
FACULDADE DE TECNOLOGIA SENAI DE
DESENVOLVIMENTO GERENCIAL-FATESG
CURSO SUPERIOR DE TECNOLOGIA EM REDES DE COMPUTADORES

ROGÉRIO BALTAZAR DE JESUS

# POLÍTICAS DE SEGURANÇA EM AMBIENTE HOSPITALAR

PROFESSOR-ORIENTADOR: ME. RAFAEL LEAL

Goiânia
2012

Rogério Baltazar de Jesus

# POLÍTICAS DE SEGURANÇA EM AMBIENTE HOSPITALAR

Trabalho de Conclusão de curso apresentado à Faculdade de Tecnologia Senai de Desenvolvimento Gerencial - FATESG, para obtenção do título de
Graduado em Tecnologia em Redes de Computadores**.**
Professor-Orientador: ME. **Rafael Leal**

Goiânia
2012

## AGRADECIMENTOS

Agradeço a DEUS por ter me fortalecido durante essa caminhada, afinal Ele é o grande responsável por essa obra. A minha amada esposa Elcilene M. B. Baltazar por ter me dado força no momento que mais precisei. Aos meus amados pais Adauto e Eva, aos meus queridos irmãos Ricardo e Leidiane que sempre me apoiaram, a meus avós "Zizi" e "Dona fia" por terem me ensinado grande parte do que a vida não ensinou. Aos meus amigos de sempre que não citarei nomes para não cometer a injustiça de esquecer alguém. Amo todos por tudo e sempre.

Às vezes, a vida bate com um tijolo na sua cabeça. Não perca a fé. Estou convencido de que a única coisa que me permitiu seguir adiante foi o meu amor pelo que fazia. Você tem que descobrir o que você ama. Isso é verdadeiro tanto para o seu trabalho quanto para com as pessoas que você ama.

Seu trabalho vai preencher uma parte grande da sua vida, e a única maneira de ficar realmente satisfeito é fazer o que você acredita ser um ótimo trabalho. E a única maneira de fazer um excelente trabalho é amar o que você faz.

Steve Jobs

## LISTA DE ILUSTRAÇÕES

**FIGURA 1 -** Planilha de *Check List* **.....** Erro! Indicador não definido.
**FIGURA 2** – IP Monitor**.....** Erro! Indicador não definido.

## LISTA DE ABREVIATURAS SIGLAS E SÍMBOLOS

CLT - Consolidação das Leis do Trabalho

ING - Instituto de Neurologia de Goiânia

PSI - Políticas de Segurança da Informação

TI- Tecnologia da informação

## RESUMO

Este trabalho visa abordar um estudo sobre políticas de Segurança da Informação para o Instituto de Neurologia de Goiânia, haja vista que o requisito segurança esta se tornando cada vez mais essencial na gerencia de qualquer departamento de tecnologia da informação. Existem vários modelos de padronização para políticas de segurança, como exemplo podemos citar ITIL, COBIT e as normas ABNT NBR ISO IEC 17799, ABNT NBR ISO IEC 27001, entre outras. Na elaboração deste trabalho foi referenciada a norma ABNT NBR ISO IEC 17799 – 2005 que trata da segurança da informação de uma forma mais generalizada. As diretrizes aqui descritas deverão ser atualizadas constantemente, mantendo-se assim sempre atuais.



**Palavras-chave**: Política de Segurança da Informação. normas ABNT NBR ISO IEC 17799, ABNT NBR ISO IEC 27001.

## ABSTRACT

This work aims to address a study on information security policy for the Institute of Neurology in Goiânia, given that the security requirement is becoming increasingly essential in the management of any department of information technology. There are several models of standardization to security policies, we can cite as an example ITIL, COBIT and ISO standards IEC 17799, ISO IEC 27001, among others.
In preparing this work has been referenced to standard ISO IEC 17799 - 2005 which deals with information security more generally. The guideline described will be updated constantly, thus remaining ever present.



**Key words**: Information Security Policy. ISO standards IEC 17799, ISO IEC 27001

**SUMÁRIO**

**1. INTRODUÇÃO ..... 10**
1.1 OBJETIVO GERAL ..... **10**
1.2 OBJETIVOS ESPECÍFICOS ..... **12**
1.3 SEGURANÇA DA INFORMAÇÃO ..... **1**Erro! Indicador não definido.
1.4 POLITICAS DE SEGURANÇA DA INFORMAÇÃO ..... **Erro! Indicador não definido.**
1.5 O QUE SÃO POLITICAS DE SEGURANÇA? ..... **Erro! Indicador não definido.**
**2. O INSTITUTO DE NEUROLOGIA DE GOIANIA - ING.** Erro! Indicador não definido.
**3. ELABORACÃO DE UMA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO**Erro! Indicador não
3.1. PRINCÍPIOS DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO ..... 15
3.2 REQUISITOS DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO ..... 16
**4. DAS RESPONSABILIDADES DE CADA COLABORADOR ..... 18**
4.1 DAS COLABORADORES TERCEIRIZADOS ..... **Erro! Indicador não definido.**
4.2 QUANTO AS RESPONSABILIDADES DOS GERENTES DE DEPARTAMENTOS ..... **Erro! Indicador não definido.**
4.3 DO DEPARTAMENTO DE TECNOLOGIA DA INFORMAÇÃO**Erro! Indicador não definido.**9
4.4 A BOA PRATICA DO CORREIO ELETRONICO (email)**Erro! Indicador não definido.**9
**5. DAS DISPOSIÇÕES FINAIS ..... 22**
**CONCLUSÃO ..... 23**
**REFERENCIAS BIBLIOGRAFICAS ..... 24**
**ANEXOS .....** Erro! Indicador não definido.

# 1. INTRODUÇÃO

As facilidades que envolvem o setor de tecnologia da informação promoveram significativamente o grau de dependência que as empresas possuem com a informação, por isso pré-definir políticas e mecanismos de segurança para proteger e preservar essas informações são cada dia mais necessários independente do setor de atuação dos negócios.

O setor de segurança hospitalar tem se tornado um dos mais importantes na organização administrativa de qualquer estabelecimento de saúde do Brasil. Essas instituições devem manter os dados dos pacientes o mais seguro e protegido possível. Com o emprego de novas tecnologias da informação nas organizações de saúde, o termo segurança passou a ter um papel fundamental nas políticas de segurança.

A privacidade das informações do paciente depende da manutenção da confidencialidade, integridade controle ao acesso, trilhas de auditoria das informações armazenadas e a disponibilidade do sistema empregado para esse controle. Partindo da premissa básica de que as informações do paciente devem ser resguardadas de qualquer forma de manipulação não autorizada, devemos elaborar políticas de segurança para o Instituto de Neurologia de Goiânia (ING), tendo como objetivo aplicar políticas e mecanismos de segurança em todo o hospital e também nas empresas terceirizadas que fazem parte da estrutura organizacional do Instituto de Neurologia de Goiânia.

Para elaboração desta política de segurança foi realizado um estudo de campo, no qual se verificou a inexistência de qualquer tipo de normas ou procedimentos de segurança por escrito que possa ser consultado em caso de necessidade.

## 1.1 OBJETIVO GERAL

O objetivo geral deste trabalho é desenvolver uma proposta conceitual de processos estruturados para implementação e manutenção da segurança da informação em ambiente hospitalar utilizando como base a norma ABNT NBR ISO IEC 17799 – 2005.

## 1.2 OBJETIVOS ESPECÍFICOS

Consiste em elaborar uma política de segurança que se adapte às necessidades e seja um referencial para a busca de soluções dos sistemas informáticos do ING através da norma ABNT NBR ISO IEC 17799 – 2005.

## 1.3 SEGURANÇA DA INFORMAÇÃO

Segurança da informação pode ser entendida como o processo de proteger informações das ameaças para a sua integridade, disponibilidade e confidencialidade, segundo BEAL (2005, p.1).

Desta forma, o princípio fundamental da segurança da informação está no controle de acesso os recursos críticos que requerem a proteção contra modificação e revelação não autorizada, aponta DEY (2007).

A segurança da informação visa assim preservar ativos da informação considerando três objetivos fundamentais:

- **Confidencialidade:** A informação está disponível apenas para usuários autorizados;
- **Integridade:** A informação deve estar disponível sempre que necessários para todos que tem autorização para manipulá-la;
- **Disponibilidade:** A informação deve ser confiável e completa, devendo ser protegida contra modificações não autorizadas.

A segurança da informação não envolve somente as questões técnicas, mas também questões gerenciais e humanas que fazem parte deste conceito, já que a tecnologia por si mesma não garante a integridade da segurança da informação; é necessário treinar e conscientizar os colaboradores de uma forma geral sobre a importância da segurança da informação através de políticas de segurança.

## 1.4 POLÍTICAS SEGURANÇA DA INFORMAÇÃO

A elaboração de uma Política de Segurança da Informação (PSI) é um passo importantíssimo no estabelecimento de um sistema de gestão da segurança da informação eficiente e que conduza a um tratamento eficiente da informação. O propósito da elaboração da política de segurança é estabelecer diretrizes e regras que serão seguidas por todos os colaboradores do ING.

A PSI é composta por um conjunto de normas e padrões que determina o que terá de ser realizado para garantir que as regras de confidencialidade, disponibilidade e integridade sejam cumpridas para proteger a informação. Segundo a descrição do item 0.1 da norma ABNT NBR ISSO IEC 17799 que trata da segurança da informação: Segurança da informação é a proteção da informação de vários tipos de ameaça para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio.

## 1.5 O QUE SÃO POLÍTICAS DE SEGURANÇA?

Uma PSI descreve a filosofia e as regras básicas para o uso dos recursos da informação independente do ambiente em que a mesma será empregada. Com a elaboração da mesma todos os setores da organização devem cumprir determinadas regras para o tratamento da informação.

Uma PSI bem elaborada deve-se alinhar aos objetivos da organização e fazer uma análise dos riscos que os recursos de segurança da organização suportam. Sem uma PSI, a organização fica a deriva no mar de problemas que diariamente as organizações enfrentam ao lidar com dados de clientes ou, no nosso caso, pacientes. São informações complexas como: dados pessoais, informações financeiras e principalmente informações realtivos ao estado geral de saúde do paciente.

# 2 O INSTITUTO DE NEUROLOGIA DE GOIÂNIA – ING

Em 1960 criava-se, em Goiânia, a Faculdade de Medicina e, a seguir, a Universidade Federal de Goiás. Ambas foram o marco inicial de uma nova fase de desenvolvimento das Ciências Médicas no Estado. Lá se formaram médicos que foram verdadeiros pioneiros e que tiveram pela frente o desafio de estruturar novos serviços e especialidades médicas. Em março de 1968, quatro médicos, Orlando Martins Arruda - o primeiro neurocirurgião de Goiânia -, Roberto Arão Gomes, Ruy Ignácio Carneiro e Sebastião Eurico de Melo Souza, numa atitude de vanguarda, criaram a Clínica Neurológica de Goiânia no centro da cidade.

> "As internações e intervenções neurocirúrgicas eram efetuadas na Santa Casa de Misericórdia e no Hospital do Câncer de Goiânia, únicos hospitais da capital que comportavam realização de d i a g nó s t i c o e tratamento neurocirúrgico", recorda Ruy Carneiro. "Podemos afirmar que esses dois hospitais foram um marco importante em nossas vidas profissionais". Mais tarde o grupo passou a atender no Hospital São Francisco de Assis. "Era um hospital privado, muito bem montado, com serviço de radiologia, microscópio cirúrgico e CTI, onde realizávamos todas as cirurgias neurológicas de grande porte", conta o médico.

Tempos depois, ao grupo inicial de fundadores da Clínica Neurológica juntaram-se também: Abdo Badim, Henrique Veiga Lobo, Valter da Costa e o professor da Faculdade de Medicina de Goiás, Paulo Afonso do Egipto Guimarães. Em agosto de 1971, estes oito profissionais criaram o Instituto de Neurologia de Goiânia, que passou a funcionar no Hospital São Francisco de Assis. "Nosso sonho não parou por ali. Passamos a idealizar um hospital próprio para neurocirurgia, localizado em local estratégico, mais ou menos no centro geográfico a capital, onde grandes avenidas se cruzassem", continua Ruy Carneiro. "O ideal foi colocado em prática, e, durante o processo de construção, num local ainda inóspito - mas que era ponto de convergência das entradas da cidade -, muito sacrifício foi feito, mas o sonho superava os obstáculos", avalia o médico.

Durante a construção, um dos médicos pioneiros do projeto – Roberto Arão – deixou a equipe e, em maio de 1975, o grupo passou a contar com a colaboração do médico Luiz Fernando Martins. No dia 29 de novembro de 1975, um convite histórico circulou em Goiânia. Nele, os idealizadores do projeto do Instituto de Neurologia de

Goiânia tinham a elevada honra de convidar a sociedade local para o coquetel de inauguração do hospital. Era a concretização do sonho.

Com o passar dos anos o ING cresceu, os médicos saíram para fazer cursos no exterior e modernas tecnologias de ponta foram adquiridas. “Nossa criança cresceu e se expandiu. Hoje, não é mais um hospital que guarda apenas sua identidade de Neurociências. Tornou-se uma unidade de saúde que abriga várias especialidades médicas. É o único hospital privado no Brasil, autorizado pelo Ministério da Saúde a fazer cirurgias de epilepsia e também pioneiro na cirurgia funcional”, observa Ruy Carneiro, com o orgulho de quem acompanhou tudo desde o princípio.

Atualmente o ING ocupa uma área correspondente a dez lotes e está próximo a alcançar o número de 100 leitos, feito que será possível após a finalização das reformas - já em fase de conclusão. “É motivo de orgulho sentir que o sonho de alguns pioneiros se transformou numa instituição voltada aos estudos médicos e ao bem estar da sociedade”, comemora o membro do grupo idealizador do ING, Ruy Carneiro.

# 3 ELABORACÃO DE UMA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

A PSI é o documento que orienta e estabelece as diretrizes corporativas do Instituto de Neurologia de Goiânia visando à proteção dos ativos de segurança da informação contra riscos e ameaças sejam elas internas ou externas. A adoção da PSI visa garantir a integridade da informação que está sendo manipulada de diversas formas; por meio de arquivos eletrônicos, mensagens eletrônicas (*e-mails*), bancos de dados, meios impressos, em mídias de áudios e vídeos, verbalmente, etc. Por isso, esta PSI deve ser cumprida e aplicada em todos os setores do ING.

Para elaboração desta PSI, vamos seguir os três aspectos básicos de segurança aqui já citados que são: confidencialidade, integridade e disponibilidade.

Para garantir a integridade dos três itens referenciados, a informação deve ser gerenciada e protegida contra roubos, fraudes, perdas não intencionais, acidentes, espionagens e qualquer outro tipo de ameaça que possa comprometer a informação.

Essa PSI devera ser utilizada por todos os departamentos do ING, inclusive pelos colaboradores e empresas terceirizadas que fazem uso da infraestrutura de informática do ING.

## 3.1 PRINCÍPIOS DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Qualquer tipo de informação produzida, recebida ou confiada aos colaboradores do ING como resultado de qualquer atividade profissional exercida ou contratada pertence à referida instituição. Qualquer exceção deve ser formalizada entre as partes envolvidas com aprovação da mesa diretora.

Os equipamentos de informática, comunicação, sistema de gerenciamento hospitalar, sejam eles pertencentes ou não ao ING que são utilizados pelos colaboradores contratos ou terceirizados, devem ser utilizados para realização das atividades profissionais. O uso pessoal dos recursos é permitido deste que não prejudique o desempenho das atividades dos sistemas e dos serviços.

O ING, por meio da gerência dos sistemas informáticos, poderá registrar, guardar e monitorar todo o uso dos sistemas, computadores e registros do uso da internet, visando garantir a disponibilidade e a segurança da informação.

Os profissionais terceirizados ou contratados, que fazem uso das instalações físicas e lógicas do hospital, deverão seguir essas mesmas políticas de segurança da informação. O uso de tablets, notebooks, smartphones ou qualquer outro dispositivo móvel deverão ser previamente aprovados pelo departamento de Tecnologia da Informação do hospital.

Devem-se considerar os dispositivos a serem protegidos, os recursos de *hardware* e *software*, utilizados na administração e geração da informação pertencente ou não ao ING, sejam eles alugados ou licenciados ao mesmo.

## 3.2 REQUISÍTOS DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

A fim de garantir a transparência da informação, a PSI deverá ser comunicada a todos os colaboradores do ING, fazendo-se assim cumprir todos os parâmetros por ela definido.

Tanto esta PSI quanto as normas por ela estabelecidas deverão ser revisadas e atualizadas periodicamente, sempre que as necessidades do ING motivem esta revisão. Deverá conter em todos os contratos do ING uma cópia assinada pelos colaboradores e prestadores de serviços do hospital, a fim de resguardar que todos tem ciência da PSI, sendo esta uma condição imprescindível para ter acesso aos ativos de informação disponibilizados pelo hospital. As responsabilidades relativas à segurança da informação devem ser comunicadas no ato da contratação do colaborador.

Qualquer incidente relativo à segurança da informação deverá ser comunicado imediatamente ao departamento de Tecnologia da Informação (TI) do ING. Os colaboradores deverão buscar orientação do superior hierárquico em caso de dúvidas relacionadas à PSI.

O acesso aos servidores de arquivos, firewall, Proxy ou qualquer outro tipo de ativo de segurança da informação está autorizado somente para os responsáveis pelo departamento de TI, qualquer outra exceção deverá ser informada e acompanhada pelo responsável pelo departamento de TI.

O não cumprimento dos requisitos previstos nesta PSI e nas normas de segurança da informação ocasionará na violação às regras internas do ING e consequentemente o usuário estará sujeito às medidas administrativas e legais cabíveis.

O Instituto de Neurologia de Goiânia exonera-se de toda e qualquer responsabilidade decorrente do uso indevido, negligente ou imprudente dos recursos e informações causados pelos seus colaboradores. O ING reserva-se no direito de auditar, analisar e investigar as evidências a fim de obter quaisquer tipos de provas que serão utilizadas no processo investigatório e adotar as medidas cabíveis.

# 4 DAS RESPONSABILIDADES DE CADA COLABORADOR

Entende-se por colaborador toda e qualquer pessoa física contratada em regime de Consolidação das Leis do Trabalho (CLT) ou prestador de serviços vinculados ao ING por meio de contrato de prestação de serviços seja por meio de pessoa jurídica ou não, que exerça alguma atividade dentro ou fora do hospital.

Será de responsabilidade do colaborador qualquer prejuízo ou dano que vir a sofrer ou causar ao ING e/ou terceiros em virtude da não obediência às diretrizes da PSI.

O colaborador que causar qualquer tipo de prejuízo ao ING e/ou a terceiros terá que arcar com as devidas responsabilidades sejam elas materiais e/ou financeiras.

## 4.1 DOS COLABORADORES TERCEIRIZADOS

Devem seguir e cumprir as mesmas diretrizes que os colaboradores em regimes de CLT, estes estão sujeitos às mesmas regras, normas e sanções estabelecidas na PSI.

## 4.2 QUANTO AS RESPONSABILIDADES DOS GERENTES DE DEPARTAMENTOS.

Os gerentes de todos os departamentos do ING deverão ter uma postura exemplar em relação à segurança da informação, servindo como modelo de conduta aos demais colaboradores que estão sob sua gestão.

Devem ser informadas aos colaboradores em fase de contratação e formalização de contratos de prestação de serviços ou parcerias, as diretrizes e as responsabilidades quanto ao cumprimento da PSI desenvolvida para o ING deverá ser exigido a assinatura no termo de compromisso e ciência, assumindo o dever de seguir as normas estabelecidas, manter sigilos sobre as informações e privilégios aos quais possui acessos.

## 4.3 DO DEPARTAMENTO DE TECNOLOGIA DA INFORMAÇÃO

Entende-se como obrigações do departamento de Tecnologia da Informação:

- Configurar os equipamentos, ferramentas e sistemas disponíveis aos colaboradores com todos os ativos necessários para cumprir os requerimentos de segurança estabelecido por essa PSI. Os administradores e operadores do sistema de gestão hospitalar deverão ter acesso aos arquivos e dados de outros usuários;
- Criar, configurar e manter trilhas para auditoria suficientemente detalhada para detectar possíveis falhas e fraudes;
- Administrar, proteger e testar cópias de seguranças dos programas e dados utilizados no ambiente do hospital, além de monitorar a capacidade de armazenamento, processamento e transmissão dos dados e dos sistemas;
- Atribuir as contas e dispositivos de acessos aos computadores, sistemas ou base de dados através de *logins* (usuários), de forma individual, sendo que os *logins* (usuários) são de responsabilidades dos seus respectivos "logados";
- Desenvolver políticas de proteção dos ativos de informação do hospital contra códigos maliciosos, trojans, *worms*, vírus e todas as formas de ameaças virtuais que possam comprometer as atividades do hospital.

## 4.4 A BOA PRÁTICA DO CORREIO ELETRÔNICO (*e-mail*)

O uso do correio eletrônico (*e-mail*) do ING é para fins corporativos e relacionados às atividades do colaborador dentro da instituição. A utilização desse serviço para fins pessoais é permitida desde que feita com bom senso, não prejudique o ING e também não cause transtornos ao tráfego da rede.

Vamos listar o que é proibido aos colaboradores no uso do correio eletrônico do ING:

- Enviar qualquer mensagem por meios eletrônicos que torne seu remetente e/ou o ING vulneráveis a ações civis ou criminais;

- Divulgar informações não autorizadas ou imagens de tela, sistemas, documentos e afins sem autorização expressa e formal concedida pelo proprietário desse ativo de informação;
- Apagar mensagens pertinentes de correio eletrônico quando qualquer quando o ING estiver investigando a algum tipo de dano,
- Produzir, transmitir ou divulgar mensagem que contenha ameaças eletrônicas, como: spam, *mail bombing*, vírus de computador, que contenha arquivos com código executável (.exe, .com, .bat, .pif, .js, .vbs, .hta, .src, .cpl, .reg, .dll, .inf) ou qualquer outra extensão que represente um risco à segurança;
- Possibilite obter acesso não autorizado a outro computador, servidor ou rede;
- Possibilite interromper um serviço, servidores ou rede de computadores por meio de qualquer método não autorizado;
- Possibilite burlar qualquer sistema de segurança;
- Instalar qualquer *software* para vigiar secretamente ou assediar outro usuário tais como keyloggers, entre outros;
- Acessar informações confidenciais sem prévia autorização do responsável pela mesma;
- Acessar qualquer tipo de informações que gere prejuízos de qualquer natureza a qualquer pessoa;
- Contenha conteúdo considerado impróprio, obsceno ou ilegal;
- Promova, acesse, crie ou distribua qualquer informação de caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico entre outros;
- Promova perseguição preconceituosa baseada em sexo, raça, incapacidade física ou mental ou outras situações que possa denegrir a honra ou conduta de qualque colaborador do ING;
- Promover, distribuir ou criar conteudo de fins políticos locais ou do país (propaganda política);
- Promover, distribuir ou criar conteudo de fins religiosos, independente de qualquer credo religioso;

- Promover ou distribuir material protegido por direitos autorais sem a permissão do detentor dos direitos.

As mensagens de correio eletrônico sempre deverão incluir assinatura com o seguinte formato:

- Nome do colaborador;
- Departamento ao qual pertence;
- Nome da empresa;
- Telefone(s);
- Correio eletrônico.

## 5 DAS DISPOSIÇÕES FINAIS

Esta PSI visa gerenciar, monotorar e minimizar possíveis falhas na segurança da informação do Instituto de Neurologia de Goiânia, portanto contamos com o compromisso de todos os profissionais, funcionários e parceiros do ING no cumprimento desta política.

# CONCLUSÃO

Fica evidenciado que cada dia mais as empresas buscam maior autonomia no requisito segurança da informação. Podemos analisar que cada vez mais as dependências dos ambientes computadorizados tornam-se mais vulneráveis a ameaças e possíveis às falhas, sejam elas virtuais ou humanas.

Esta política visou definir normas, procedimentos e definir responsabilidades a serem seguidas pelos usuários e colaboradores de forma geral do ING.

Durante o processo de desenvolvimento desta política, ficou evidenciado que a Política de Segurança da Informação é a base para todas as questões relacionadas à proteção da informação. Para a elaboração desta PSI foi utilizado à norma ABNT NBR ISO IEC 17799 – 2005. Esta norma trata de vários aspectos relativos à segurança da informação. O resultado final está sendo implementado junto ao Departamento de Tecnologia da Informação do Instituto de Neurologia de Goiânia com o objetivo de melhorar e garantir a preservar as informações seja dos pacientes, colaboradores ou ambientes administrativos do ING.

Como proposta de trabalhos futuros, poderão ser desenvolvidos trabalhos de divulgação, implementação e por que não ampliação desta PSI.

## REFERÊNCIAS BIBLIOGRÁFICAS

ABNT – Associação Brasileira de Normas Técnicas. **NBR ISO/IEC 17799 de 2005**: Tecnologia da informação — Técnicas de segurança — Código de prática para a gestão da segurança da informação, 2005.

FERREIRA, Fernando Nicolau Freitas, ARAÚJO, Márcio Tadeu de, **Políticas de Segurança da Informação – Guia Prático para Elaboração e Implementação.** 02 Ed. Revisada. Rio de Janeiro: Ciência Moderna, 2008.

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

NAKAMURA, Emilio Tissato, GEUS Paulo Lício de, **Segurança de redes em ambientes cooperativos .** 01. ed.. São Paulo: Novatec, 2007.

Instituto de Neurologia de Goiânia: www.neurologico.com.br%2Fneurologico2009%2Frevista_pdf%2Fneuroacao2_jul09.pdf. Acessado em... www.neurologico.com.br/neurologico2009/inst_historico.html

SESC São Paulo: www.sp.senac.br%2Fnormasadministrativas%2Fpsi_normas_administrativas.pdf. Acessado em...

## ANEXOS

Foi gerado o documento em PDF como documento padrão