Política de Segurança da Informação e Comunicações (POSIC)
da Universidade Federal de Pelotas (UFPel)

Capítulo I
ASPECTOS GERAIS

Art. 1 - A UFPel, por meio desta política, reconhece que um ambiente seguro para a informação é fundamental ao sucesso e continuidade das suas atividades acadêmicas e administrativas. Dessa forma, se compromete a garantir os meios necessários para a proteção da informação sob sua guarda, demonstrando assim a sua responsabilidade institucional.

Capítulo II
CONCEITOS E DEFINIÇÕES

Art. 2 - Entende-se por conceitos, definições e termos utilizados nesta política:

I - Agente Público: todo aquele que exerce, ainda que transitoriamente ou sem remuneração, por eleição, nomeação, designação, contratação ou qualquer forma de investidura ou vínculo, mandato, cargo, emprego ou função pública na UFPel;

II - Ativo de Informação: qualquer componente (humano, tecnológico, físico ou lógico) que sustenta um ou mais processos de negócio de uma unidade ou área, incluindo a própria informação;

III - Comitê de Segurança da Informação e Comunicações: grupo de pessoas com a responsabilidade de assessorar a implementação das ações de segurança da informação e comunicações na UFPel;

IV - Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR): grupo de pessoas com a responsabilidade de receber, analisar e responder a notificações e atividades relacionadas a incidentes de segurança em computadores;

V - Gestor de Segurança da Informação e Comunicações: responsável pelas ações de segurança da informação e comunicações na UFPel;

VI - Incidente de Segurança: é um evento de segurança ou um conjunto deles, confirmado ou sob suspeita de impactar a Disponibilidade, Confidencialidade, Integridade ou Autenticidade de um ativo de informação, assim como qualquer violação da Política de Segurança da Informação e Comunicações (POSIC);

VII - Política de Segurança da Informação e Comunicações (POSIC): documento aprovado pelo Comitê de Segurança da Informação e Comunicações, com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da segurança da informação e comunicações.

Capítulo III
PROPÓSITO

Art. 3 - Esta Política de Segurança da Informação e Comunicações (POSIC) visa estabelecer diretrizes estratégicas, responsabilidades e competências objetivando viabilizar e assegurar a Disponibilidade, Integridade, Confidencialidade e Autenticidade (DICA) das informações da UFPel ou sob sua responsabilidade, incluindo as informações de propriedade de seus usuários, quando no uso dos recursos da UFPel, contra ameaças, vulnerabilidades e falhas, inclusive as humanas, de modo a preservar os seus ativos de informação, como também sua imagem institucional.

Capítulo IV
CAMPO DE APLICAÇÃO

Art. 4 - Esta política se aplica a todos os agentes públicos, discentes e terceiros, incluindo mas não limitado aos docentes, técnicos administrativos, consultores, prestadores de serviços, estagiários, e a qualquer indivíduo ou instituição que esteja autorizado a acessar ativos de informação e/ou dados, produzidos ou custodiados pela UFPel.

Capítulo V
PRINCÍPIOS

Art. 5 - O compromisso da UFPel com o tratamento adequado de suas informações, assim como as de seus usuários, estão fundamentados nos seguintes princípios:

I - Disponibilidade: propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade;

II - Integridade: propriedade de que a informação não seja modificada ou destruída de maneira não autorizada ou acidental;

III - Confidencialidade: propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizado e credenciado;

IV - Autenticidade: propriedade que consiste na segurança de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade, ou seja, relaciona-se com a confirmação de autoria, a certificação e a originalidade da informação.

Capítulo VI
DIRETRIZES GERAIS

Art. 6 - Toda informação produzida ou recebida pelos agentes públicos, discentes e terceiros, em resultado da função exercida e/ou atividade profissional contratada, pertence à UFPel.

Art. 7 - Ao longo de seu ciclo de vida, toda a informação acessada, processada, transmitida e gerenciada pela UFPel deve ser protegida de maneira adequada contra acesso, modificação, destruição ou divulgação não autorizada.

Art. 8 - As informações da UFPel devem ser tratadas de forma ética e sigilosa e de acordo com as leis vigentes e normas internas, evitando seu mau uso e exposição indevida.

Art. 9 - Os ativos de informação da universidade devem ser utilizados apenas para as finalidades aprovadas pela Instituição.

Art. 10 - O uso dos ativos de informação da UFPel deve ser realizado considerando a ética e o bom senso, respeitando as leis vigentes, assim como políticas, normas e procedimentos internos.

Art. 11 - Os responsáveis por sistemas, ativos ou informações devem garantir que os mesmos estejam adequadamente protegidos.

Art. 12 - Deverão ser criados e instituídos controles apropriados, trilhas de auditoria ou registros de atividades em todos os pontos e sistemas em que a Instituição julgar necessário.

Art. 13 - Todo o acesso a redes, computadores e sistemas da UFPel deve ser feito por meio de *login* de acesso único, pessoal e intransferível.

Art. 14 - Cada usuário é responsável pela segurança das informações dentro da UFPel, principalmente daquelas que estão sob sua responsabilidade.

Art. 15 - Diretrizes específicas e procedimentos próprios sobre temas como Tratamento da Informação, Tratamento de Incidentes, Gestão de Risco, Gestão de Continuidade, Controles de Acesso, entre outros, deverão ser fixados em normas complementares.

Capítulo VII
RESPONSABILIDADES

Art. 16 - Compete aos agentes públicos, discentes e terceiros:

I - cumprir a POSIC, assim como as normas e os procedimentos da UFPel aplicáveis de acordo com suas atividades;

II - manter-se atualizado em relação à POSIC e as normas e procedimentos relacionados;

III - buscar informação junto ao Gestor de Segurança da Informação e Comunicações da UFPel sempre que não estiver absolutamente seguro quanto ao tratamento de informações;

IV - reportar todo e qualquer incidente de segurança a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR) da UFPel.

Art. 17 - Compete ao Comitê de Segurança da Informação e Comunicações (em conformidade com o disposto no artigo 6º da 03/IN01/DSIC/GSIPR):

I - assessorar na implementação das ações de segurança da informação e comunicações;

II - constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre segurança da informação e comunicações;

III - propor projetos, normas e procedimentos internos relativos à segurança da informação e comunicações, em conformidade com as legislações existentes sobre o tema;

IV - apoiar a Política de Segurança da Informação e Comunicações (POSIC);

V - garantir a revisão periódica desta política e de suas normas e procedimentos relacionados;

VI - analisar os incidentes de segurança quando solicitado pela Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR), especialmente aqueles que resultarem na violação desta Política de Segurança da Informação e Comunicações (POSIC) e das normas e procedimentos relacionados;

VII - determinar a elaboração de relatórios, levantamentos e análises que dêem suporte à gestão de segurança da informação e à tomada de decisão;

VIII - acompanhar o andamento dos principais projetos e iniciativas relacionados à segurança da informação.

Art. 18 - Compete ao Gestor de Segurança da Informação e Comunicações (em conformidade com o disposto no artigo 7º da 03/IN01/DSIC/GSIPR):

I - promover cultura de segurança da informação e comunicações por meio de atividades de conscientização, capacitação e especialização;

II - divulgar esta política assim como suas normas e procedimentos relacionados;

III - acompanhar as investigações e as avaliações dos danos decorrentes de incidentes de segurança;

IV - propor recursos (financeiros, humanos e tecnológicos) necessários às ações de segurança da informação e comunicações;

V - coordenar o Comitê de Segurança da Informação e Comunicações e a ETIR;

VI - realizar e acompanhar estudos de novas tecnologias, quanto a possíveis impactos na segurança da informação e comunicações;

VII - manter contato permanente e estreito com o Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da Republica para o trato de assuntos relativos à segurança da informação e comunicações;

VIII - propor projetos, normas e procedimentos relativos à segurança da informação e comunicações;

IX - participar do desenvolvimento e da análise crítica periódica da Política de Segurança da Informação e Comunicações, bem como das normas e procedimentos ou quando mudanças significativas ocorrerem.

Art. 19 - Compete à ETIR:

I - atuar em grupo de trabalho instituído pelo Comitê de Segurança da Informação e Comunicações, quando um incidente envolver ativos de informação, juntamente com representantes da área afetada.

II - receber, registrar, analisar, investigar, classificar e responder às notificações e atividades relacionadas a incidentes de segurança, além de armazenar registros para formação de séries históricas como subsídio estatístico.

III - implantar em parceria com a unidade gestora de Tecnologia da Informação mecanismos de detecção e prevenção de intrusão, e análise de vulnerabilidades.

IV - estabelecer um plano de gerenciamento de incidentes que consistir de um plano de ações claramente definido e documentado, para ser usado quando ocorrer um incidente de segurança.

V - reportar ao Comitê de Segurança da Informação e Comunicações os incidentes considerados relevantes e as providências tomadas, podendo propor medidas de prevenção a futuros incidentes.

Art. 20 - Compete à unidade gestora de Tecnologia da Informação (Pró-Reitoria de Gestão da Informação e Comunicação):

I - evitar que sejam inseridos novos riscos no ambiente de tecnologia da UFPel;

II - implementar e avaliar a eficácia dos controles de segurança da informação nas tecnologias utilizadas na UFPel, seguindo, sempre que possível, guias de boas práticas em segurança da informação;

III - informar ao Gestor de Segurança da Informação e Comunicações e demais interessados os riscos residuais resultantes da avaliação que trata o inciso I do art. 20;

IV - definir metodologia e realizar auditorias e análises de vulnerabilidades periódicas do ambiente de tecnologia da UFPel;

V - monitorar o ambiente de tecnologia, gerando indicadores e históricos de uso:

a) da capacidade instalada da rede e dos equipamentos;

b) tempo de resposta no acesso à Internet e aos sistemas críticos;

c) períodos de indisponibilidade no acesso à Internet e aos sistemas críticos;

d) atividades de todos os usuários durante os acessos às redes externas, inclusive Internet.

VI - tomar as ações cabíveis em seu âmbito de atuação quando da identificação de incidentes de segurança.

VII - sugerir à Administração Superior o Gestor de Segurança da Informação e Comunicações;

VIII - sugerir à Administração Superior, ouvido o Comitê de Segurança da Informação e Comunicações, a composição da Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR).

Art. 21 - Compete à Procuradoria Federal junto à UFPel e à unidade gestora de administração (Pró-Reitoria Administrativa):

I - incluir na análise e na elaboração de contratos, sempre que necessário, cláusulas específicas relacionadas à segurança da informação, com o objetivo de proteger os interesses da UFPel.

Art. 22 - Compete à unidade de gestão de pessoas (Pró-Reitoria de Gestão de Pessoas):

I - apresentar a Política de Segurança da Informação e Comunicações, junto às normas consideradas de conhecimento geral pertinentes ao cargo ocupado;

II - obter a assinatura de um Termo de Compromisso Individual no momento da admissão de novos servidores e demais usuários (professores visitantes e de trabalho voluntário, estagiários, entre outros);

III - instituir programas permanentes e regulares de conscientização e capacitação em segurança da informação;

IV - manter o repositório de usuários ativos, o qual reflete o quadro funcional, atualizado e demais cadastros de sua responsabilidade.

Art. 23 - Compete às unidades finalísticas (Pró-Reitoria de Ensino, Pró-Reitoria de Extensão, e Pró-Reitoria da Pesquisa, Pós-Graduação e Inovação:

I - apresentar aos discentes a Política de Segurança da Informação e Comunicações, junto as normas consideradas de conhecimento geral;

II - obter a assinatura de um Termo de Compromisso Individual no momento do ingresso de novos discentes e demais usuários (pós-doc, visitantes de curto período, bolsistas não vinculados à UFPel, entre outros);

III - manter atualizado o repositório de usuários ativos, no que diz respeito às atualizações no cadastro de discentes da UFPel (ingresso, trancamento ou cancelamento de matrícula, conclusão ou desligamento da Instituição, sejam temporários ou definitivos) e demais cadastros de sua responsabilidade.

Art. 24 - Compete à unidade gestora de administração (Pró-Reitoria Administrativa):

I - apresentar a Política de Segurança da Informação e Comunicações às empresas contratadas junto as normas consideradas relevantes de acordo com os produtos e/ou serviços contratados;

II - obter a assinatura de um Termo de Compromisso Individual no momento do ingresso de terceirizados;

III - obter a assinatura de um Termo de Responsabilidade no momento da aquisição de produtos e/ou serviços.

Art. 25 - Compete às unidades administrativas e acadêmicas:

I - divulgar esta política assim como as normas e procedimentos específicos relacionados que estejam de acordo com as atividades exercidas em seu âmbito de atuação.

II - disseminar a cultura de segurança da informação na unidade e para incentivar a participação dos programas de conscientização e treinamentos em segurança da informação.

Art. 26 - Compete à Comissão Permanente de Processos Administrativos e Disciplinares (CPPAD) aplicar o processo disciplinar, quando necessário.

Capítulo VIII
CONFORMIDADE

Art. 27 - A UFPel reserva-se o direito de auditar todo e qualquer tipo de ativo de informação para garantir a conformidade com esta Política, por meio de vários métodos, em conformidade com a Norma Complementar nº 11/IN01/DSIC/GSIPR.

Art. 28 - Qualquer exceção a esta Política deve ser solicitada com antecedência através de formalização ao Comitê de Segurança da Informação e Comunicações. Exceções a esta Política serão revisadas periodicamente para adequação.

Art. 29 - A violação desta Política pode resultar na suspensão ou perda de privilégios de uso do infrator, com relação ao acesso aos dados institucionais e aos ativos de informação da universidade, sem prejuízo das sanções administrativas, civis e criminais aplicáveis.

Capítulo IX
DISPOSIÇÕES FINAIS

Art. 31 - Esta Política de Segurança da Informação e Comunicações deve ser revisada e/ou atualizada a cada 03 anos ou quando eventos ou mudanças significativas assim exigirem.

Art. 32 - Todo usuário pode propor mudanças a esta Política de Segurança da Informação e Comunicações e em suas normas e procedimentos relacionados, desde que devidamente fundamentadas, para avaliação do Comitê de Segurança da Informação e Comunicações.

Art. 33 - A presente Política entra em vigor a partir da data de sua publicação.