POLÍTICA DE SEGURANÇA DA INFORMAÇÃO NAS UNIVERSIDADES: TEORIA E PRÁTICA

Afonso Comba de Araújo Neto

Universidade Federal do Rio Grande do Sul - UFRGS
Centro de Processamento de Dados
E-mail: afonso@cpd.ufrgs.br

Resumo. *As universidades federais têm características que tornam a implementação de mecanismos e controles de segurança uma tarefa particularmente desafiadora, tarefa esta que ao mesmo tempo é indispensável no cenário atual de expansão dos serviços de TI prestados. Neste artigo são apresentadas e discutidas as características que tornam esta tarefa difícil e qual o papel de uma boa política de segurança da informação na solução deste problema. Neste contexto, é apresentado o caso da UFRGS, sendo descrito o histórico da sua PSI e os efeitos positivos obtidos com a sua implantação.*

Tipo de trabalho: *Relato de Experiência*
Palavras chaves: *Política de Segurança da Informação, Universidades Federais, Serviços de TI*

1 INTRODUÇÃO

O aumento progressivo da informatização dos processos de negócio e da coleta e armazenamento de informações pelos sistemas desenvolvidos para isso reforça cada vez mais a importância da proteção destes sistemas, e que esta proteção seja considerada requisito básico dos mesmos. Notícias de roubo de informações, invasão de computadores, mau uso de informações pessoais e a exploração de fragilidades informáticas para a prática de crimes, que antes eram executados de outras formas, já fazem parte do dia a dia das instituições públicas e privadas.

Nos últimos anos, o assunto "Política de Segurança da Informação" (PSI) tem ganhado cada vez mais importância. O governo federal encontra-se em um momento no qual já demonstra a clara a necessidade do fortalecimento de iniciativas de segurança da informação, não apenas nas áreas de TI, mas em todos os processos de negócio que lidam com informações governamentais e dos cidadãos. Necessariamente, esta preocupação estende-se às autarquias e, portanto, às universidades federais. Embora o Decreto nº 3.505, de 13 de junho de 2000 institua a Política de Segurança da Informação nestes órgãos, a verdade é que a sua regulamentação particular, considerando as especificidades de cada órgão, é imprescindível para a sua efetiva aplicação.

Uma PSI é um instrumento administrativo cuja finalidade principal é a de atribuição responsabilidades quanto aos aspectos de segurança da informação associados ao negócio da instituição que lhe define. Não existe uma PSI genérica, pois a sua coerência depende estritamente da organização à qual ela se aplica. De certa forma, pode-se dizer que uma PSI tem como objetivo final alterar os processos de negócio que lidam com informações das mais variadas naturezas, a fim de prover os mesmos de mecanismos que garantam as propriedades de segurança que são atribuídas a estas informações. Por exemplo, não existe sentido em rotular uma determinada informação como de *acesso restrito* caso os processos de trabalho e de manipulação da mesma não sejam modificados de acordo a garantir que apenas as pessoas autorizadas tenham acesso à mesma. Existe a necessidade explícita de que alguém fique responsabilizado pela idealização destes processos, implantação dos mesmos e posterior auditoria destes, de forma a verificar que os processos estão sendo seguidos de forma consistente. Uma PSI formaliza estes requisitos de segurança e atribui responsabilidades para que eles sejam implementados e mantidos. Em outras palavras uma boa PSI:

- Define explicitamente o que é segurança da informação e seus atributos, e quais os objetivos que se pretende obter com a sua promoção,
- Atribui explicitamente a todos os membros da organização a responsabilidade para com a segurança das informações da mesma,

- Define papeis e responsabilidades específicas para todas atividades das quais a segurança da informação depende,
- Define normas, princípios e procedimentos que permitem a resolução dos conflitos que podem surgir da implementação de controles de segurança,
- Deve estar ligada e conectada à gestão de TI, mas não unicamente.

Neste artigo, é feita uma apresentação e discussão dos requisitos de segurança típicos enfrentados pelas organizações atuais, tomando em atenção o caso particular das Universidades, abordando os aspectos relativos a como estes requisitos contrastam com a natureza aberta das instituições de nível superior no Brasil. Também é apresentado o caso da UFRGS, descrevendo-se o histórico do desenvolvimento bem-sucedido e aprovação de uma política de segurança própria, bem como os efeitos positivos da sua implantação até o momento.

2 SEGURANÇA DA INFORMAÇÃO E AUTONOMIA UNIVERSITÁRIA

Há tempos as universidades federais investem progressivamente na área de TI. É um investimento não só absolutamente natural para o momento em que a sociedade vive, mas também coerente com a otimização do serviço público e aperfeiçoamento dos processos de ensino, pesquisa extensão que são responsabilidades destes órgãos. Esta informatização faz com que cada vez mais a TI nas IFES deixe de ter o caráter de benefícios pontuais para serem considerados como requisitos de infraestrutura. Serviços de conectividade e a disponibilização de autosserviços para a comunidade universitária são assumidos como obrigações da instituição, o que acaba por tornar a mesma uma provedora de serviços de TI. Dentre as expectativas mais comuns para estes serviços, podemos citar:

- Conectividade ubíqua,
- Aplicações úteis, sincronizadas e eficientes,
- Compatibilidade com múltiplos dispositivos,
- Utilização simultânea de dispositivos pessoais e institucionais,
- Dados universalmente acessíveis,
- Usabilidade alta em todas as suas vertentes: do desenho das interfaces à complexidade de configuração.

Claramente, estes serviços de TI vão sempre estar atrelados ao processamento de informações, sensíveis ou não, dos mais variados tipos, e desta situação emerge a necessidade da imposição de requisitos de segurança e proteção das mesmas. A lista de problemas se segurança enfrentados pelas IFES no provimento de serviços de TI é numerosa, destacando-se:

- Gestão de identidades e privilégios de acesso,
- Confiabilidade dos mecanismos de autenticação e de restauração de acesso,
- Conformidade legal,
- Tratamento de incidentes de segurança da informação e auditabilidade,
- Gestão de configuração.

É importante ressaltar que serviços de TI sem os respectivos requisitos de segurança fazem mais mal do que bem. Isso é evidente quando se imagina que neste caso as pessoas podem ter a privacidade dos seus dados violada (incluindo suas informações pessoais), que os usuários podem agir uns em nome dos outros e que os sistemas não poderiam ser confiados como tendo informações íntegras. De forma a garantir que um cenário destes não ocorra, o próprio governo federal possui normativas como o Marco Civil da Internet, que impões restrições legais à forma como a qual o tráfego de Internet deve ser administrado, e os tipos de registros que pode ou não podem ser feitos relativamente ao tráfego dos usuários e também como o Decreto 8135/2013, que em última instância decide que dados governamentais não podem ser armazenados nem comunicados através de dispositivos de TI privados.

Ao mesmo tempo, as universidades federais são, segundo a Constituição Federal de 1988, instituições autônomas administrativamente, segundo seu Art. 207, o que induz às mesmas a se

organizarem da forma que desejarem, desde que primem pela "*indissociabilidade entre ensino, pesquisa e extensão*". Assim, no caso da UFRGS, em seu Estatuto Geral, Art. 2º, a universidade é "*expressão da sociedade democrática e pluricultural, inspirada nos ideais de liberdade, de respeito pela diferença*", e, em seu Regimento Geral, Art. 2º, enuncia que a administração universitária "*far-se-á pela articulação entre esta [Reitoria], as Unidades Universitárias e demais órgãos da Universidade*", evidenciando um paradigma muito mais de cooperação interna do que de hierarquia. Em outras palavras, pode-se resumir a caracterização administrativa das Universidades através dos seguintes pontos:

- Hierarquia não é rígida, e a autonomia também é compreendida no nível das Unidades,
- A instituição é fundamentada em princípios democráticos, tolerando divergências e formas de ação alternativas,
- É consenso de que o ensino, pesquisa e extensão têm prioridade sobre necessidades administrativas, dado o objetivo da instituição. As necessidades da atividade docente precisam ser atendidas.

Dado que a segurança da informação se coloca primariamente pelo estabelecimento de regras e controles bem definidos, é natural perceber que as universidades possuem características que tornam a implementação de controles de segurança um desafio bastante complexo. Uma sólida política de segurança aprovada pelo Conselho Universitário e apoiada pela administração central aparece como exigência fundamental para qualquer iniciativa de segurança bem-sucedida.

3 PSI UFRGS: HISTÓRICO

Desde antes de 2010, algumas tentativas de desenvolvimento de uma Política de Segurança na UFRGS ocorreram. Diversos fatores concorreram para o insucesso destas tentativas iniciais:

- Foco em tecnologia e políticas de uso de dispositivos de TI e rede
- Falta das pressões externas que hoje existem
- Falta de conhecimento da comunidade a respeito do assunto e da sua importância

A origem da atual PSI UFRGS remonta à criação do Comitê Gestor de TI da UFRGS em 2010, e pode ser evidenciada pela seguinte cronologia:

- 2010 - Criação do Comitê Gestor de TI (CGTI) e do Plano de Desenvolvimento Institucional da UFRGS;
- 2010/2011 – CGTI nomeia a ComPDTI, com o objetivo de traçar o plano de trabalho para desenvolvimento de um Plano de Desenvolvimento de TI (PDTI):
  - O PDTI 2011-2015 é criado com um GT específico de segurança da informação;
  - GT de segurança define o desenvolvimento de um PSI como item prioritário;
- 2012 - O Reitor nomeia um grupo de servidores para o trabalho específico de desenvolvimento de uma proposta de PSI para a Universidade;
- 2013 - Após um trabalho extenso em diversas reuniões, o grupo chega a uma proposta de PSI, que é entregue para análise do CGTI;
- 2013 - O CGTI envia a proposta de PSI para o CONSUN, onde é analisada por toda a comunidade acadêmica;
- 2014 - A PSI é aprovada pelo CONSUN;
  - É interessante evidenciar que a maior resistência à esta aprovação partiu justamente da comunidade discente, que inicialmente entendeu a PSI como um mecanismo de controle, e não de responsabilização como ele realmente é. Este mal entendido demonstrou que a consciência sobre a necessidade de segurança da informação e o caráter desta atividade ainda carecem de discussão e disseminação na comunidade;
- 2014 – Apoiado na PSI, o CPD cria o Departamento de Segurança da Informação, determinado explicitamente na PSI. O DSInf passa a coordenar o TRI, Time de Resposta a Incidentes de Segurança da Informação, que antes fazia parte do Departamento de Rede e Suporte;

- 2015 - São nomeados os membros do Comitê de Segurança da Informação, que começam os trabalhos de normatização da PSI (atualmente em desenvolvimento).

4 EFEITOS DA PSI UFRGS

Ainda em implementação, podemos citar como efeitos imediatos da aprovação da PSI:

- Diferenciação clara entre os papeis de gestores e custodiantes da informação, facilitando a definição dos responsáveis por definir os requisitos envolvidos nos processos de trabalho;
- Atribuição da responsabilidade a todos os membros da comunidade (incluindo alunos), significando que todas as atividades da UFRGS precisam explicitamente levar em conta requisitos de segurança informação adequados;
- Criação do Comitê de Segurança da Informação, responsável pela criação de normas;
- Criação do Departamento de Segurança da Informação, responsável pela execução de projetos de segurança e implementação de controles;
- Formalização do ETIR-UFRGS, chamado TRI (Time de Resposta a Incidentes de Segurança), como grupo responsável pelo tratamento de incidentes de segurança.

Ressalta-se que a formalização do TRI por si só trouxe benefícios bastante significativos. Especificamente, no que diz respeito ao tratamento dos incidentes de segurança, na falta de uma PSI:

- Os grupos de segurança podem detectar os problemas, mas não são capazes de induzir a adequação necessária para a correção dos mesmos;
- Os grupos de segurança podem ter suas recomendações ignoradas por funcionários hierarquicamente superiores;
- Os grupos de segurança podem ter seu acesso a sistemas comprometidos negado, impossibilitando investigação adequada;
- Os grupos de segurança podem ver-se obrigados a não trazer a luz incidentes ou ocorrências de segurança envolvendo pessoas de alto escalão, ou que possam eventualmente causar prejuízos a terceiros.

À luz da PSI, o TRI identifica-se como a autoridades no escopo da resolução de incidentes, induzindo as partes envolvidas nos incidentes a fornecer as informações necessárias para que a investigação dos incidentes possa ir sempre até o fim, garantindo a detecção e correção dos problemas existentes. Outra vantagem desta nomeação é a caracterização inequívoca do grupo como responsável interno e externo da organização frente a problemas de segurança organizando e centralizando o conjunto de informações relacionadas com os incidentes.

5 CONCLUSÕES

O natural desenvolvimento e implementação de serviços de TI nas Universidades trazem diversos desafios de gestão, e são particularmente complexos para as questões de segurança da informação. As características das universidades, que primam pela descentralização administrativa e valorização dos ideais de diversidade e tolerância, complicam ainda mais iniciativas de segurança que por natureza dependem de restrições e controles rígidos.

O desenvolvimento de uma boa política de segurança, apoiada pela alta gestão, pode ser vista como o mecanismo que permite o início da resolução dos desafios apresentados, e o que faz com que as comunidades das universidades finalmente tomem a questão da segurança como algo prioritário no conjunto de requisitos colocados às suas atividades. A UFRGS é um caso de sucesso neste sentido, já colhendo frutos de ordem prática sem ferir os ideais de liberdade que são tão importantes e fazem parte natural das universidades federais.