão e dos investimos das empresas. Hoje esse item já faz parte do negócio das organizações.

Segurança da informação consiste na proteção da informação de vários tipos de ameaças para garantir a confidencialidade, disponibilidade e integridade da informação a fim de proporcionar a continuidade do negócio, minimizar o risco ao negócio e maximizar o retorno sobre os investimentos e as oportunidades de negócio (ABNT NBR ISO/IEC 27002, 2005). Ela é essencial para qualquer empresa, independentemente do tamanho, seja ela de grande, médio ou pequeno porte (Krause (1999) e Albuquerque (2002).

Pesquisas realizadas pelas revistas CIO, CSO e Pricewaterhousecoopers entrevista mais de 12.800 executivos incluindo CEO (Chief Executive Officer - Diretor Executivo), CFO (Chief Financial Officer – Diretor de Finanças), CIO (Chief Information Officer – Diretor de TI), CISO (Chief Information Security Officer – Gestor de Segurança da Informação) e OSC (Office of Career Services – Diretor de Recursos Humanos) em mais de 170 países chega à conclusão que há resistência na liberação de recursos para aplicação da segurança da informação (COMPUTERWORLD, 2014).

Outra pesquisa realizada, dessa vez pela Microsoft mostra que o volume de computadores infectados por vírus é proporcional ao volume de sistema operacional pirata (MICROSOFT,

2014). Mais uma pesquisa de extrema importância realizada pela IDC, mostra que se os números de softwares piratas caíssem em 10% nos próximos quatro anos, mais de 500.000 novos postos de trabalhos poderiam ser gerados, podendo criar US$ 142 bilhões em novas atividades econômicas e US$ 32 bilhões em receitas fiscais para 2013 (PLAY-IT-SAFE, 2014).

Porém, a falta de informação geralmente leva as organizações a não adotar medidas de segurança dos seus ativos.

Mas, como promover aos gestores das organizações ações de conscientização, esclarecimento e informação no que se diz respeito a aplicabilidade da segurança da informação em suas organizações?

No decorrer desse trabalho conheceremos mais sobre o que é a ISO e o que diz a norma ABNT NBR ISO/IEC 27002 sobre gestão da segurança da informação. A técnica e metodologia utilizadas para realização da pesquisa, amostra e aptidão das empresas, cruzamentos das informações, métricas utilizadas para transformar dados em informação acompanhado do resultado final. Quais as sugestões da ISO estão sendo aplicadas nas empresas entrevistadas, relação aplicabilidade versus tamanho da organização, desempenho de aplicabilidade individual e por grupo de empresas, aplicabilidade por complexidade.

2. REFERENCIAL TEÓRICO

Várias referências bibliográficas foram de vital importância para o desenvolvimento desse artigo. A mais utilizada, com certeza, foi a norma ABNT NBR ISO/IEC 27002. Além de ser a principal referência para assegurar uma eficaz implantação de segurança da informação, também é, a principal referência para demonstrar um termômetro da conformidade de segurança da informação aplicado em uma empresa. A norma NBR ISO/IEC 27002 é a referência para o tema proposto, as outras referências serviram como apoio e complemento teórico no decorrer do artigo.

2.1. ISO - International Organization for Standardization

A ISO é uma Organização Internacional para Padronização formada por um conselho e comitês com membros oriundos de vários países. Seu objetivo é criar normas e padrões universalmente aceitos sobre a realização de atividades comerciais, industriais, científicas e tecnológicas. A IEC é uma organização voltada ao aprimoramento da indústria da informação (FERREIRA e ARAÚJO, 2006).

2.2. ABNT NBR ISO/IEC 27002

O objetivo da Norma ABNT (Associação Brasileira de Normas Técnicas) ISO/IEC (International Electrotechnical Commission – Comissão Eletrotécnica Internacional) 27002 é estabelecer diretrizes e princípios gerais para iniciar, implementar, manter e melhorar a gestão de segurança da informação em uma organização.

Os objetivos e os controles tem como finalidade ser implementados para atender aos requisitos identificados por meio da análise e/ou avaliação de riscos. A norma pode servir como um guia prático para desenvolver os procedimentos de segurança da informação da organização e as eficientes práticas de gestão da segurança.

2.3. ESTRUTURA DA ABNT NBR ISO/IEC 27002

As principais informações da norma se encontram distribuída em 11 seções, que correspondem a controles de segurança da informação que juntas totalizam 39 categorias principais de segurança. Dentro de cada seção contém um número de categorias principais de segurança da

informação.

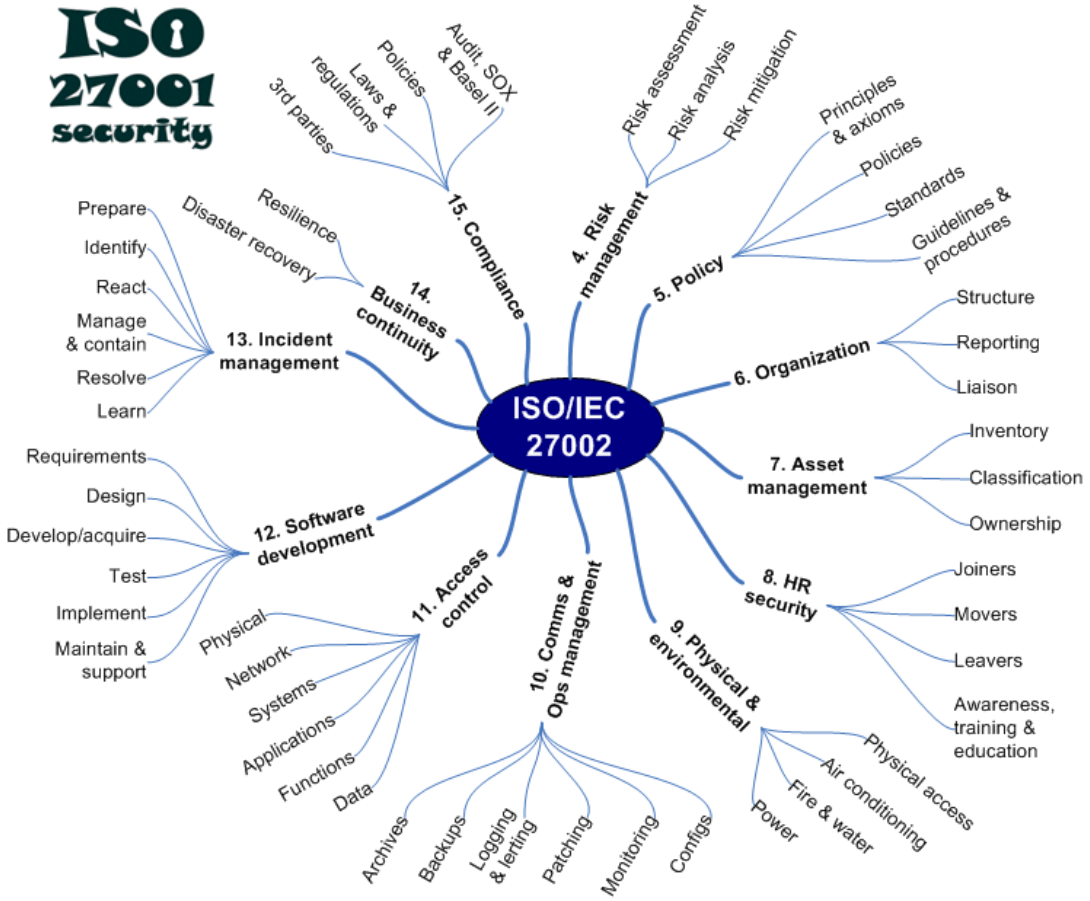

Imagem 1

Avaliação de risco e tratamento: Trata da análise/avaliação, e tratamento dos riscos, sugerindo que essas avaliações sejam realizadas periodicamente, na situação de risco e quando alguma mudança significativa ocorrer.

É necessário que um escopo definido para ser eficaz. Esse escopo pode ser tanto toda a organização quanto partes dela.

Política de segurança: A política de segurança normalmente descreve os requisitos da organização para a segurança da informação, escopo do sistema de gerenciamento de segurança da informação, incluindo as necessidades do negócio, áreas e locais cobertos.

Políticas específicas e procedimentos dentro do sistema de gerenciamento de segurança da informação devem ser consistentes com a política de segurança.

Organização da segurança da informação: A organização da segurança da informação trata de como a organização gerencia segurança da informação, as responsabilidades de cada pessoa, comitê ou fórum. Inclui responsabilidades para criar, revisar e seguir procedimentos e políticas.

Administração de ativos: É utilizada para fazer inventários de ativos físicos – por exemplo, computadores, impressoras, switches. Essas informações são vitais para uma organização, mas o valor dela depende de fatores como, por exemplo, o custo para se obter essas informações, o custo de atualização e a extensão do dano causado caso essas informações vazem para o público ou concorrente.

Segurança de recursos humanos: Este tópico cobre aspectos para reduzir o risco de erro humano e assegurar que a equipe entenda quais são seus direitos e responsabilidades em se tratando de

segurança da informação. A organização deve gerenciar bem os direitos de acessos ao sistema para quem está entrando, se mudando de área ou deixando a empresa e deve se encarregar de fazer o trabalho de conscientização sobre segurança, treinamentos e atividades educativas

Segurança física e do ambiente: Detalha qualquer aspecto físico do controle de acesso para a informação. Os seguintes aspectos devem ser considerados:

Proteção: da informação, dos sistemas de elementos e do acesso físico, o qual deve ser restrito para pessoas autorizadas. Equipamentos de TI são tentadores para ladrões e pode ser danificado por acidentes ou sabotagem.

Manutenção: dos equipamentos de suporte como ar-condicionado ou rede elétrica e do ambiente físico na sala do servidor.

Administração de operações e comunicações: Manter TI e sistemas de comunicações seguros é fundamental para a maioria das organizações e é coberto nesta seção, a maior seção da ISO 27002.

Procedimentos e responsabilidades operacionais: tem como objetivo garantir a operação segura e correta dos recursos de processamento da informação através da documentação dos procedimentos de operação, mantendo-os atualizados e disponíveis a todos os usuários e que qualquer mudança nessa documentação seja autorizada pela direção e que recursos de desenvolvimento, teste e produção sejam separados para reduzir o risco de acessos ou modificações não autorizadas aos sistemas operacionais.

Gerenciamento de serviços terceirizados: tem como objetivo, implementar e manter o nível apropriado se segurança da informação e de entrega de serviços em consonância com acordos de entrega de serviços terceirizados.

Planejamento e aceitação de sistemas: Tem como objetivo minimizar os riscos de falhas nos sistemas através de ações como a projeção de requisitos de capacidade futura para reduzir os riscos de sobrecarga dos sistemas, e estabelecimento dos requisitos operacionais dos novos sistemas, atualizações e novas versões, elaborando suas documentações e testando antes da sua aceitação de uso.

Proteção contra códigos maliciosos: Tem como objetivo proteger a integridade do software e da informação através da atualização regular dos softwares de detecção e remoção de códigos maliciosos e a execução de verificação, tanto de forma preventiva quanto rotineira.

Back-up: manter a integridade e disponibilidade da informação e dos recursos de processamento de informação. É importante a definição da política de geração de cópias de segurança e que ela reflita os requisitos de negócios da organização.

Gerenciamento da segurança em redes: Tem como objetivo garantir a proteção das informações em redes e a proteção da infraestrutura de suporte, gerenciando e controlando-as de forma a protegê-las contra ameaças. Firewall e IDS são exemplos para esta finalidade.

Manuseio de mídias: Tem como objetivo prevenir contra divulgação não autorizada, modificação, remoção ou destruição aos ativos, e interrupções das atividades do negócio. As mídias e os dados precisam ser controlados e fisicamente protegidos. O descarte das mídias também deve ser feito de forma segura e protegida quando não forem mais necessários.

Controle de acesso: Controlar o acesso à informação, recursos de processamento das informações e processos de negócios com base nos requisitos de negócio e segurança da informação. Fatores como procedimento formal de registro e cancelamento de usuário, gerenciamento de privilégios, gerenciamento de senha do usuário, revisão dos direitos dos usuários, o uso de senhas, controle de acesso à rede, segregação de rede, controle de acesso ao

sistema operacional, trabalho remoto, dentre outros, são abordados neste tópico.

Aquisição, desenvolvimento e manutenção de sistemas de informação: Tem como objetivo, garantir que segurança seja parte dos sistemas de informação, o qual inclui:

Requisitos de segurança: consiste na especificação de requisitos para controle de segurança para novos sistemas de informação ou pra melhoria dos sistemas já existentes.

Processamento correto nas aplicações: tem como objetivo prevenir a ocorrência de erros, perdas, modificação não autorizada ou mau uso de informações em aplicações

Controles criptográficos: tem como objetivo proteger a confidencialidade, autenticidade ou a integridade das informações através de métodos criptográficos.

Segurança dos arquivos do sistema: tem como objetivo garantir a segurança dos arquivos de sistema controlando o acesso aos arquivos de sistema e aos programas de código fonte.

Segurança em processo de desenvolvimento e suporte: tem como objetivo manter a segurança de sistemas, aplicativos e da informação. Convém que ambientes de projeto e de suporte sejam estritamente controlados.

Gestão de vulnerabilidades técnicas: reduzir os riscos resultantes da exploração de vulnerabilidades técnicas já conhecidas. Um inventário de ativos preciso é essencial para assegurar que vulnerabilidades potenciais sejam identificadas.

Gestão de incidentes de segurança da informação: Tem como objetivo trazer orientações para que fragilidades e eventos de segurança da informação sejam comunicados, permitindo a tomada de ação corretiva em tempo hábil. Para isso deve existir um procedimento de notificação formal para relatar esses eventos de segurança e para que haja mecanismos para quantificar esses incidentes e que essa informação seja usada para identificar incidentes recorrentes.

Gestão da continuidade de negócio: Tem como objetivo não permitir a interrupção das atividades do negócio e proteger os processos críticos contra falhas ou desastres, e assegurar sua retomada em tempo hábil. Minimizar um impacto sobre a organização.

Convêm que sejam identificados os eventos que podem causar interrupções aos processos do negócio, seus impactos e consequência para segurança da informação. Conformidade: Tem como objetivo evitar violações de quaisquer obrigações legais, regulamentares ou contratuais. Determina que os gestores garantam que todos os procedimentos de segurança a informação dentro da sua área estão sendo executados em conformidade com as políticas e normas de segurança de informação, através de análises críticas em intervalos regulares. Caso seja encontrada alguma não conformidade, convém que atitudes como a determinação da causa dessa não conformidade, uma ação corretiva, bem como ações para que ela não volte a se repetir sejam tomadas.

3. PROPOSTA

Este artigo tem como proposta a elaboração de uma pesquisa exploratória e descritiva a fim de coletar informações relativas as práticas de segurança da informação aplicadas nas empresas goianas, independente do setor de atividade ou quantidade de colaboradores e/ou tamanho do parque computacional.

Baseado na norma ABNT NBR ISO/IEC 27002, obteremos uma visão geral de como as empresas goianas lidam com a segurança da informação e medindo assim a aplicabilidade e entendimento delas.

Com a conclusão dos estudos de pesquisa, análise e resultados, esperamos fornecer um infográfico da aplicabilidade da segurança da informação nas empresas goianas com equipe de

TI interna.

3.1. SELEÇÃO DE AMOSTRA/APTIDÃO

Ficou estabelecido que para participar da pesquisa, as empresas deveriam estar localizada na grande Goiânia e possuir equipe interna de TI. Isso devido a terceirização não garantir os pilares da segurança da informação, ou seja, confidencialidade, integridade e disponibilidade.

(Compreende como grande Goiânia: Goiânia e Aparecida de Goiânia).

3.2. ESTRATÉGIAS DE COLETA

A coleta de dados da pesquisa foi realizada através de um questionário contendo 77 perguntas objetivas com apenas uma resposta válida das duas opções, sim ou não, ou seja, apenas uma seria marcada com base na aplicabilidade da norma. Para isso, foi utilizado como referência as sugestões encontradas na norma ABNT NBR ISO/IEC 27002, que estão descritas no tópico 2.2.

As empresas obtiveram acesso ao questionário mediante formulário eletrônico (Google Form) enviado via e-mail, sempre destinados ao responsável pela área de TI da empresa.

Foram entrevistadas ao todo 16 empresas do mercado goiano, sendo 1 Empresa com 1 a 9 funcionários, 6 empresas com 10 a 49 funcionários, 4 empresas com 50 a 99 funcionários, 5 empresas com mais de 99 funcionários.

Assim que finalizado o período para coleta de informações das empresas, e de posse do resultado apresentando foi possível identificar três características básicas no que tange a segurança da informação.

O questionário pode ser acessado pelos seguintes endereços URL

Short URL: http://bit.ly/HISYdL

Regular URL:
https://docs.google.com/a/cuidadodigital.com.br/spreadsheet/viewform?usp=drive_web&formkey=dFJLY3ZfOHpid1VhNVdyUzVoWFJaS0E6MQ#gid=0

3.3. ANÁLISE E RESULTADOS

Após a coleta das informações através do formulário, foi realizado o cruzamento desses dados a fim de se obter um panorama da segurança nessas empresas através da aplicabilidade da norma ABNT NBR/ISO 27002. Três tabelas foram criadas com o objetivo de facilitar a análise das informações obtidas.

Para que se possa entender as tabelas seguintes é importante lembrar que as perguntas elaboradas só possuíam como resposta ***sim*** ou ***não*** e que cada resposta sim representa um ponto e cada resposta não representa nenhum ponto.

Cruzando os dados relacionando tamanho da organização versus aplicabilidade chegamos as seguintes informações.

Na Tabela 1 é apresentado a quantidade total de pontos de cada empresa, ou seja, quantas respostas positivas foram aplicadas de cada regra da ISO, ordenadas de forma crescente por número de funcionários.

Tabela 1. Relação Empresa X Aplicabilidade por N. de Funcionários

	Nº de Funcionários	Somatório de Pontos
1	1 a 9	57
2	10 a 49	56
3	10 a 49	49
4	10 a 49	35
5	10 a 49	22
6	10 a 49	16
7	10 a 49	12
8	50 a 99	62
9	50 a 99	31
10	50 a 99	24
11	50 a 99	19
12	Maior que 100	53
13	Maior que 100	69
14	Maior que 100	53
15	Maior que 100	26
16	Maior que 100	17

Sobre os dados apresentados pode verificar que 9 empresas aplicam menos de 50% das regras consultadas no formulário. Dentre essas 9 empresas, 7 pertencem as empresas de porte médio, ou seja, de 10 a 49 funcionários e de 50 a 99 funcionários.

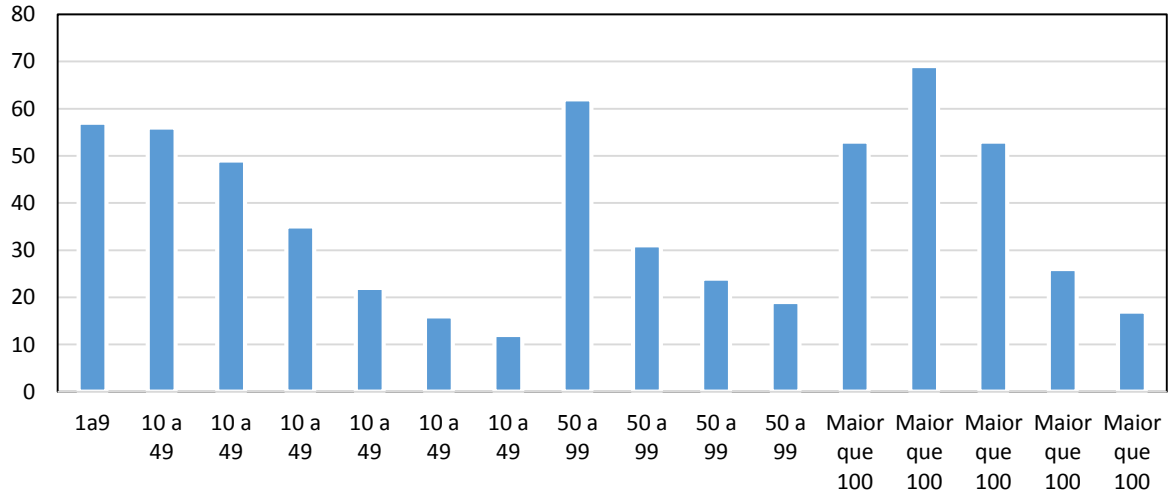

Gráfico 1. Relação Empresa X Aplicabilidade por N. de Funcionários

Na Tabela 2, em vez de apresentar o desempenho individual de cada empresa, foi apresentado o desempenho de cada grupo de empresa, grupos esses definidos pela quantidade de funcionários. Foi feito um somatório total de toda a pontuação de cada grupo e calculado assim a porcentagem de aplicabilidade das regras dentro de cada grupo. Por exemplo, a linha 1 representa o desempenho das empresas que possuem mais de 100 funcionários. Foram pesquisadas 5 empresas dessa categoria. O formulário possui 77 questões, ou seja, a pontuação máxima possível e de 77 pontos por cada empresa. Como nesse grupo há 5 empresas, a pontuação máxima seria de 385, como descrito na tabela.

Analisando a pontuação obtida pelo grupo com a pontuação máxima, foi realizado assim a média de itens da norma aplicados por aquele grupo.

Tabela 2. Desempenho por grupo de empresas

Empresas	Empresas Pesquisadas	Pontuação	Questões	Max. Pts.	Média
Maior que 100	5	218	77	385	57%
50 a 99	4	136	77	308	44%
10 a 49	6	190	77	462	41%
1 a 9	1	57	77	77	74%

Foi usado a seguinte equação para chegar o resultado médio. Média = Pontuação / Máximo de pontos * 100

Obs. Os valores da média em porcentagem foram arredondados.

Foi possível assim verificar que a menor pontuação foi obtida pelas empresas do grupo de 10 a 49 funcionários e a maior pontuação no grupo de 1 a 9 funcionários.

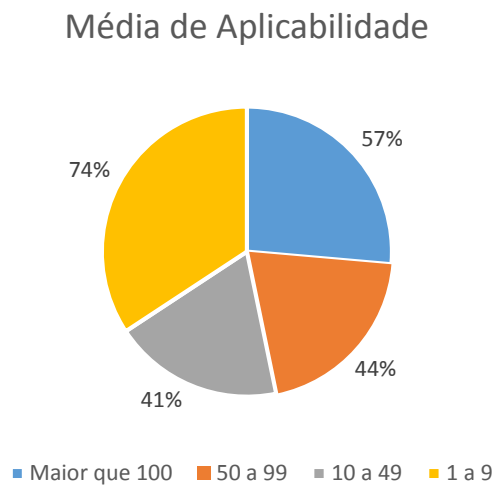

Gráfico 2. Média da aplicabilidade da norma ABNT NBR ISO/IEC 27002 por grupo de empresas

No entanto essas informações relatam somente o que cada empresa tem aplicado de maneira geral, sem ser analisado de forma mais específica regra a regra. A norma deixa bem clara que cada item informado não deve ser considerado obrigação mas apenas uma sugestão, pois tem de ser verificado as necessidades específicas de cada empresa.

Entendemos que alguns itens são considerados fundamentais para a segurança da informação e assim classificamos os tópicos como básico, intermediários e avançado considerando a facilidade da aplicação da norma, ou seja, para regras que consomem poucos recursos (humanos, financeiro e operacional), foram definidas, como básico, para regras que consomem maiores recursos foram definidas como intermediário, para as mais complexas como avançadas.

Para que possamos definir esses níveis, classificamos todas as questões com pesos que vão e 1 a 3 sendo questões de valor “1” como básico,” 2” intermediário e “3” avançado. Essa definição foi feita com base em uma análise pessoal do grupo, levando-se em conta a experiência profissional e conhecimento teórico sobre segurança da informação.

Segurança da Informação em nível Básico:

1. Identificação dos ativos
2. Inventário dos Ativos

3. Processo Disciplinar
4. Devolução de Ativos
5. Controle de Códigos Maliciosos
6. Cópias de Segurança
7. Gerenciamento de Rede Local
8. Descarte Mídias
9. Informações Publicamente Disponíveis
10. Políticas de Controle de Acesso
11. Direitos de Acesso
12. Manutenção de Equipamentos
13. Reutilização e Alienação Segura dos Equipamentos
14. Gerenciamento de Instalação e Configuração de Software

Segurança da Informação em nível Intermediário:

1. Seleção de Pessoal
2. Segregação de Redes
3. Documentação dos Sistemas
4. Limite e tempo de Sessões
5. Gerenciamento de Chaves
6. Notificações de fragilidades.
7. Registro de Logs
8. Segregação de Função
9. Tratamento de Informação
10. Contato com Autoridade
11. Manutenção das políticas
12. Perímetro de Segurança Física
13. Entrega de Serviço Terceirizado
14. Papéis e Responsabilidades
15. Responsabilidade da Direção
16. Controle de Códigos Móveis
17. Validação dos dados de entrada
18. Computação Móvel e Acesso Remoto
19. Monitoramento de uso do Sistema
20. Gerenciamento de Mídias Removíveis

21. Acordos de Confidencialidade
22. Conscientização, Educação e Treinamento.
23. Controle de acesso ao código fonte do programa.
24. Existe análise de risco dentro da organização.
25. Documentação dos Procedimentos Operacionais Padrão
26. Aceitação dos Termos de uso dos Ativos da Organização
27. Áreas de Teste, Produção e Desenvolvimento estão separadas?
28. Restrições em mudanças nos pacotes de software
29. Existe dentro da Organização Políticas de segurança da informação?
30. As ameaças que comprometem a segurança da informação estão identificadas?

Nível de segurança da informação em nível avançado.

1. Coleta de Evidências
2. Gestão de capacidade
3. Segurança do Cabeamento
4. Notificações de eventos.
5. Mecanismos de controles efetivos e funcional.
6. Identificação das consequências.
7. Política de Segurança Documentada
8. Controle, gestão e manutenção de vulnerabilidade técnica.
9. Aprendendo com incidentes
10. Analise / Avaliação dos riscos na Continuidade de Negócios
11. Desenvolvimento e implementação dos planos de continuidade.
12. Analise Crítica da Política de segurança da informação
13. Coordenação da segurança da informação
14. Aceitação de Sistemas
15. Transação On-line
16. Política Mesa Limpa, Tela Limpa.
17. Política de Acesso a Rede
18. Analise e Especificações dos Requisitos de Segurança
19. Controle do Processamento Interno
20. Validação de dados na saída.
21. Controles Criptográficos
22. Vazamento de Informações

23. Segurança da informação na Continuidade do negócio.
24. Comércio Eletrônico
25. Comprometimento da Direção com a segurança da informação
26. Identificando segurança da informação com Clientes e Terceiros
27. Rótulos e Tratamento da Informação
28. Ameaça Externa e Meio Ambiente
29. Segurança de Equipamentos fora das Dependências da Organização
30. Monitoramento e Analise Crítica
31. Gerenciamento de Mudanças para Serviços Terceirizados
32. Segurança dos Serviços de Rede Terceirizado
33. Políticas e Procedimentos para Troca de Informações

A Tabela 3 mostra esses dados a fim de verificarmos a aplicabilidade dos itens de nível básico, intermediário e avançado. Após a análise de cada item pesquisado, chegou-se ao resultado de 14 perguntas de nível básico, 30 de nível intermediário e 33 de nível avançado. Tomando como exemplo o grupo de nível avançado, são 33 perguntas no total, multiplicado pelo número de 16 empresas, chegamos ao valor máximo de 528 pontos que poderia ser obtido, dividindo a aplicabilidade "179" pelo valor máximo "528" multiplicado por "100", chegamos a aplicabilidade em porcentagem "33,90%". Cruzando esse número total possível com o número real obtido para as perguntas desta categoria, obtém-se a porcentagem de aplicabilidade dessa categoria.

Tabela 3. Aplicabilidade da norma ABNT NBR ISO/IEC 27002 de acordo aos níveis básico, intermediário e avançado.

	Básico	Intermediário	Avançado
Total de Questões	14	30	33
Total de Empresas	16	16	16
Soma total de questões	224	480	528
Aplicabilidade	163	256	179
Aplicabilidade em %	73%	53%	34%

Obs. Os valores da média em porcentagem foram arredondados.

Pode-se verificar que as questões de nível avançado são as que possuem menor aplicabilidade, o que pode ser deduzido devido a maior complexidade para implementação e demanda de maiores recursos.

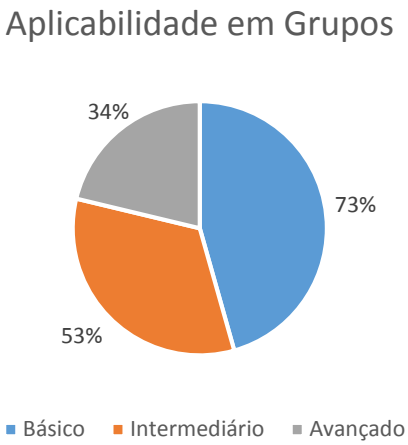

Gráfico 3. Níveis da aplicabilidade da norma ABNT NBR ISO/IEC 27002

4. Analise Modal

Analise modal tem a intenção de filtrar dentre todas as questões respondidas no formulário e em todas as empresas entrevistadas, quais das regras de S.I. são mais utilizadas e quais sofrem mais carência de uso.

Foram filtradas as regras por ordem de aplicabilidade e chegamos à conclusão que: Controle de Códigos Móveis, Cópias de Segurança e Políticas de Controle de Acesso são as regras mais aplicadas como 15 pontos cada e Analise Crítica da Política de Segurança da Informação, Rótulos e Tratamento da Informação e Política Mesa Limpa, Tela Limpa são as regras menos aplicadas com 1 ponto cada.

Em posse desses dados pode-se verificar que as regras menos aplicadas se encontram dentro da categoria de segurança avançado e das três mais aplicadas, duas estão dentro do nível básico e uma no nível intermediário, ou seja, nenhuma delas se encontra no nível avançado.

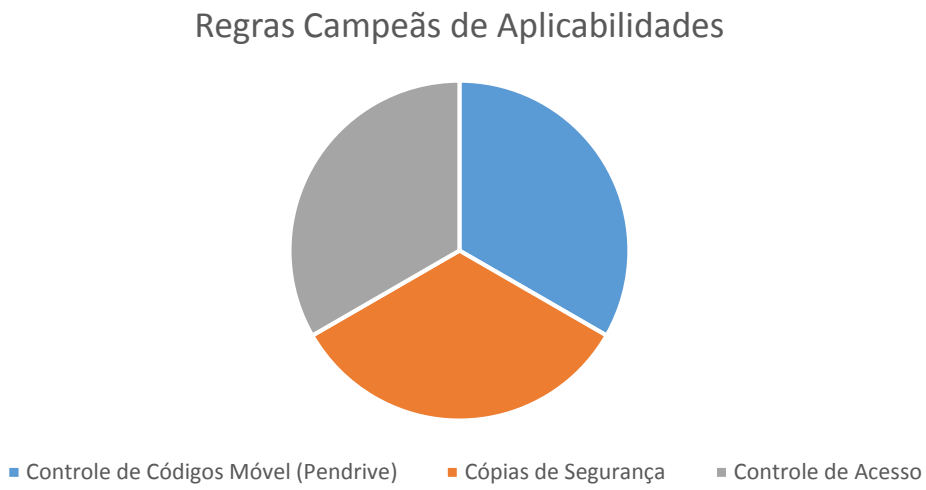

Gráfico 4. Regras mais aplicadas da norma ABNT NBR ISO/IEC 27002

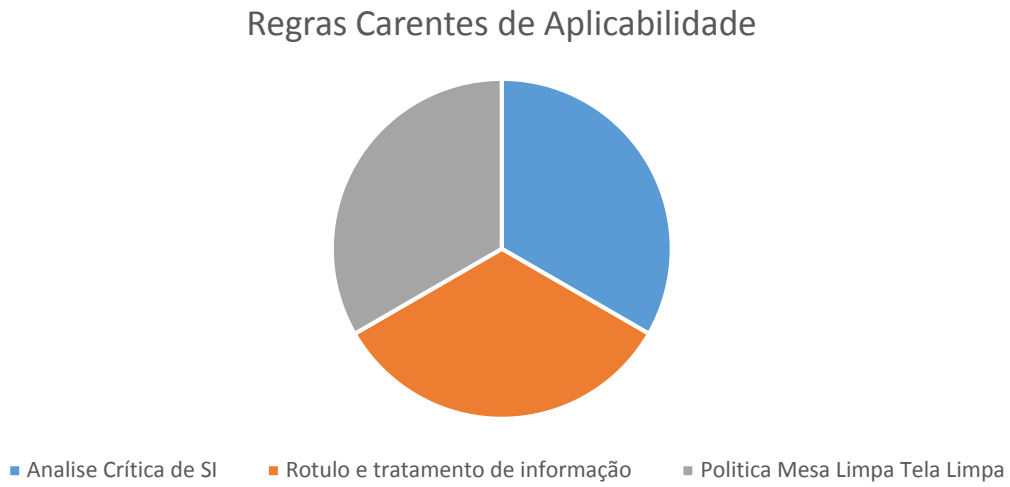

Gráfico 5. Regras menos aplicadas da norma ABNT NBR ISO/IEC 27002

5. CONCLUSÃO

Este trabalho apresentou algumas referências e diretrizes de segurança da informação, com base na norma ABNT NBR/ISO 27002.

Foram entrevistadas 16 empresas do mercado goiano, que possuem departamento ou equipes de T.I., através de um formulário eletrônico (Google Form), com um total de 77 questões abstraídas da ABNT NBR/ISO 27002, usando técnica de pesquisa descritiva e exploratória.

Após a fase de preenchimento de formulário de pesquisa, tabulamos todas as informações e pode-se verificar que as empresas que possuem entre 10 a 49 funcionários foram as que menos aplicam os itens da norma e que os itens definidos como básicos foram os mais implementados dentro das empresas enquanto os níveis definidos como avançados foram os menos aplicados.

O fato da maior porcentagem de aplicabilidade da norma ser encontrada dentro dos itens de categoria básica pode demonstrar que as empresas goianas ainda precisam avançar mais no que diz respeito a segurança da informação. O fato dos itens de níveis básicos terem obtido uma boa pontuação mostra que o estado não é crítico, mas pode avançar. Isso poderia ser obtido investindo-se mais em capacitação técnica e através da alocação de mais recursos financeiros e humanos destinados a este fim.

A análise modal também veio confirmar a informação obtida nas tabelas, de que os aspectos mais negligenciados pelas empresas no que se refere a ISO, se encontram dentro da categoria avançada.

Esperamos que os dados apresentados possam servir de referência para que os profissionais e gestores de TI continuem a seguir a linha dos itens mais aplicados da ISO, mas principalmente que possam dar mais atenção aos itens mais negligenciados a fim de que as brechas de segurança venham diminuir. Entendemos que se não houver primeiro uma conscientização dos profissionais da área sobre as ameaças e riscos existentes, não haverá uma mudança de mentalidade dos gestores das empresas, mantendo assim a resistência em liberação de recursos para essa área, como mostrou a pesquisa no início deste artigo.

Espera-se também que outros trabalhos sejam desenvolvidos visando um maior debate sobre o tema, acrescentar com a ajuda do infográfico a conscientização, esclarecimento e informação sobre a importância da segurança da informação nas organizações goianas. É interessante acrescentar ao escopo da pesquisa, empresas sem equipe de TI interna (Setor de TI Terceirizado), divisão por negócio e ramo da empresa, por tipo de empresa industrial ou

comercial e demonstrar a aplicabilidade da norma ABNT NBR ISO/IEC 27002 apresentando os itens acrescidos no infográfico.

Sendo possível também tema para trabalhos futuros, a existência de outras normas para garantir a segurança da informação, porém com objetivo idêntico que é manter a Segurança de Informação de todos os ativos da organização.

REFERENCIAS

ABNT. Tecnologia da Informação – Código de Prática para a Gestão de segurança da informação. NBR ISO/IEC 17799, 2002. ISBN 85-07-00214-5. Disponível em: <Associação Brasileira de Normas Técnicas>.

KUROSE, J. E ROSS, K. "Redes de computadores e a internet: uma abordagem top-down". Editora Addison Wesley. 3ªed., São Paulo. 2006.

COMPUTERWORLD, Disponível em: <http:/www.computerworld.com.pt/media/2011/02/Global-State-of-Information-Security-Survey-2011.pdf>. Acesso em 12 fev. 2014.

MICROSOFT, Disponível em: <http://www.microsoft.com/pt-br/download/details.aspx?id=9058>. Acesso em 12 fev. 2014.

MICROSOFT, Disponível em: <http://www.microsoft.com/en-us/news/download/presskits/antipiracy/docs/idc030513.pdf>. Acesso em 12 fev. 2014.

PLAY-IT-SAFE, Disponível em: <http://www.play-it-safe.net/>. Acesso em 12 fev. 2014.

PLAY-IT-SAFE, Disponível em: <http://play-it-safe.net/Resumo-para-clientes.pdf> Acesso em 12 fev. 2014.

BSA / IBC, Disponível em: <http://portal.bsa.org/insead/assets/studies/2013softwarevaluestudy_brazil_portuguese.pdf >. Acesso em 12 de fev. 2014.

SÊMOLA, Marcos. Gestão da segurança da informação: Uma visão executiva. Rio de Janeiro: Campus, 2003.