# Implantação de Um Sistema de Gestão de Segurança da Informação Baseado nas Normas ISO 27001, 27002 e 27005 para Pequenas Empresas

**Fernando Vieira da Silva[1], Mirkos Ortiz Martins[1]**

[1]Sistemas de Informação – Centro Universitário Franciscano
Santa Maria – RS – Brazil
nando.infocc@gmail.com, mirkos@unifra.br

***Abstract.*** *The new technologies and the Internet come help reduce costs and facilitate communication with customers and bring agility to processes that involve organizations, however opened up opportunities for the threats and attempts of virtual systems and their networks crimes. This work presents the ISO 27001, 27002 and 27005 standards, presenting a study on the implementation of the same and the main forms of vulnerabilities related to Information Technology. The objective is to implement a Management System of Information Security, with their focus on small businesses, the model will be deployed in a small business that is engaged in providing services, it needs improvements in its security requirements Information, detecting improper activities that may cause damage to the company and business continuity.*

***Resumo.*** *As novas tecnologias e a Internet vêm ajudar na redução de custos e facilitar a comunicação com os clientes e trazem agilidade aos processos que envolvem as organizações, porem abriu oportunidades para as ameaças e tentativas de crimes virtuais aos seus sistemas e redes. Este trabalho apresenta as normas ISO 27001, 27002 e 27005, apresentando um estudo sobre a implantação das mesmas e as principais formas de vulnerabilidades relacionadas à Tecnologia da Informação. O objetivo é implantar um Sistema de Gestão de Segurança da Informação, tendo seu foco voltado para pequenas empresas, o modelo será implantado em uma empresa de pequeno porte que atua no ramo de prestação de serviços, a mesma necessita de melhorias em seus requisitos de Segurança da Informação, detectando atividades indevidas que podem acarretar algum dano à empresa e a continuidade do negócio.*

## 1. Introdução

Com o surgimento de novas tecnologias e a facilidade que a mesmas dispõem, houve um aumento no número de informações processadas e trafegadas em todo o mundo. Em um ambiente caracterizado por estas mudanças a Tecnologia da Informação assume um papel fundamental para melhoria da competitividade das organizações, transformando suas informações em base para os negócios possibilitando agilidade nas tomadas de

decisões internas e externas. O sucesso empresarial depende da capacidade de perceber, organizar e administrar as informações, aproveitando as ferramentas e os recursos que a TI (Tecnologia da Informação) tem a oferecer. Consequentemente tem-se um aumento no número de vulnerabilidades que essas tecnologias têm demonstrado nesses últimos anos.

Diante dessa situação a Segurança da Informação torna-se um meio indispensável para as organizações, sejam elas do setor público ou privado, afim de garantir um nível de proteção adequado para seus ativos de informação. Neste trabalho, é apresentado o embasamento teórico para o entendimento das normas ISO 27001, 27002 e 27005, avaliação da implantação da mesma em uma organização. Além disso,são apresentados trabalhos relacionados ao assunto proposto, para base de elaboração deste trabalho.

O objetivo deste trabalho é estudar e avaliar as normas ISO 27001, 27002 e 27005 , suas principais diferenças e benefícios, assim com as principais ameaças envolvendo Segurança da Informação, o atual cenário da organização estuda e a implantação de um Sistema de Gestão de Segurança da Informação.

Desta forma, pode-se enumerar os seguintes objetivos específicos: identificar as principais ameaças e falhas da organização, implantar as normas estudadas ,definição de métricas para medição de melhorias, analisar os resultados obtidos através do modelo PDCA e comparar as diferenças entre as normas.

## 2. Referencial Teórico

Este capítulo apresenta conceitos relacionados com este trabalho, que se referem à utilização de técnicas de Segurança da Informação e algumas das principais normas utilizadas para criar ou aperfeiçoar políticas de Segurança da Informação nas organizações.

### 2.1Sistemas de informação

Inicialmente, é preciso considerar que os processos de negócios são grupos de pessoas ou atividades relacionadas que utilizam pessoas, informações e outros recursos para agregar valor interno ou externo aos clientes [AUDY e CIDERAL, 2007]. Muitos desses procedimentos são incorporados aos Sistemas de Informação, como por exemplo, cadastro de clientes, envio de mensagens eletrônicas, etc. Um sistema tem como principal objetivo armazenar, tratar e oferecer informações processadas para uma determinada situação, suas funções básicas são: **Entrada dos dados:** é a atividade de captar dados e informações; **Processamento:** refere-se às atividades de tratamento através de conversões ou transformações; **Saída:** refere-se a toda informação útil produzida pelo sistema; **Realimentação (*feedback*):** fazer ajustes nas atividades de entrada, processamento ou saída. [Furtado 2002].

## 2.2 Segurança da Informação

Segurança da Informação é entendida como a preservação das propriedades de confidencialidade, integridade, disponibilidade [ABNT, 2006].

Confidencialidade tem como objetivo dispor as informações somente a quem esta devidamente autorizado a acessá-las. É a proteção de Sistemas de Informação para impedir que pessoas não autorizadas tenham acesso ao mesmo, garantindo a identificação e autenticação das partes envolvidas [Laureano, 2005].

Integridade da informação deve ser retornada em sua forma original no momento em que foi armazenada. É a proteção dos dados ou informações contra modificações intencionais ou acidentais não autorizadas [Laureano, 2005].

Disponibilidade tem como objetivo dispor a informação para o usuário que a utiliza no momento em que a mesma for necessária [Laureano, 2005]. Quando tratamos de Segurança da Informação a mesma pode ainda ser classificada em segurança física.

### 2.2.1 Segurança Física

O controle de acesso físico tem como objetivo impedir que pessoas estranhas ou não autorizadas tenham acesso às dependências onde podem ficar os servidores de bancos de dados, servidores de e-mail, switches e demais equipamentos de Tecnologia da Informação evitando assim roubos ou vazamentos de informação. Segundo Fontes (1991), segurança física tem como principais objetivos: garantir a continuidade das rotinas, assegurar a integridade dos ativos, manter a integridade e confidencialidade das informações. Dentro da segurança física devemos destacar os seguintes aspectos como mostramos na a Tabela-1:

**Tabela 1- Ataques a meios físicos (GOODRICH, 2013)**

| | |
|---|---|
| Proteção de localização | Proteção dos locais físicos onde reside o hardware do computador. |
| Detecção de intrusão física | Detecção de acesso não autorizado ao local físico onde reside o hardware do computador. |
| Ataques ao hardware | Métodos de ataque físico como discos rígidos, adaptadores de rede, placas de memória entre outros. |
| Intromissão | Ataques que monitoram luz, som, rádio ou outros sinais para detectar comunicações. |
| Ataques físicos a interfaces | Ataques que penetram na segurança do |

| | |
|---|---|
| | sistema por meio de exploração de fragilidade a sua interface física. |

### 2.2.2 **Vulnerabilidades e Ameaças**

Vulnerabilidades são falhas em sistemas computacionais que permitem um usuário malicioso obter acesso a dados privados ou ate mesmo assumir o controle de uma máquina [GOODRICH e TAMASSIA, 2013]. Existem vulnerabilidades, que não ocorrem de uma falha ou má configuração de um sistema ou serviço e sim devido ao uso descuidado ou indevido por parte de usuários como mensagens de origem desconhecidas de correios eletrônicos, a instalação de softwares não confiáveis, acesso a sites de conteúdos duvidosos entre outros que ajuda a propagar os vírus, *spywares*, *trojan*. Facilitando assim um *hacker* a explorar tal vulnerabilidade para obter acesso não autorizado ao computador ou rede vulnerável.

## 2.3 Norma ISO 27001

A norma ISO 27001 [ABNT, 2006] é um padrão de referência internacional que surgiu da evolução da norma BS-7799-2, que foi publicada pelo BSI (*British Standard Institute*) em 1999. Ela fornece um modelo para estabelecer, implementar, operar, monitorar, analisar criticamente e melhorar um Sistema de Gestão de Segurança da Informação (SGSI), a norma adota o modelo conhecido como *Plan-Do-Check-Act* (PDCA) que é aplicada para estruturar todos os processos do SGSI. Abaixo, a Figura-1 demonstra os ciclos do PDCA.


**Figura 1- Modelo PDCA aplicado aos processos do SGSI Fonte: (ABNT ISO/IEC: 2006, p.6)**

O ciclo do PDCA é a metodologia proposta pela ISO 27001 para melhoria contínua de um SGSI, é formada por um ciclo iterativo, sua fases são sequências, mas não quer dizer que as mesmas possuem um fim, auxilia a conhecermos melhor o

ambiente da empresa podendo assim surgir a necessidade de novas mudanças no planejamento e na operação do SGSI.

**Quadro 1. Especificações dos ciclos do modelo PDCA**

| | |
|---|---|
| *Plan* (planejar) | Planejar as políticas, objetivos, processos e procedimentos do SGSI, de acordo com as características da organização. Estabelecimento de politicas, processos e procedimentos de segurança. |
| *Do* (implantar e operar o SGSI) | Implementar e operar a políticas, controles. Processos e procedimentos do SGSI. |
| *Check* (checar) | Avaliação das ações de segurança implementadas e análise dos resultados alcançados. |
| *Act* (agir) | Executar as ações corretivas e preventivas com base nos resultados da auditória interna, de modo que seja alcançada a melhoria. |

### 2.3.1 Família da norma ISO 27000

A família da série 27000 é formada por um conjunto de normas sendo elas, a norma ISO 27002, (consiste dos códigos de práticas para Gestão de Segurança da Informação), 27003 (guia de implementação de um Sistema de Gestão de Segurança da Informação), 27004 (métricas e medição para Gestão da Segurança da Informação), 27005 (diretrizes de gestão de risco da Segurança da Informação) e 27006 (diretrizes de serviços de recuperação de desastres da Segurança da Informação).

## 3.Trabalhos Correlatos

Neste capítulo, são abordados trabalhos relacionados com o escopo da presente proposta.

### 3.1 Um modelo de Sistema de Gestão da Segurança da Informação Baseado nas Normas ABNT ISO/IEC 27001:2006, 27002: 2005 E 27005: 2008

O trabalho realizado por Santos (2012) tem por objetivo propor um modelo de Sistema de Gestão da Segurança da Informação (SGSI), com mapeamento dos processos e descrição das atividades a serem realizadas, baseado nas normas ABNT NBR ISO/ EC 27001, 27002 e 27005. Sua finalidade é construir um guia prático de orientação, que

possibilite uma organização implementar ou averiguar a situação em que se encontra e a conformidade com as normas existentes . No modelo proposto, cada enfoque referente a um sistema de gestão de segurança é visto sob a perspectiva de um processo, com seus objetivos que recebem entradas, executam atividades e oferecem saídas, sendo assim o SGSI formado por um conjunto de processos inter-relacionado.

### 3.2 Um Modelo Faseado de Gestão da Segurança da Informação

O trabalho de Froio (2008), tem o objetivo de propor um modelo faseado de Gestão de Segurança da Informação, atendendo os principais objetivos do negócio, comparando com os atuais modelos ISO/ICE 17799:2005, CobiT, ITIL, SSE-CMM, ISM3 e ISO/IEC 27001:2005, identificando as principais diferenças existentes entre elas e deficiências que comprometeriam o sucesso da implementação do SGSI na organização. A implementação do modelo proposto ocorre de forma gradual dentro da organização sendo capaz de integrar os componentes que compreendem os elementos gerais da questão Segurança da Informação. A vantagem do modelo faseado é o estabelecimento de processos para seleção, implantação e revisão de melhores práticas e guias de segurança, conforme a necessidade do negócio, o seu diferencial em relação aos outros modelos é que seus processos visam manter as ações de segurança alinhados com os objetivos do negocio em qualquer nível ou fase do modelo, facilitando as organizações que não dispõem de recursos para integrar diversos modelos.

## 4. Metodologia

Este trabalho busca entender as principais funcionalidades, requisitos e resultados desejados na utilização de normas de Segurança da Informação baseados na família de normas ISO 27000. A escolha pelas normas da família 27000 possibilita gerenciar todo o ambiente coorporativo envolvendo questões como gestão de risco, implementação de controles de segurança e demais tópicos que cada uma abrange.

A partir dos conceitos discutidos nos capítulos anteriores, obteve-se embasamento para a seleção da norma, e a criação de um modelo para pequenas empresas, cada organização tem suas características e particularidades que possibilitam a criação de um modelo específico englobando as reais necessidades de cada empresa. O levantamento da atual situação da empresa é realizado por meio de análise do ambiente de TI, entrevistas e questionários com os funcionários e diretoria. A aplicação da norma é realizada em uma empresa de pequeno porte que necessita de um melhor controle de seus dispositivos e meios de comunicação que envolvem Tecnologia da Informação.

Os principais processos serão identificados pelo grau de sua relevância, atendendo as principais necessidades da organização, incluindo um levantamento dos ativos que serão envolvidos, como equipamentos, sistemas, redes, pessoas entre outros que serão documentados e constantemente avaliados, através de indicadores específicos obtém-se as condições e o desempenho do SGSI, por fim a aplicação dos processos e seus resultados serão mostrados em tabelas.

## 5. Resultados e discussões

Nesta seção serão demonstrados os resultados obtidos durante implantação e a verificação do nível de aderência do Sistema de Gestão de Segurança da Informação, através de análise de documentos, entrevistas com funcionários, diretoria e observação do ambiente computacional da organização. A verificação do nível de aderência que compõem os diversos processos das normas da família ISO 27000, foram valorados da seguinte forma:

- **Valores atribuídos ao grau de relevância:** determinar o valor que as atividades representam para a organização conforme a Tabela - 2

**Tabela 2. Grau de relevância**

| GRAU DE RELEVÂNCIA | VALOR |
|---|---|
| Nenhuma relevância | 0 |
| Baixa relevância | 1 |
| Média relevância | 2 |
| Alta relevância | 3 |

- **Valores atribuídos ao nível de implementação:** determinar o valor atribuído a cada atividade de acordo com seu nível de implementação conforme a Tabela - 3

**Tabela 3- Nível de Implementação**

| NÍVEL DE IMPLEMENTAÇÃO | VALOR |
|---|---|
| Não implementada | 0 |
| Implementação baixa | 1 |
| Implementação alta | 2 |
| Implementação total | 3 |

Para calcular o nível de aderência das atividades de cada um dos processos, estabelecemos um valor de referência (VR), que representa a situação ideal para a empresa. Assim a seguinte equação é obtida:

$$VR = GR \times 3$$

GR representa o grau de relevância das atividades e a constante 3 refere-se à valoração máxima possível, conforme a Tabela-2.

Através das pesquisas realizadas no ambiente da empresa, obtemos o valor apurado (VA), referente a cada atividade, assim a seguinte equação é obtida:

$$VA = GR \times NI$$

GR representa o grau de relevância das atividades, conforme a Tabela-2 e NI representa o nível de implementação da atividade, conforme a Tabela- 3.

Através dos resultados obtidos de VR e VA calcula-se o nível de aderência de cada processo (NAp), sendo o mesmo calculado em percentuais por meio da equação abaixo:

$$NAp = \frac{\sum VA}{\sum VR} \times 100$$

## 5.1 Levantamento estatístico

A descrição das atividades e os resultados obtidos detalhadamente estão descritos nos seguintes anexos: (A, B, C, D, E). A Tabela-4 demonstra os resultados dos níveis de aderência em percentuais dos processos que fazem parte do Sistema de Gestão de Segurança da Informação, tendo como base as normas estudadas, os valores foram obtidos através da comparação entre o somatório dos valores apurados e de referência, que compõem os processos.

**Tabela 4- Nível de Aderência por processo do SGSI**

| PROCESSO | NÍVEL DE ADERÊNCIA |
|---|---|
| Implementação, manutenção e melhoria do Sistema de Gestão de Segurança da Informação | **72,72 %** |
| Segurança física e do ambiente | **80,55%** |
| Gerenciamento das comunicações e operações | **85,71 %** |
| Controles de acesso | **92,59%** |
| Gestão de Continuidade do negócio | **50%** |

A média geral obtida do Sistema de Gestão de Segurança da Informação obtida através da média aritmética dos processos foi de 76,31% o valor demonstra o grau de conformidade do SGSI em relação ao que esta previstos nas normas da família ISO 27000. Analisando os valores de aderência de cada processo percebe-se que o processo

de Gestão de Continuidade do negócio (com 50%) e Implementação, Manutenção e Melhoria do Sistema de Gestão de Segurança da Informação (com 72,72%) estão abaixo da média geral.

### 5.2 Problemas encontrados

Devido não existir até o momento auditoria ações corretivas não foram implementadas, por se tratar de uma empresa de pequeno porte que abrange uma área aproximadamente de 60 m² a instalação de barreiras de proteção se torna inviável, a implantação de proteção das salas está em fase de conclusão,por ter sua localização em um edifício comercial, o mesmo possui pára-raios e extintores de incêndio em cada andar, diminuindo assim a possibilidade de certos tipos de acidentes naturais ou causados pelo homem, mas não os evitando totalmente.

A proteção do cabeamento de eletricidade e comunicação esta em faze de conclusão, a documentação dos procedimentos de utilização dos sistemas deve ser concluída, aquisição de softwares mais completos para monitoramento de erros de roteamento de pacotes pela rede, criar *log* de registro de utilização do sistema da empresa, assim como já existe *log* para monitoramento do sistema operacional das estações de trabalho e rede da empresa, a política de controle de acesso deve ser concluída e a política de controle de redes deve ser concluída.

### 5.3 Questionários sobre percepção da Segurança da Informação

O seguinte questionário foi realizado em um período de 15 dias, no qual 40 pessoas responderam ao total de 15 perguntas a respeito de Segurança da Informação dentro de empresas privadas e publicas de forma anônima , as perguntas em relação ao tema tratado e os gráficos com os resultados obtidos podem ser consultados no anexo (F).

## 6 Conclusão

O estudo foi de grande valia para o conhecimento sobre diversos assuntos apresentados no trabalho, que envolveram ameaças, vulnerabilidade, Segurança da Informação, normas ISO 27001,27002 e 2007 e um melhor controle da Gestão de Tecnologia da Informação dentro das organizações.

A escolha das normas ISO 27000 foi em razão das mesmas possuírem uma série de padrões relacionados entre elas, possibilitando assim a melhoria de uma política de segurança já existente ou a criação de uma nova política que se encaixe a cada tipo de negócio.Observou-se durante a pesquisa um nível de conscientização por parte de usuários e diretoria a respeito do tema tratado, devido aos últimos acontecimentos demonstrados pela mídia a respeito de Segurança da Informação , empresas e usuários estão dando uma atenção maior ao tema tratado. Como trabalhos futuros são sugeridos a aplicação do modelo em outras organizações envolvendo áreas distintas como setor de saúde, público, instituições de ensino.

## 7 Referências


ABNT - Associação brasileira de normas técnicas . NBR 27001: Tecnologia da informação – Técnicas de Segurança – Sistema de Gestão de Segurança da informação, (2008).

ABNT - Associação brasileira de normas técnicas. NBR 27002: Tecnologia da informação – Técnicas de Segurança – Código de Prática para a Gestão da Segurança da Informação, (2005).

ABNT - Associação brasileira de normas técnicas. NBR 27003: Tecnologia da informação – Técnicas de Segurança – Diretrizes para Implantação de Um Sistema de Gestão de Segurança da Informação, (2011).

ABNT - Associação brasileira de normas técnicas. NBR 27004: Tecnologia da informação – Técnicas de Segurança – Gestão da Segurança da Informação - Medição, (2010).

ABNT - Associação brasileira de normas técnicas. NBR 27005: Tecnologia da informação – Técnicas de Segurança – Gestão de Riscos de Segurança da Informação, (2008).

Abreu, Dimitri. Melhores práticas para classificar as informações http://www.modulo.com.br, Agosto

Audy, Andrade, Cidral. Fundamentos de Sistemas de Informação. Porto Alegre, RS: [Bookman, 2007].

CERT.br. Centro de Estudos,Respostas e tratamento de Incidentes de Segurança no Brasil. http://www.cert.br, Agosto.

CGI.br. Comitê Gestor da Internet no Brasil. http://www.cgi.br/, Setembro.

Fróio, Leandro Ramalho. Um modelo Faseado de Gestão da Segurança da Informação. (2008). Dissertação de Mestrado(Mestre em Engenharia Elétrica) – Universidade de Brasília, 2008. http://repositorio.unb.br/handle/10482/6687, Agosto

Furtado, Vasco . Tecnologia e Gestão da Informação na Segurança Pública. Rio de Janeiro, RJ: Editora Garamond Ltda, (2002).

Goodrich, Tamassia. Introdução à Segurança de Computadores. Porto Alegre, RS: [Bookman, 2013].

Kenneth c. Laudon. Sistemas de Informação Gerenciais 7ª edição. São Paulo, SP: [Pearson, 2007].

Laureano, Marcos AurelioPchek. Gestão de Segurança da Informação. (2005). http://www.vazzi.com.br/moodle/pluginfile.php/225/mod_resource/content/1/apostila_LAUREANO.pdf, Agosto

Morales, César Silvério. Modelo Integrado para Avaliação de Riscos da Segurança da Informação em Ambiente Corporativo. (2010). Dissertação de Mestrado(Mestre em Engenharia Elétrica) – Universidade de Brasília, (2010). http://repositorio.unb.br/handle/10482/8945, Agosto

Machado Marcel Jacques. Segurança da Informação: Uma Visão Geral Sobre as Soluções Adotadas em Ambientes Organizacionais. (2012). Monografia (Bacharel em Ciência da Computação) – Universidade Federal do Paraná, (2012). http://books.google.com.br/books?id=kRHs3cXr5h4C&printsec=frontcover&dq=seguran%C3%A7a+da+informa%C3%A7%C3%A3o&hl=pt-BR&sa=X&ei=v7xtUrmJJ4rH0QX1xYCACg&ved=0CGQQ6AEwCA#v=onepage&q=seguran%C3%A7a%20da%20informa%C3%A7%C3%A3o&f=false, Outubro.

Oliveira, Djalma de Pinho Rebouças. Sistemas de informações Gerenciais. São Paulo, SP: Atlas, (1992).

Rezende. Engenharia de Software e Sistemas de Informação. Rio de Janeiro, RJ: Brasport, (2005).

Santos, Quem mexeu no meu sistema. Rio de Janeiro, RJ: Brasport, (2008).

Santos, Valdeci Otacilio. Um modelo de Sistema de Gestão da Segurança da Informação Baseado Nas Normas ABNT NBR/ISSO/IEC 27001, 27002, 27005. (2012). Dissertação de Mestrado(Mestre em Engenharia Elétricia) – Universidade Estadual de Campinas, (2012). http://www.bibliotecadigital.unicamp.br/document/?code=000897647>,Agosto.

Silva, Rita Maria Santos, SANTOS, Daiana Luísa Rocha. Segurança da Informação: a Norma ISO/IEC 27000 e ISO/IEC 27001. 2012. Dissertação de Mestrado(Mestre em Ciência da Informação) – Universidade do Porto, (2012).http://paginas.fe.up.pt/~jmcruz/seginf/trabs-als/final/G4T9-ISO.27000.final.pdf. Setembro.

Souza. Fundamentos para Sistemas de Informação. Universidade Santa Cecília, (2012).

Ulbrich, Henrique Cesar, Valle, James Della. Universidade H4CK3R 4ª edição. São Paulo, SP: Digerati Books, (2004).

# 8. Anexos

## ANEXO A- Implementação, Manutenção e Melhoria do Sistema de Gestão de Segurança da Informação

| Implementação, manutenção e melhoria do Sistema de Gestão de Segurança da Informação | | | Controles Implantados | | | Atende aos requisitos da família 27000 | | | Grau de Relevância | Nível Implantação |
|---|---|---|---|---|---|---|---|---|---|---|
| **Item** | **Nº** | **Controle** | **Sim** | **Par** | **Não** | **Sim** | **Par** | **Não** | **Atual** | **Atual** |
| Política de Segurança | 27001 | Definir e aprovar a política do SGSI | x | | | | x | | 3 | 3 |
| | | Assegurar que as metas da SI estão identificadas e atendem os requisitos da organização. | x | | | x | | | 3 | 3 |
| | | Comprometimento da direção por meio de manifestação clara de apoio, com a SGSI. | x | | | x | | | 3 | 3 |
| | | Implementar planos e programas de conscientização e treinamento. | x | | | x | | | 3 | 3 |
| | | Conduzir auditorias internas em intervalos planejados, visando a conformidade com os objetivos da SGSI. | x | | | x | | | 3 | 2 |
| | | Executar ações corretivas e preventivas baseado nos resultados da auditoria. | | x | | | x | | 3 | 2 |
| **Legenda: Grau de relevância: 0 - nenhuma, 1 - baixa , 2- Média, 3 - Alta**<br>**Nível de Implementação: 0 - Não, 1 - baixa , 2- alta, 3 - Total** | | | | | | | | | **TOTAL IMPLANTADO: 72,72 %** | |

## ANEXO B – Segurança Física e do Ambiente

| Segurança física e do ambiente | | | Atividades implantadas | | | Atende aos requisitos da família 27000 | | | Grau de Relevância | Nível de Implantação |
|---|---|---|---|---|---|---|---|---|---|---|
| Item | Nº | Atividade | Sim | Par | Não | Sim | Par | Não | Atual | Atual |
| Áreas Seguras | 27001 | Utilizar perímetros de segurança com barreiras para proteger as áreas que contenham informações e instalações de processamento da informação | | x | | | x | | 3 | 1 |
| | | Proteger escritórios, salas e instalações | | x | | | x | | 3 | 2 |
| | | Projetar e aplicar proteção contra ameaças externas e do meio ambiente(desastres naturais ou causados pelo homem) | x | | | x | | | 3 | 2 |
| | | Implementar planos e programas de conscientização e treinamento | x | | | x | | | 3 | 3 |
| | | Conduzir auditorias internas em intervalos planejados, visando a conformidade com os objetivos da SGSI | x | | | x | | | 3 | 2 |
| | | Executar ações corretivas e preventivas baseado nos resultados da auditoria | x | | | x | | | 3 | 2 |
| Segurança de equipamentos | 27001 | Proteger os equipamentos contra ameaças e perigos do meio ambiente, bom como acesso não autorizado | | x | | x | | | 3 | 3 |
| | | Proteger os equipamentos contra falta de energia | x | | | x | | | 3 | 3 |
| | | Proteger o cabeamento de energia e telecomunicações | x | | | x | | | 3 | 2 |
| | | Manutenção dos equipamentos para assegurar sua disponibilidade e integridade permanente | x | | | x | | | 3 | 3 |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | Realizar a reutilização e alienação dos equipamentos de forma segura, examinando, quando for o caso, as mídias de armazenamento de dados antes do descarte | X | | | X | | | 3 | 3 |
| | | Assegurar que equipamentos, informações ou softwares não sejam retirados do local sem autorização prévia | X | | | X | | | 3 | 3 |
| Legenda: Grau de relevância: 0 - nenhuma, 1 - baixa , 2- Média, 3 - Alta<br>Nível de Implementação: 0 - Não, 1 - baixa , 2- alta, 3 - Total | | | | | | | | | TOTAL IMPLANTADO: 80,55% | |

# ANEXO C – Gerenciamento das Comunicações e Operações

| Gerenciamento das comunicações e operações | | | Atividades implementadas | | | Atende aos requisitos da família 27000 | | | Grau de Relevância | Nível de Implantação |
|---|---|---|---|---|---|---|---|---|---|---|
| Item | Nº | Atividades | Sim | Par | Não | Sim | Par | Não | Atual | Atual |
| Procedimentos e responsabilidades operacionais | 27001 | Documentar, atualizar e disponibilizar aos usuários os procedimentos de operação dos sistemas | | X | | | X | | 3 | 2 |
| | | Controlar as mudanças nos sistemas e nos recursos de processamento de dados | X | | | X | | | 3 | 3 |
| | | Separar os recursos de desenvolvimento , testes e produção | X | | | X | | | 3 | 3 |
| Planejamento e aceitação dos sistemas | | Estabelecer critérios para aceitação de novos sistemas realizando testes | X | | | | X | | 3 | 3 |
| Proteção contra códigos maliciosos | | Implementar controle de proteção (detecção, prevenção e recuperação) contra códigos maliciosos, bem como procedimentos de conscientização dos usuários | X | | | X | | | 3 | 3 |
| | | Política formal proibindo o uso de softwares não autorizados | X | | | X | | | 3 | 3 |
| Cópias de segurança | | Realizar e testar regularmente, cópias de segurança das informações e de softwares | X | | | X | | | 3 | 3 |
| Manuseio de mídias | | Implementar procedimentos visando o gerenciamento das mídias removíveis | X | | | X | | | 3 | 3 |
| | | Realizar descarte das mídias de forma segura e por meio de procedimentos formais | X | | | | X | | 3 | 2 |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| Gerenciamento da segurança em redes | | Redes devem ser adequadamente gerenciadas e controladas, de forma a protegê-las contra ameaças e manter a segurança de sistemas e aplicações que utilizam estas redes | X | | | X | | | 3 | 3 |
| Serviço de comércio eletrônico | | Proteger as mensagens eletrônicas em transito nas redes públicas contra fraudes, divulgação e modificações não autorizadas | X | | | X | | | 3 | 3 |
| | | Proteger informações envolvidas em transações on-line para prevenir transmissões incompletas, erros de roteamento, alterações não autorizadas das mensagens, divulgação não autorizada e duplicação | | X | | | X | | 3 | 2 |
| Monitoramento | | Monitoramento do uso do sistemas, estabelecendo procedimentos para o monitoramento do uso dos recursos de processamento da informação e os resultados das atividades de monitoramento devem ser analisados criticamente , de forma regular | | X | | | X | | 3 | 3 |
| | | Registro de log de falhas, devem ser registradas e analisadas e devem ser adotadas as ações apropriadas | X | | | | X | | 3 | 2 |
| **Legenda: Grau de relevância: 0 - nenhuma, 1 - baixa , 2- Média, 3 - Alta**<br>**Nível de Implementação: 0 - Não, 1 - baixa , 2- alta, 3 - Total** | | | | | | | | | **TOTAL IMPLANTADO:**<br>**85,71%** | |

# ANEXO D – Controles de Acesso

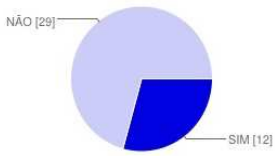
| Controles de acesso | | | Atividades implementadas | | | Atende aos requisitos da família 27000 | | | Grau de Relevância | Nível de Implantação |
|---|---|---|---|---|---|---|---|---|---|---|
| | Nº | Atividade | Sim | Par | Não | Sim | Par | Não | Máx | Atual |
| Requisitos de negócio para controle de acesso | 27001 | A política de controle de acesso deve ser estabelecida , documentada e analisada, tomando-se como base os requisitos de acesso do negócio e da segurança da informação | X | | | | X | | 3 | 2 |
| Gerenciamento de acesso do usuário | | Estabelecer procedimento de registro e cancelamento de usuários para garantir o acesso em todos os sistemas e serviços | X | | | X | | | 3 | 3 |
| | | Restringir e controlar a concessão e uso dos privilégios | X | | | X | | | 3 | 3 |
| | | Controlar a concessão de senhas | X | | | X | | | 3 | 3 |
| | | Solicitar aos usuários que sigam boas práticas de segurança da informação | X | | | X | | | 3 | 3 |
| Responsabilidades dos usuário | | Política de mesa limpa e tela limpa, para os recursos de processamento da informação | X | | | | X | | 3 | 3 |
| Controle de acesso á rede | | Política de uso dos serviços de rede, devem receber acesso somente aos serviços que tenham autorização a usar | X | | | X | | | 3 | 3 |
| | | Formular uma política relativa ao uso de redes e serviços de redes | X | | | | X | | 3 | 2 |
| | | Segregar em redes os grupos de serviços e sistemas de informação | | | | | | | | |
| Controle de acesso á aplicação e a informação | | Restringir e controlar o uso de programas e utilitários de sistema | X | | | X | | | 3 | 3 |
| **Legenda: Grau de relevância: 0 - nenhuma, 1 - baixa , 2- Média, 3 - Alta**<br>**Nível de Implementação: 0 - Não, 1 - baixa , 2- alta, 3 - Total** | | | | | | | | | **TOTAL IMPLEMENTADO:** | **92,59%** |

## ANEXO E – Gestão da Continuidade do Negócio

| Gestão da Continuidade do Negócio | | | Controles Implantados | | | Atende aos requisitos da família 27000 | | | Grau de Relevância | Nível de Implantação |
|---|---|---|---|---|---|---|---|---|---|---|
| Item | Nº | Controle | Sim | Par | Não | Sim | Par | Não | Atual | Atual |
| Aspectos da gestão da continuidade do negócio, relativos a segurança da informação | 27001 | Um processo de gestão deve ser desenvolvido e mantido para assegurar a continuidade do negócio por toda a organização e que contemple os requisitos de segurança da informação necessários para continuidade do negócio | | X | | | X | | 3 | 2 |
| | | Devem ser identificados os eventos que podem causar interrupções aos processos de negócio, junto á probabilidade e impacto de tais interrupções e as conseqüências para a segurança da informação | | X | | | X | | 3 | 2 |
| | | Desenvolver e implementar planos para manutenção ou recuperação das operações assegurando disponibilidade da informação, após a ocorrência de interrupções ou falhas | | X | | | X | | 3 | 1 |
| | | Testar e atualizar regularmente os planos de continuidade do negócio | | X | | | X | | 3 | 1 |
| Legenda: Grau de relevância: 0 - nenhuma, 1 - baixa , 2- Média, 3 - Alta<br>Nível de Implementação: 0 - Não, 1 - baixa , 2- alta, 3 - Total | | | | | | | | | TOTAL IMPLEMENTADO:<br>50% | |

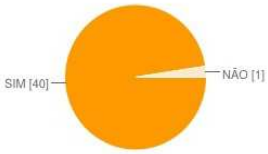
# ANEXO F – Questionário Sobre Percepção da Segurança da Informação

**1- As informações de negócio da sua empresa deveriam estar sempre disponível na web?**



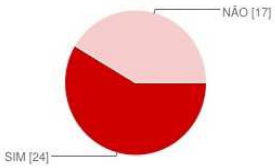

| | | |
|---|---|---|
| SIM | 12 | 29% |
| NÃO | 29 | 71% |

**2- Deveria existir treinamento e conscientização aos funcionários da empresa para a segurança das informações internas bem como utilização correta dos dispositivos de T.I?**



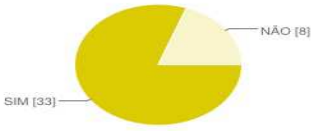

| | | |
|---|---|---|
| SIM | 40 | 98% |
| NÃO | 1 | 2% |

**3-Você acredita que a restrição ao acesso de aplicações ou páginas - por exemplo Facebook, Twitter, etc - aumentam a Segurança da Informação de sua empresa?**




| | | |
|---|---|---|
| SIM | 24 | 59% |
| NÃO | 17 | 41% |

**4- Você possuí antivírus instalado em seu computador?**




| | | |
|---|---|---|
| SIM | 33 | 80% |
| NÃO | 8 | 20% |

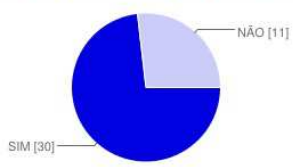
**5- Costuma atualizar seu antivírus?**


| | | |
|---|---|---|
| SIM | 28 | 72% |
| NÃO | 11 | 28% |

**6- Sabe o que é um firewall?**

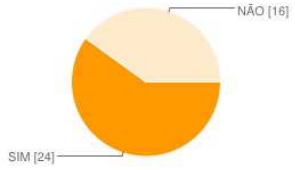

| | | |
|---|---|---|
| SIM | 33 | 80% |
| NÃO | 8 | 20% |

**7- Seu computador é protegido por senha?**



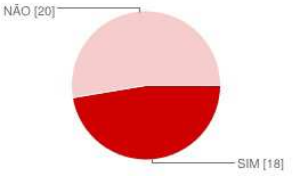

| | | |
|---|---|---|
| SIM | **30** | 73% |
| NÃO | **11** | 27% |

**8- Utiliza algum software para segurança do seu computador?**



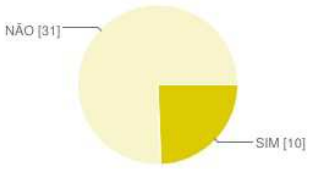

| | | |
|---|---|---|
| SIM | **24** | 60% |
| NÃO | **16** | 40% |

**9 - Você considera a Internet um modo seguro para realizar transações bancárias ou financeiras?**




| | | |
|---|---|---|
| SIM | **18** | 47% |
| NÃO | **20** | 53% |

**10- Você já foi vitima de algum incidente de segurança na Internet(perda de acesso ao mail, perda de senha, fraudes, etc)**

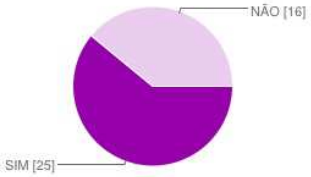



| | | |
|---|---|---|
| SIM | **10** | 24% |
| NÃO | **31** | 76% |

**11- O local em que você trabalha ou estuda possui algum sistema de segurança computacional?**

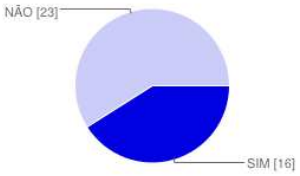

| | | |
|---|---|---|
| SIM | **28** | 68% |
| NÃO | **13** | 32% |

**12- Você realiza backup (salvar os dados) freqüentemente ?**



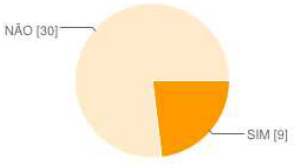

| | | |
|---|---|---|
| SIM | **25** | 61% |
| NÃO | **16** | 39% |

**13- A empresa onde você trabalha possui política de segurança da informação?**



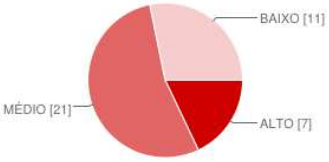

| | | |
|---|---|---|
| SIM | **16** | 41% |
| NÃO | **23** | 59% |

**14- Você costuma criar suas senhas com datas comemorativas, apelidos, número de telefone ou placa do carro?**




| | | |
|---|---|---|
| SIM | **9** | 23% |
| NÃO | **30** | 77% |

**15- Qual o nível de conscientização da diretoria de sua empresa quanto à Segurança da Informação?**




| | | |
|---|---|---|
| ALTO | **7** | 18% |
| MÉDIO | **21** | 54% |
| BAIXO | **11** | 28% |