INSTITUTO FEDERAL
PARANÁ

MINISTÉRIO DA EDUCAÇÃO

GOVERNO FEDERAL
BRASIL
PAÍS RICO É PAÍS SEM POBREZA

PORTARIA N.º 791 DE 16 DE DEZEMBRO DE 2011.

O Reitor do Instituto Federal do Paraná, no uso da competência que lhe confere o Decreto de 13 de junho de 2011, da Presidência da República, publicado no Diário Oficial da União do dia 14 de junho de 2011, seção 2;

RESOLVE:

I. Instituir a Política de Segurança da Informação do Instituto Federal do Paraná – IFPR.

II. Esta portaria entra em vigor na data de sua publicação, revogando-se as disposições em contrário.

IRINEU MARIO COLOMBO

Política de Segurança da Informação

Autor	Comitê Gestor da Segurança da Informação - CGSI do IFPR
Dono	Comitê Gestor da Segurança da Informação - CGSI do IFPR
Organização	IFPR
Versão	1.0
Data	30/11/2011
Classificação do Documento	Documento Aberto

Sumário

1. Controle do Documento

1.1. Armazenamento do Documento

Título do Documento	Política de Segurança da Informação
Localização do Documento	http://reitoria.ifpr.edu.br/cgsi/politica.pdf
Formato do Documento	PDF

1.2. Histórico de Versão

Versão	Data	Sumário de Mudanças
0.9	18/11/2011	Primeira versão
1.0	30/11/2011	Segunda versão

1.3. Aprovações

Nome	Cargo	Data da Aprovação	Versão Aprovada
Irineu Mário Colombo	Reitor		1.0
Eduardo Liquio Takao	Presidente do CGSI		1.0

2. Visão Geral

A informação é um ativo que a organização tem o dever e a responsabilidade de proteger. A disponibilidade da informação de forma completa e precisa é essencial para que a organização forneça de forma eficiente serviços.

Segundo a norma NBR ISO 27002 a informação pode existir em diversas formas, sendo submetida constantemente a diversas situações de compartilhamento, sendo recomendado que ela seja sempre protegida adequadamente.

Para a segurança da informação, realizar a proteção adequada da informação consistem em garantir a Confidencialidade, Integridade e Disponibilidade.

A proposta desta Política de Segurança da Informação (PSI) é estabelecer as diretrizes para a proteção dos ativos de informação do IFPR. Estas diretrizes devem ter como objetivos:

- Proteger as informações do IFPR de ameaças, internas ou externas, deliberadas ou acidentais.
- Permitir o compartilhamento das informações de forma segura.
- Assegurar que esteja claro para todas as pessoas do IFPR (servidores, discentes, terceirizados, empresas contratadas) seus papéis na utilização e proteção da informação.
- Garantir a continuidade e minimizar possíveis danos ao negócio.
- Proteger o IFPR de responsabilidades legais do uso inadequado das informações.

A Política de Segurança da Informação é um documento que contem diretrizes gerais de segurança e controles para proteção da informação. Tais controles são entregues, descritos e padronizados pelos processos e procedimentos de segurança da informação apoiados por ferramentas e treinamentos.

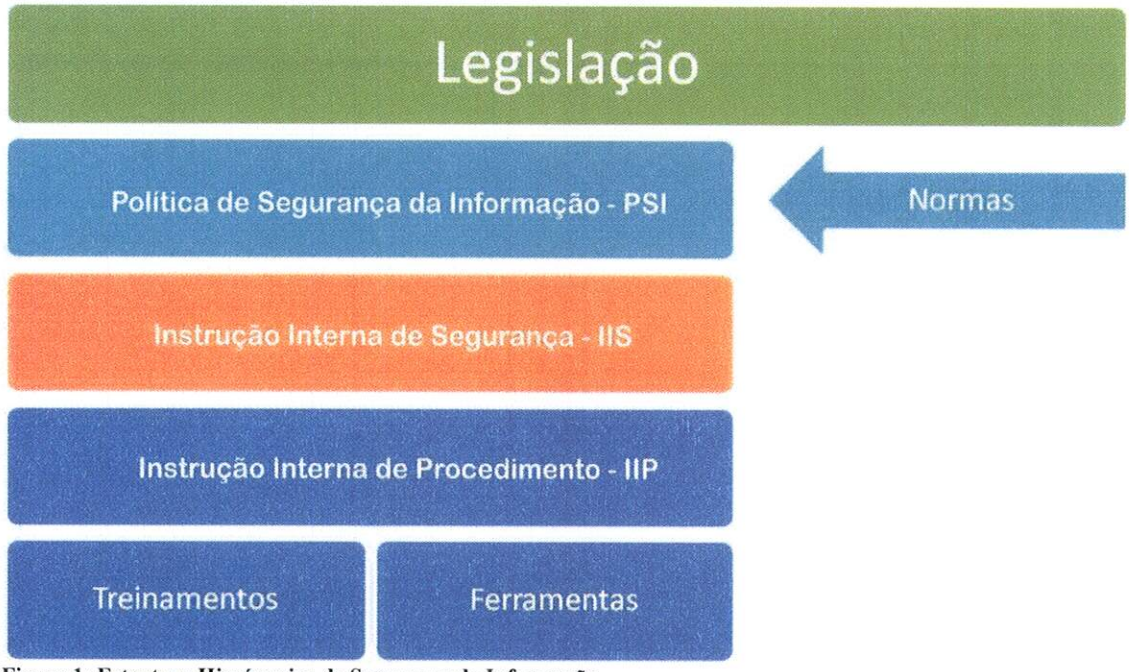

Figura 1: Estrutura Hierárquica de Segurança da Informação

A PSI define os conceitos de segurança da informação devendo respeitar a legislação vigente. Ela não contêm técnicas e orientações tecnológicas, apenas diretrizes do que deve-se proteger.

As normas são recomendações e boas práticas que auxiliam na implantação de políticas de segurança da informação. As tecnologias e técnicas para a segurança da informação são definidas nas Instruções Internas de Segurança (IIS), sendo atualizadas sempre que necessário.

As IIP implementam os processos descritos nas IIS, podendo existir mais de uma IIP para uma IIS.

Os treinamentos e as ferramentas são mecanismos para que as IIP sejam de fato implementados.

3. Do Escopo

As PSI, IIS e IIP se aplicam a todos os colaboradores, empresas terceiras ou agentes que possuem acesso as informações do IFPR.

A PSI se aplica a todas as formas de informação, incluindo:

- Discursos, reuniões, comunicados por telefone ou qualquer outro sistema de comunicação.
- Dados impressos, manuscritos ou armazenados digitalmente.
- Comunicações por correios, correios eletrônicos, fax, mensagens de texto.
- Processadas por computadores ou dispositivos eletrônicos quaisquer.
- Armazenados em quaisquer tipo de mídias (papel, CD, DVD, Pendrive, câmeras digitais, etc).

4. Estrutura da Política de Segurança

Esta PSI é baseada na norma ISO 27002 e define de formas gerais as diretrizes da política de segurança da informação da organização. Como apoio a esta política existem IIS e IIP que definem como as informações serão gerenciadas, acessadas e destruídas.

A PSI é única, acompanhada de IIS e IIP. A PSI define as diretrizes gerais, as IIS especificam cada um dos casos e as IIP definem a forma de aplicação das IIS.

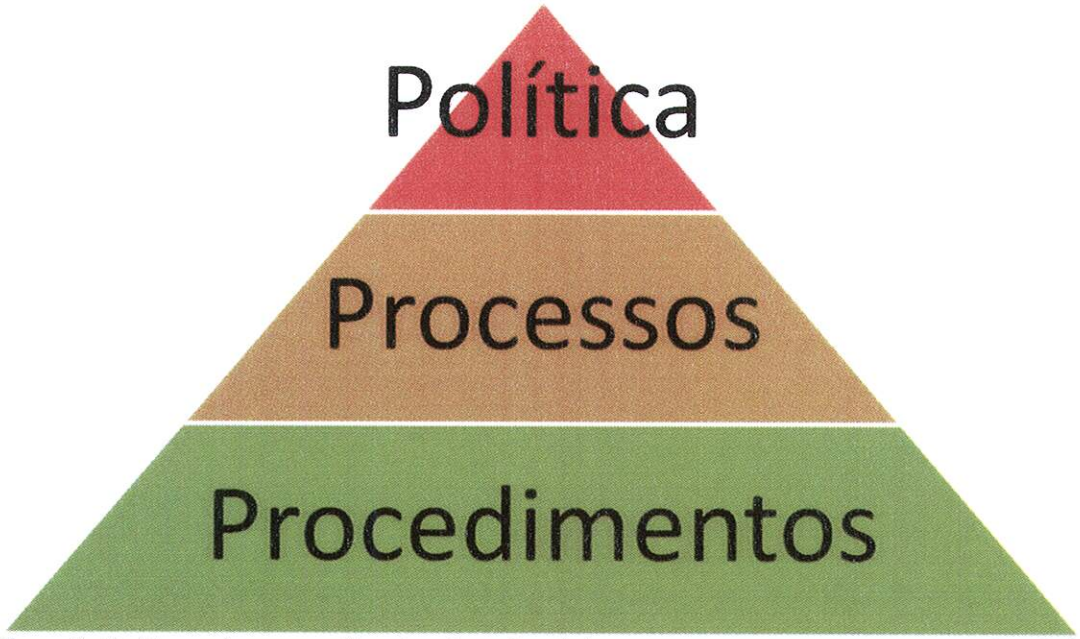

Figura 2: Na hierarquia os procedimentos não podem ferir os processos que por sua vez não podem ferir a política de segurança.

5. Riscos

Os dados e informações institucionais que são coletados, analisados, armazenados, comunicados e relatados podem estar sujeitos a roubos, perdas, mau uso ou corrupção.

Os mesmos dados podem ser postos em risco devido a má informação, educação e treinamentos deficientes, maus uso e quebras de controle de segurança.

Os incidentes de segurança da informação podem dar origem a constrangimentos, perdas financeiras, descumprimentos de normas ou legislações, implicações legais e danos a imagem do IFPR.

O IFPR deve realizar avaliações de risco para identificar, quantificar e priorizar riscos com base na ABNT ISO/IEC 27005.

6. Politica de Segurança da Informação

6.1. Documento de Segurança da Informação

As informações do documento de segurança da informação definem as diretrizes e abordagem da gestão da segurança da informação.

O documento deve ser aprovado pela gestão e divulgado a todos colaboradores, empresas terceiras e prestadores de serviço da instituição.

6.2. Revisão

A PSI deve ser revista anualmente para que seja feita a adequação da política à realidade institucional.
Solicitações formais de alteração da política serão realizadas no período de revisão.

7. Organização da Segurança da Informação

7.1. Declaração de Intenções da Gestão

A política da organização garante que informações serão protegidas caso haja perda de:

- Confidencialidade: para que as informações sejam acessíveis apenas aos indivíduos autorizados.
- Integridade: Salvaguarda da exatidão e integridade das informações.
- Disponibilidade: Os usuários autorizados tenham acesso a informação quando necessitarem.

A gestão deve comprometer-se com a política de segurança e suas diretrizes.

O Comitê Gestor da Segurança da Informação (CGSI) deve acompanhar as IIS e IIP de segurança para garantir a aplicação da segurança da informação de acordo com as orientações da PSI. Cabe ao comitê revisar, propor alterações e modificar a PSI.

Toda legislação, regulamentação e requisitos contratuais serão incorporados na política de segurança da informação, nas IIS e IIP.

O IFPR irá trabalhar para implementar as boas práticas da família de normas ABNT ISO/IEC 27000.

Todas as violações de segurança, reais ou não, devem ser relatadas e investigadas. Orientações serão dadas sobre o que constitui um incidente de segurança da informação.

Planos de continuidade de negócio serão produzidos, mantidos e testados.

As informações armazenadas pela organização deverão ser adequadas para as necessidades da instituição.

7.2. Coordenação da Segurança da Informação

A gestão da segurança da informação será realizada por meio do CGSI, sendo este responsável por atribuir funções aos membros com o objetivo de implementar esta política de segurança, e identificar os responsáveis pelos processos e procedimentos de segurança da informação.

Quando houver necessidade, consultoria externa será utilizada para que a política continue de acordo com os interesses da instituição.

7.3. Responsabilidades da Segurança da Informação

O CGSI é o dono da política de segurança da informação, respondendo por mantê-la, revisar e acompanhar a criação dos IIS e IIP.

O Reitor, Pró-reitores, Chefe de Gabinete e Diretores são responsáveis pelo comprometimento de suas equipes, sejam servidores, contratados ou empresas terceirizadas. Devem incentivar o cumprimento da política de segurança da informação, IIS e IIP.

A Auditoria Interna irá examinar a adequação dos controles que são implementados para proteger a informação e farão recomendações de melhorias.

Todos os funcionários, terceirizados e empresas contratadas que acessem as informações do IFPR deverão aceitar a política de segurança, processos e procedimentos de segurança.

O não cumprimento das politicas de segurança, IIS e IIP implicarão em medidas corretivas ou disciplinares.

8. Gestão de Ativos

Os ativos devem ser devidamente protegidos, contabilizados e possuírem um dono.

Os proprietários dos ativos serão identificados para todos os ativos e responsabilizados pela proteção dos mesmos.

9. Segurança dos Recursos Humanos

Todas as políticas, processos, procedimentos serão divulgados a todos os funcionários, contratados e empresas contratadas para que eles compreendam suas responsabilidades.

As responsabilidades de segurança da informação serão incluídas em contratos, descrições de trabalho, e em termos e condições de emprego.

Deverão ser realizadas verificações em todas as novas contratações e contratos para observância dos processos e procedimentos.

10. Segurança Física do Ambiente

As informações relevantes deverão ser armazenadas em ambientes seguros bem como os ambientes onde elas serão processadas deverão respeitar normas e padrões de qualidade de armazenamento.

As áreas de segurança deverão ser protegidas por perímetros de segurança definidos com barreiras e controles apropriados.

As informações relevantes ao IFPR armazenadas em sistemas de informação também deverão estar protegidas fisicamente de acesso não autorizado, danos e interferências.

11. Comunicação e Gestão de Operações

O IFPR irá operar suas instalações de processamento de informação de forma segura. Esta segurança deverá ser feita respeitando as IIS e IIP.

As responsabilidades do gerenciamento, operação, disponibilidade e plano de contingência de todos os dados e instalações de processamento da informação serão estabelecidas em IIS e IIP.

Procedimentos operacionais serão colocados em prática e auditados para garantir:

- Que realmente estão sendo seguidas as definições da segurança da informação, IIS e IIP.
- Verificar possíveis falhas nos procedimentos existentes.
- Certificar que os procedimentos estão mitigando riscos.

Para a redução de riscos de negligência ou erro deliberado no uso da informação poderão ser definidos níveis de acesso, uso e divulgação da informação.

12. Controle de Acesso

O acesso as informações e aos sistemas de informação serão controladas e obedecerão às necessidades da instituição. O acesso será concedido aos funcionários, parceiros e contratados de acordo com as necessidades para exercer a função e respeitarão a legislação referente a publicidade dos atos administrativos e transparência pública.

O controle de acesso a todos os serviços e informação poderá ser realizado por meio de cadastro e descadastro formal.

13. Aquisição, Desenvolvimento e Manutenção de Sistemas da Informação Computacional

Os requisitos de segurança da informação serão definidos durante o levantamento de requisitos do negócio para os novos sistemas de informação ou mudanças em sistemas já existentes.

Os controles para mitigar riscos identificados após implementação deverão ser implementados em momento oportuno.

14. Gerenciamento de Incidentes de Segurança da Informação

Um incidente de segurança da informação é uma ação ou omissão que pode ter impacto na segurança da informação, no negócio ou nos ativos da instituição. Uma vulnerabilidade é qualquer característica que pode causar impacto na segurança da informação, no negócio ou nos ativos da instituição.

Os incidentes de segurança da informação e vulnerabilidades associadas aos sistemas de informação devem ser informados em tempo hábil através de mecanismo formal de comunicação de incidentes. Uma ação corretiva apropriada deve ser tomada e poderá ser divulgada.

Todos funcionários, terceirizados e empresas contratadas devem estar cientes dos procedimentos para comunicar diferentes tipos de incidentes de segurança ou vulnerabilidade que podem ter impacto na segurança ou nos ativos da instituição.

15. Gerenciamento de Continuidade do Negócio

O IFPR deve implantar dispositivos para proteger os processos críticos do negócio dos efeitos de falhas ou desastres e assegurar sua retomada em tempo hábil.

Os processos de gerenciamento da continuidade do negócio devem ser implementados para minimizar o impacto no IFPR e para recuperação de perdas da informação e ativos. Os processos críticos para a instituição deverão ser identificados e classificados.

A análise de impacto no negócio será realizada para avaliar as consequências de desastres, falhas de segurança, perda ou indisponibilidade do serviço.

16. Treinamentos e Softwares

Os colaboradores e empresas terceirizadas devem ser treinados nos procedimentos de segurança e nos softwares de segurança quando necessário.

Na aquisição de softwares para segurança deverão ser exigidas garantias de confidencialidade, integridade e disponibilidade do software.

17. Penalidades

A não observância dos preceitos desta Política poderá implicar na aplicação de sanções administrativas, cíveis e penais previstas na legislação em vigor que regule ou venha regular a matéria.

As penalidades administrativas serão aplicadas após a devida apuração em processo administrativo disciplinar, sendo observados critérios de gravidade e reincidência dos atos de violação cometidos à Política de Segurança da Informação.

As violações às normas que compõem essa Política de Segurança da Informação deverão ser analisadas pelo gestor imediato do infrator, que deverá comunicar imediatamente a Diretoria da DTIC para fins de determinação da apuração das eventuais responsabilidades dos funcionários envolvidos.

18. Disposições Finais

As exigências regulamentares, legislativas e contratuais deverão ser incorporadas na política de segurança, IIS e IIP.

O desenho, operação, uso e gerenciamento dos sistemas de informação deverão cumprir todas as definições legais, os requisitos de segurança regulamentares e contratuais.

19. Definições

- **Ativo** – qualquer coisa que tenha valor para a organização (ISO/IEC 13335-1:2004)
- **Confidencialidade** – propriedade que limita o acesso a informação tão somente às entidades legítimas, ou seja, àquelas autorizadas pelo proprietário da informação. (ISO-17799)
- **Integridade** – propriedade que garante que a informação manipulada mantenha todas as características originais estabelecidas pelo proprietário da informação, incluindo controle de mudanças e garantia do seu ciclo de vida (nascimento, manutenção e destruição). (ISO-17799)
- **Disponibilidade** - propriedade que garante que a informação esteja sempre disponível para o uso legítimo, ou seja, por aqueles usuários autorizados pelo proprietário da informação. (ISO-17799)

EDUARDO LIQUIO TAKAO
PRESIDENTE DO CGSI

Prof. Dr. Eduardo Liquio Takao
INSTITUTO FEDERAL DO PARANÁ
Diretor de TI e Comunicação
Matrícula SIAPE 1850866

IRINEU MÁRIO COLOMBO
REITOR

Prof. Irineu Mario Colombo
INSTITUTO FEDERAL DO PARANÁ
Reitor
Matrícula SIAPE 393241