RESOLUÇÃO Nº 21/14-COPLAD

Cria a Política de Segurança da Informação na Universidade Federal do Paraná (PSI/UFPR).

O **CONSELHO DE PLANEJAMENTO E ADMINISTRAÇÃO** da Universidade Federal do Paraná, no uso de suas atribuições regimentais e estatutárias, e considerando a Resolução n° 22/11-COPLAD, e consubstanciado no parecer nº 75/14 constante no processo nº 049123/2014-12 exarado pelo Conselheiro Luiz Antonio Passos Cardoso e por unanimidade de votos.

RESOLVE:

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

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

Art. 2º A PSI/UFPR 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 e devem ser executadas em conformidade com os princípios básicos da administração pública e com as seguintes diretrizes:

I- observância da publicidade como preceito geral e do sigilo como exceção;

II- divulgação de informações de interesse público, independentemente de solicitações;

III- utilização de meios de comunicação viabilizados pela tecnologia da informação;

IV- fomento ao desenvolvimento da cultura de transparência na administração pública;

V- desenvolvimento do controle social da administração pública.

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

I- informação: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;

II- documento: unidade de registro de informações, qualquer que seja o suporte ou formato;

III- informação sigilosa: aquela submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado;

IV- informação pessoal: aquela relacionada à pessoa natural identificada ou identificável;

V- tratamento da informação: conjunto de ações referentes à produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle da informação;

VI- disponibilidade: qualidade da informação que pode ser conhecida e utilizada por indivíduos, equipamentos ou sistemas autorizados;

VII- autenticidade: qualidade da informação que tenha sido produzida, expedida, recebida ou modificada por determinado indivíduo, equipamento ou sistema;

VIII- integridade: qualidade da informação não modificada, inclusive quanto à origem, trânsito e destino;

IX- primariedade: qualidade da informação coletada na fonte, com o máximo de detalhamento possível, sem modificações.

X- segurança da informação: ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;

XI- gestão de Segurança da Informação: ações e métodos que visam à integração das atividades de gestão de riscos, gestão de continuidade do objetivo, tratamento de incidentes, tratamento da informação, conformidade, credenciamento, segurança cibernética, segurança física, segurança lógica, segurança orgânica e segurança organizacional aos processos institucionais estratégicos, operacionais e táticos, não se limitando, portanto, à tecnologia da informação;

XII- 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;

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

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

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

XVI- 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;

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

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

III- integridade: propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;

IV- autenticidade: propriedade de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade;

Art. 5º Compete ao Centro de Computação Eletrônica (CCE), por meio de Departamento específico, especializado em Segurança da Informação (DSInf):

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

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

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/UFPR.

§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 Comitê de Segurança da Informação 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 Segurança da Informação 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 Objetivo, ouvidos os Comitês de Recursos de Tecnologia da Informação e de Usuários, com medidas que garantam a continuidade das atividades da Universidade em caso de desastre ou falhas nos recursos que suportam os processos vitais de finalidade 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 Comitê de Segurança da Informação, com o apoio das demais unidades pertinentes.

Art. 9° Qualquer interessado poderá apresentar pedido de acesso a informações aos órgãos e unidades desta Universidade, por qualquer meio legítimo, devendo o pedido conter a identificação do requerente e a especificação da informação requerida.

§1° Para o acesso a informações de interesse público, a identificação do requerente não pode conter exigências que inviabilizem a solicitação.

§2° A Universidade priorizará que os pedidos de informação sejam solicitados diretamente às unidades de competência correspondente a informação de interesse, ou para a ouvidoria, que classificará e encaminhará a unidade correspondente.

§3° A Universidade prioriza que as solicitações sejam encaminhadas para suas unidades através de seus sítios oficiais na internet.

§4° Está Resolução não disciplina e não se aplica a pedidos de informações relacionados aos Processos Seletivos, Concursos Públicos, Processos Avaliativos e demais processos classificatórios, que pela natureza da concorrência, serão regidos por Editais próprios.

Art. 10 O órgão ou unidade deverá autorizar ou conceder o acesso imediato à informação disponível.

§1° Não sendo possível conceder o acesso imediato, na forma disposta no caput, o órgão ou entidade que receber o pedido deverá, em prazo não superior a 20 (vinte) dias:

I- comunicar a data, local e modo para se realizar a consulta, efetuar a reprodução ou obter a certidão;

II- indicar as razões de fato ou de direito da recusa, total ou parcial, do acesso pretendido; ou

III- comunicar que não possui a informação, indicar, se for do seu conhecimento, o órgão ou a entidade que a detém, ou, ainda, remeter o requerimento a esse órgão ou entidade, cientificando o interessado da remessa de seu pedido de informação.

§2° O prazo referido no §1° poderá ser prorrogado por mais 10 (dez) dias, mediante justificativa expressa, da qual será cientificado o requerente.

§3° Sem prejuízo da segurança e da proteção das informações e do cumprimento da legislação aplicável, o órgão ou entidade poderá oferecer meios para que o próprio requerente possa pesquisar a informação de que necessitar.

§4° Quando não for autorizado o acesso por se tratar de informação total ou parcialmente sigilosa, o requerente deverá ser informado sobre a possibilidade de recurso, prazos e condições para sua interposição, devendo, ainda, ser-lhe indicada a autoridade competente para sua apreciação.

§5° A informação armazenada em formato digital será fornecida nesse formato, caso haja anuência do requerente.

§6° Caso a informação solicitada esteja disponível ao público em formato impresso, eletrônico ou em qualquer outro meio de acesso universal, serão informados ao requerente, por escrito, o lugar e a forma pela qual se poderá consultar, obter ou reproduzir a referida informação, procedimento esse que desonerará o órgão ou entidade pública da obrigação de seu fornecimento direto, salvo se o requerente declarar não dispor de meios para realizar por si mesmo tais procedimentos.

Art. 11 O serviço de busca e fornecimento da informação é gratuito, salvo nas hipóteses de reprodução de documentos pelo órgão ou entidade pública consultada, situação em que poderá ser cobrado exclusivamente o valor necessário ao ressarcimento do custo dos serviços e dos materiais utilizados.

Parágrafo único. Estará isento de ressarcir os custos previstos no caput todo aquele cuja situação econômica não lhe permita fazê-lo sem prejuízo do sustento próprio ou da família, declarada nos termos da Lei no 7.115, de 29 de agosto de 1983.

Art. 12 Quando se tratar de acesso à informação contida em documento cuja manipulação possa prejudicar sua integridade deverá ser oferecido a consulta de cópia, com certificação de que esta confere com o original.

Parágrafo único. Na impossibilidade de obtenção de cópias, o interessado poderá solicitar que, a suas expensas e sob supervisão de servidor público, a reprodução seja feita por outro meio que não ponha em risco a conservação do documento original.

Art. 13 É direito de o requerente obter o inteiro teor de decisão de negativa de acesso, por certidão ou cópia.

Art. 14 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 Resolução 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 UFPR.

§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. 15 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 públicas, 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.

§5° As informações de projetos de pesquisas aprovados pelas diferentes instâncias da Universidade e devidamente registradas na PRPPG são pré-classificadas como reservadas;

§6° A classificação referida no parágrafo anterior e os efeitos do mesmo são automaticamente cancelados em decorrência de publicação de resultados, mesmo que parciais, ou de defesas públicas de trabalhos finais de cursos, dissertação ou tese.

§7° A classificação da informação em determinado grau de sigilo deverá considerar entre outros:

I- a exigência de restrição imposta por decisão judicial;

II- a existência de prerrogativa diplomática;

III- a exposição ou favorecimento de risco ao individuo, vinculado ou não a Universidade;

IV- A Universidade tratará as informações pessoais nos termos do Art. 31 da Lei 12.527/11, priorizando o sigilo e a integridade do individuo, excetuando os dados necessários ao funcionamento, transparência e controle das atividades de Ensino, Pesquisa e Extensão.

Art. 16 Cabe ao gestor da informação classificá-la quanto à confidencialidade no momento em que a informação for produzida ou obtida, ressalvados os procedimentos disposto pelo Comitê de Segurança da Informação.

§1° 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.

§2° 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. 17 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. 18 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. 19 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 objetivo 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 objetivo 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 objetivo da Universidade, ou causar perda financeira significativa à Universidade.

Art. 20 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 objetivo da Universidade.

Art. 21 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 objetivo 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 objetivo 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 objetivo da Universidade, ou causar perda financeira significativa à Universidade.

Art. 22 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.

§3º Os servidores têm a obrigação de manter os sistemas de informações atualizados;

§4º Compete aos servidores informar imediatamente a ouvidoria da UFPR, quando encontrar informação com qualquer grau de inconsistência. A ouvidoria deverá destinar a unidade correspondente e encaminhar para conhecimento do COPLAD mensalmente, as ocorrências registradas, organizadas por assunto.

Art. 23 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. 24 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. 25 Fica instituído o Gestor de Segurança da Informação, indicado pelo Reitor, com as seguintes responsabilidades:

I- promover a cultura de segurança na Universidade;

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

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

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

Art. 26 Os contratos, convênios, acordos de cooperação e outros instrumentos congêneres celebrados pela Universidade devem observar, no que couber, os dispositivos integrantes da PSI/UFPR.

Art. 27 O uso de recursos de tecnologia da informação da Universidade será regulamentado em norma específica, respeitando-se os dispositivos legais.

Art. 28 A não observância dos dispositivos da PSI/UFPR 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. 29 Esta Resolução entra em vigor na data de sua publicação.

Sala de Sessões, em 24 de setembro de 2014.

Rogério Andrade Mulinari
Presidente em exercício