UFRGS
UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL
www.ufrgs.br

CONSUN
Conselho Universitário

DECISÃO Nº 124/2014

O CONSELHO UNIVERSITÁRIO, em sessão de 28/03/2014, tendo em vista o constante no processo nº 23078.020136/13-35, de acordo com o Parecer nº 494/2013 da Comissão de Legislação e Regimentos,

D E C I D E

aprovar a Política de Segurança da Informação da Universidade Federal do Rio Grande do Sul, como segue:

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DA UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL

Art. 1° - A Política de Segurança da Informação da Universidade Federal do Rio Grande do Sul (PSI/UFRGS) observará os princípios, objetivos e diretrizes estabelecidos nesta Resolução, bem como as disposições constitucionais, legais e regimentais vigentes.

Parágrafo único. Integram, também, a PSI/UFRGS, normas gerais e específicas de segurança da informação, bem como procedimentos complementares, destinados à proteção da informação e à disciplina de sua utilização, emanados no âmbito da Universidade.

Art. 2º - A PSI/UFRGS alinha-se às estratégias da Universidade e tem por objetivo garantir a autenticidade, a confidencialidade, a disponibilidade e a integridade das informações produzidas ou custodiadas pela Universidade.

Art. 3º - Para os efeitos desta Resolução, entende-se por:

I - informação: conjunto de dados, textos, imagens, métodos, sistemas ou quaisquer formas de representação dotadas de significado em determinado contexto, independentemente do suporte em que resida ou da forma pela qual seja veiculada;

II - segurança da informação: proteção da informação contra ameaças para garantir a continuidade do negócio, minimizar os riscos e maximizar a eficiência e a efetividade das ações do negócio;

III - gestor da informação: unidade ou projeto da Universidade que, no exercício de suas competências, produz informações ou obtém, de fonte externa

à Universidade, informações de propriedade de pessoa física ou jurídica;

IV - custodiante: entidade detentora da posse, mesmo que transitória, de informação produzida ou recebida pela Universidade;

V - incidente em segurança da informação: evento que tenha probabilidade de comprometer as operações do negócio ou ameaçar a segurança da informação;

VI - rótulo: identificação física ou eletrônica da classificação atribuída à informação;

VII - documento de natureza pública: documento relativo ou pertencente à coletividade, de uso comum a todos, universalmente conhecido ou sem restrição de acesso a qualquer pessoa;

VIII - documento de domínio público: documento ou obra (artística, invenção, desenho industrial, etc.) que pode ser livremente reproduzido, apresentado ou explorado sem necessidade de autorização ou de pagamento de direitos autorais, por esgotamento do prazo previsto em lei ou por outro motivo que tenha feito expirar a propriedade intelectual.

Art. 4º - A segurança da informação na Universidade abrange aspectos físicos, tecnológicos e humanos da organização e orienta-se pelos seguintes princípios:

I - confidencialidade: garante que a informação seja acessada somente pelas pessoas ou processos que tenham autorização para tal;

II - disponibilidade: garante que as informações estejam acessíveis às pessoas e aos processos autorizados, no momento requerido;

III - integridade: garante a não violação das informações, com intuito de protegê-las contra alteração, gravação ou exclusão acidental ou proposital;

IV - autenticidade: assegura a correspondência entre o autor de determinada informação e a pessoa, processo ou sistema a quem se atribui a autoria.

Art. 5º - Compete ao Centro de Processamento de Dados (CPD), por meio de Departamento específico, especializado em Segurança da Informação (DSInf):

I - coordenar e acompanhar a implementação da PSI/UFRGS e das normas complementares;

II - homologar processos de trabalho e procedimentos operacionais necessários para a implementação da PSI/UFRGS;

III - monitorar, auditar e avaliar periodicamente as práticas de segurança da informação adotadas pela Universidade;

IV - constituir e coordenar a Equipe de Tratamento de Incidentes de Segurança da Informação da Universidade.

Parágrafo único. Cabe às demais unidades da Universidade, no âmbito de suas competências, a implementação e o acompanhamento de ações para segurança da informação.

Art. 6º - Para fins de segurança da informação, os usuários que tenham acesso, de forma autorizada, às informações produzidas ou custodiadas pela

Universidade classificam-se em:

I - usuário interno: qualquer servidor ativo da Universidade;

II - usuário colaborador: prestador de serviço terceirizado, estagiário, bolsista ou qualquer outro colaborador da Universidade;

III - usuário discente: qualquer pessoa física que tenha vínculo em algum curso oferecido pela Universidade;

IV - usuário externo: qualquer pessoa física ou jurídica que não seja caracterizada como usuário interno, colaborador ou discente.

§ 1º - Os usuários internos, externos, discentes e colaboradores estão sujeitos às diretrizes, normas e procedimentos de segurança da informação da PSI/UFRGS.

§ 2º - Os usuários internos, discentes e colaboradores são responsáveis por garantir a segurança das informações da Universidade a que tenham acesso e por reportar ao DSInf os incidentes em segurança da informação de que tenham conhecimento.

Art. 7º - O acesso às informações produzidas ou custodiadas pela Universidade, que não seja de domínio público, deve ser limitado às atribuições necessárias ao desempenho das respectivas atividades dos usuários internos, discentes ou colaboradores.

§ 1º - Qualquer outra forma de uso que extrapole as atribuições necessárias ao desempenho das atividades dos usuários internos, discentes ou colaboradores necessitará de prévia autorização formal, pelo custodiante.

§ 2º - O acesso, quando autorizado, dos usuários discentes, colaboradores ou externos a informações produzidas ou custodiadas pela Universidade que não sejam de domínio publico é condicionado ao aceite a termo de sigilo e responsabilidade.

Art. 8º - As medidas de segurança da informação devem ser planejadas, aplicadas, implementadas e, periodicamente, avaliadas de acordo com os objetivos institucionais e os riscos para as atividades da Universidade.

§ 1º - Cabe ao Comitê de que trata o Art. 21 desta Decisão elaborar proposta e promover um Plano de Gestão de Riscos que inclua um Plano de Gestão de Incidentes de Segurança da Informação e um Plano de Continuidade de Negócio, com medidas que garantam a continuidade das atividades da Universidade em caso de desastre ou falhas nos recursos que suportam os processos vitais de negócio da Universidade.

§ 2º - Ações permanentes de divulgação, treinamento, educação e conscientização dos usuários, em relação aos conceitos e às praticas de segurança da informação em toda sua abrangência, devem ser coordenadas pelo DSInf, com o apoio das demais unidades pertinentes.

Art. 9º - As informações produzidas ou custodiadas pela Universidade serão classificadas em função do seu grau de confidencialidade, disponibilidade, integridade e prazo de retenção.

§ 1º - A classificação disposta por esta Decisão contempla critérios quanto à confidencialidade, disponibilidade e integridade das informações.

§ 2º - A classificação quanto ao prazo de retenção se dá por meio do Sistema de Acervos e Arquivos da UFRGS.

§ 3º - A autorização, o acesso e o uso das informações produzidas ou custodiadas pela Universidade devem ser controlados de acordo com a respectiva classificação.

Art. 10 - Quanto à confidencialidade, as informações produzidas ou custodiadas pela Universidade classificam-se nos seguintes graus:

I - públicas: informações que podem ser divulgadas a qualquer pessoa;

II - restritas: informações que, por sua natureza ou por interesse da Universidade, só podem ser divulgadas a um grupo restrito de pessoas;

III - sigilosas: informações que, em razão de lei, interesse público ou para a preservação de direitos individuais, devam ser de conhecimento reservado;

IV - pessoais: informações relativas à intimidade privada, vida privada, honra e imagem das pessoas.

§ 1º - Para a classificação da informação em determinado grau de sigilo deverá ser utilizado o critério menos restritivo possível.

§ 2º - Ao conjunto de informações que não possa sofrer fracionamento para fins de acesso deverá ser atribuído o grau de confidencialidade da sua parte cuja classificação seja a mais restritiva.

§ 3º - Todas as partes, seções, anexos, páginas, planilhas, gráficos ou quaisquer outros componentes de informação não pública, independentemente do suporte em que residam ou da forma pela qual sejam veiculados, devem ter seus graus de confidencialidade identificados por meio de rótulos padronizados, em consonância com as regras de identidade visual da Universidade, ressalvados os limites de fracionamento indicados no parágrafo anterior.

§ 4º - Informações classificadas como sigilosas terão os prazos de restrição de acesso definidos de acordo com a legislação vigente, a saber: 5 (cinco) anos para informações reservadas, 15 (quinze) anos para informações secretas e 25 (vinte e cinco) anos para informações ultrassecretas.

Art. 11 - Cabe ao gestor da informação classificá-la quanto à confidencialidade no momento em que a informação for produzida ou obtida, ressalvados os procedimentos dispostos no § 2º do Art. 21 desta Decisão.

§ 1º - No ato da classificação da informação, o gestor deve considerar a legislação em vigor, os controles administrativos e tecnológicos necessários ao tratamento da confidencialidade da informação, as necessidades de compartilhamento ou restrição de acesso e os custos de proteção.

§ 2º - O gestor da informação, ao classificá-la como sigilosa ou restrita, deve indicar, necessariamente, o grupo de pessoas, projetos ou unidades da Universidade com permissão para acessá-la.

§ 3º - As informações produzidas pela Universidade podem ser reclassificadas pelo gestor da informação ou pela autoridade competente, por iniciativa própria ou por solicitação de qualquer usuário, cabendo comunicação imediata da alteração aos custodiantes da informação para correta rotulação.

Art. 12 - Não deve ser conferido tratamento sigiloso ou restrito às informações contidas em documentos que, por força de lei, sejam de natureza pública ou de domínio público.

Art. 13 - As informações produzidas ou custodiadas pela Universidade são classificadas quanto à disponibilidade em função do impacto que a indisponibilidade da informação acarretaria à imagem ou às operações vitais das atividades finalísticas da Universidade.

Art. 14 - O impacto da indisponibilidade das informações produzidas ou custodiadas pela Universidade classifica-se em:

I - baixo: quando a indisponibilidade (ou interrupção de acesso) da informação não comprometer a imagem ou as operações vitais ao negócio da Universidade, nem causar qualquer tipo de perda financeira à Universidade;

II - médio: quando a indisponibilidade (ou interrupção de acesso) da informação comprometer a imagem, a tomada de decisões ou a produtividade das operações vitais ao negócio da Universidade, mas sem interrompê-las, ou causar perda financeira à Universidade;

III - alto: quando a indisponibilidade (ou interrupção de acesso) da informação comprometer severamente a imagem ou as operações vitais ao negócio da Universidade, ou causar perda financeira significativa à Universidade.

Art. 15 - As informações produzidas ou custodiadas pela Universidade são classificadas quanto à integridade em função do impacto que a alteração, inclusão ou exclusão indevida ou não autorizada da informação acarretaria à imagem ou às operações vitais ao negócio da Universidade.

Art. 16 - O impacto da perda de integridade das informações produzidas ou custodiadas pela Universidade classifica-se em:

I - baixo: quando a perda de integridade da informação não comprometer a imagem ou as operações vitais ao negócio da Universidade, nem causar qualquer tipo de perda financeira à Universidade;

II - médio: quando a perda de integridade da informação comprometer a imagem, a tomada de decisões ou a produtividade das operações vitais ao negócio da Universidade, mas sem interrompê-las, ou causar perda financeira à Universidade;

III - alto: quando a perda de integridade da informação comprometer severamente a imagem ou as operações vitais ao negócio da Universidade, ou causar perda financeira significativa à Universidade.

Art. 17 - São responsabilidades do gestor da informação, no que concerne às informações sob sua gestão, produzidas ou custodiadas pela Universidade:

I - adotar as medidas e procedimentos necessários para garantir a segurança das informações;

II - definir procedimentos, critérios de acesso e classificar as informações,

observados os dispositivos legais e regimentais relativos ao sigilo e a outros requisitos de classificação pertinentes;

III - propor regras específicas ao uso das informações.

§ 1º - As informações recebidas de pessoa física ou jurídica externa à Universidade serão submetidas, adicionalmente, a medidas de segurança da informação compatíveis com os requisitos pactuados com quem as forneceu.

§ 2º - O Reitor, os Pró-Reitores e os Diretores de Unidade podem indicar, orientar e autorizar, a qualquer tempo, procedimentos que visem garantir a segurança da informação, nos processos e documentos de sua competência, a serem seguidos pelos gestores da informação pertinentes.

Art. 18 - São responsabilidades do custodiante da informação:

I - garantir a segurança da informação sob sua posse, conforme os critérios definidos pelo respectivo gestor da informação;

II - comunicar tempestivamente ao gestor sobre situações que comprometam a segurança das informações sob custódia;

III - comunicar eventuais limitações para cumprimento dos critérios definidos pelo gestor para segurança da informação, para que este decida quanto à cessão ou não da informação.

Art. 19 - São responsabilidades dos dirigentes das unidades e demais chefias da Universidade, no que se refere à segurança da informação:

I - conscientizar usuários internos e colaboradores sob sua supervisão em relação aos conceitos e às praticas de segurança da informação;

II - incorporar aos processos de trabalho de sua unidade, ou de sua área, práticas inerentes à segurança da informação;

III - tomar as medidas administrativas necessárias para que sejam aplicadas ações corretivas nos casos de comprometimento da segurança da informação por parte dos usuários internos e colaboradores sob sua supervisão.

Art. 20 - Fica instituído o Gestor de Segurança da Informação, indicado pelo Reitor, com as seguintes responsabilidades:

I - presidir o Comitê de Segurança da Informação da Universidade, de que trata o Art. 21 desta Decisão;

II - promover a cultura de segurança na Universidade;

III - acompanhar as investigações e avaliações dos danos decorrentes de quebra de segurança na Universidade;

IV - atuar em conjunto com o DSInf na investigação e tratamento de incidentes de segurança da informação na Universidade;

V - propor recursos necessários às ações de segurança da informação na Universidade.

Art. 21 - Fica instituído o Comitê de Segurança da Informação (CSI), órgão colegiado de natureza consultiva e de caráter permanente, presidido pelo Gestor de Segurança da Informação, que tem por finalidade formular diretrizes, normas e mecanismos institucionais que visem ao cumprimento e

implementação da PSI/UFRGS, a análise periódica de sua efetividade e sua contínua melhoria.

§ 1º - Compete ao Comitê apresentar proposta de revisão da PSI/UFRGS, de modo a atualizar a política frente a novos requisitos corporativos, segundo a legislação vigente.

§ 2º - O Comitê deverá adotar as medidas necessárias ao tratamento de situações inerentes à segurança da informação preexistentes à edição da PSI/UFRGS.

§ 3º - A composição e o regulamento do Comitê serão estabelecidos por Ato do Reitor.

Art. 22 - Os contratos, convênios, acordos de cooperação e outros instrumentos congêneres celebrados pela Universidade devem observar, no que couber, os dispositivos integrantes da PSI/UFRGS.

Art. 23 - O uso de recursos de tecnologia da informação da Universidade será regulamentado em norma específica, respeitando-se os dispositivos legais.

Art. 24 - A não observância dos dispositivos da PSI/UFRGS pode acarretar, isolada ou cumulativamente, nos termos da legislação aplicável, sanções administrativas, civis e penais, assegurados aos envolvidos o contraditório e a ampla defesa.

Art. 25 - Esta Decisão entra em vigor na data de sua publicação.

Porto Alegre, 28 de março de 2014.

(o original encontra-se assinado)
CARLOS ALEXANDRE NETTO,
Reitor.