RESOLUÇÃO *AD REFERENDUM* Nº. 055 DE 14 DE NOVEMBRO DE 2017

"Dispõe sobre a aprovação da Instrução Normativa CGSIP/UERR Nº 1 de 10 de novembro de 2017, que dispõe sobre a Política de Segurança da Informação da Universidade Estadual de Roraima."

O PRESIDENTE DO CONSELHO UNIVERSITÁRIO DA UNIVERSIDADE ESTADUAL DE RORAIMA, no uso das atribuições que lhe conferem o Estatuto da UERR, em seu Art. 22, aprovado pelo Decreto nº. 24.022-E de 10 de outubro de 2017, e o Decreto nº 012 - P, de 04 de janeiro de 2016, por meio de decisão *Ad Referendum* em 07 de novembro de 2017,

RESOLVE:

Art. 1º Aprovar a Instrução Normativa CGSIP/UERR Nº. 1 de 10 de novembro de 2017, que dispõe sobre a Política de Segurança da Informação da Universidade Estadual de Roraima.

Art. 2º Esta Resolução entrará em vigor na data de sua publicação, revogando-se as disposições em contrário.

DÊ-SE CIÊNCIA, PUBLIQUE-SE E CUMPRA-SE.

Boa Vista-RR, 14 de novembro de 2017.

REGYS ODLARE LIMA DE FREITAS
Presidente do Conselho Universitário

Publicado no DOE Nº. 3120 em 14.11.17

Secretaria dos Conselhos Superiores
Rua 7 de Setembro, 231 - Canarinho
CEP 69306-530 / Boa Vista - RR - Brasil
Fone: (95) 2121-0913
E-mail: socs.conuni@uerr.edu.br
www.uerr.edu.br

ANEXO I DA RESOLUÇÃO Nº. 055 DE 14 DE NOVEMBRO DE 2017

INSTRUÇÃO NORMATIVA CGSIP/UERR Nº 1 DE 10 DE NOVEMBRO DE 2017

Dispõe sobre a Política de Segurança da Informação da Universidade Estadual de Roraima.

O PRESIDENTE DO COMITÊ GESTOR DE SEGURANÇA DA INFORMAÇÃO E PLANEJAMENTO DA UNIVERSIDADE ESTADUAL DE RORAIMA, no uso das atribuições que lhe conferem a Portaria Nº 1022 de 01 de novembro de 2017, e

CONSIDERANDO a necessidade de estabelecer diretrizes e padrões para garantir um ambiente tecnológico controlado e seguro de forma a oferecer todas as informações necessárias ao funcionamento desta IES com integridade, confidencialidade, disponibilidade e confiabilidade;

CONSIDERANDO que Universidade Estadual de Roraima, no exercício de suas competências, gera, adquire e absorve informações, que devem permanecer íntegras, disponíveis e, quando for o caso, com o sigilo resguardado;

CONSIDERANDO que a integridade e a credibilidade da instituição na prestação do serviço público devem ser preservadas;

CONSIDERANDO a constante preocupação com a qualidade e celeridade na prestação de serviços à sociedade;

CONSIDERANDO que as informações na UERR são armazenadas em diferentes meios, veiculadas por diferentes formas, manuseadas e tratadas por diversas pessoas e entidades e, portanto, vulneráveis aos incidentes em segurança da informação;

CONSIDERANDO que a adequada gestão da informação precisa nortear todos os processos de trabalho e deve ser impulsionada por uma Política de Segurança da Informação;

RESOLVE:

Art. 1º. Instituir a Política de Segurança da Informação (PSI) da Universidade Estadual de Roraima (UERR).

Publicado no DOE Nº. 3120 em 14.11.17

CAPÍTULO I

Visão Geral e Glossário

Art. 2º. A Política de Segurança da Informação (PSI) da UERR e de seus campi é uma declaração de compromisso com a proteção das informações que cria, manipula, custodia ou que são de sua propriedade, sob o gerenciamento de sua infraestrutura de Tecnologia da Informação (TI), devendo ser conhecida, compreendida e cumprida por todos que tenham acesso às informações.

Parágrafo único. A utilização dos recursos e dispositivos de Tecnologia da Informação (TI) da UERR, ou pessoais em seu proveito, deve ser pautada pelos princípios da ética, segurança e legalidade.

Art. 3º. O Comitê Gestor de Segurança da Informação e Planejamento (CGSIP) publicará, via instrução normativa, glossário específico, o que conterá denominações e limitará conceitos que se aplicarão à PSI, suas normas e procedimentos correlatos, de indispensável conhecimento pelos agentes da administração ou terceiros interessados que tiverem contato com informações e demais recursos de TI.

CAPÍTULO II

Requisitos de Capital Humano, suas Obrigações e Responsabilidades

Art. 4º. Para os efeitos desta Política entende-se por classes de agentes da administração: Reitor, Vice-Reitor, Pró-Reitores, servidores efetivos, servidores cedidos, servidores comissionados, estagiários, alunos da UERR, voluntários e funcionários terceirizados.

Art. 5º. Cabe aos agentes da Administração:

I - Firmar, obrigatoriamente, Termo de Responsabilidade e Confidencialidade sobre as informações às quais tenham acesso em razão do serviço ou do uso da infraestrutura de TI da UERR;

II - Participar das campanhas, eventos ou atualizações promovidas sobre Segurança da Informação no âmbito da UERR;

III - Estar sempre atualizado e ciente das políticas, normas e procedimentos vigentes da UERR ao executar suas tarefas;

IV - Cumprir o disposto na PSI da UERR;

V - Utilizar, modificar ou reproduzir dados e informações da UERR exclusivamente para o desempenho de suas funções, da mesma forma que a utilização dos dispositivos de TI em nome da UERR;

VI - Não divulgar, compartilhar, transmitir ou deixar-se conhecer informações a pessoas que não tenham nível de autorização suficiente;

VII - Não divulgar, compartilhar, transmitir, veicular ou permitir a divulgação, por qualquer meio, informações sobre ativos ou de procedimentos da UERR, exceto quando houver autorização prévia e formal por superior hierárquico ou de acordo com a legislação vigente para tanto;

VIII - Não conduzir, transportar, enviar, transmitir, compartilhar ou deixar que dados e informações alcancem ambiente ou destinatário fora das dependências ou controle desta Instituição de Ensino sem autorização formal;

IX - Proteger ativos de informação contra acesso, divulgação, transmissão, compartilhamento, modificação, destruição ou interferência não autorizadas;

X - Estar atento ao repassar ou transmitir informações para outras pessoas, seja de forma presencial, via telefone, comunicadores instantâneos, mensagens eletrônicas ou mídias sociais. Confirmar a identidade e idoneidade do solicitante ou destinatário antes do envio de informações e, sempre que possível, a real necessidade do compartilhamento de alguma informação solicitada por outra pessoa, mesmo que de sua confiança;

XI - Reportar à Comissão de Segurança da Informação, quaisquer eventos ou incidentes potenciais ou reais que causem riscos à segurança das informações da UERR, ou ainda sua mera suspeita.

Art. 6º. Cabe ao Reitor, Vice-Reitor, Pró-Reitores, Diretorias e chefias:

I - Conhecer, divulgar, cumprir e estimular o cumprimento da PSI, normas e procedimentos correlatos;

II - Atribuir o perfil adequado para acesso a recursos, dados e informações conforme a necessidade, com base nos princípios do conjunto mínimo de permissões que precisam ser atribuídos;

III - A responsabilidade por gerir os recursos de TI e postura dos agentes da administração que compõem sua área ou equipe em relação à Segurança da Informação.

Art. 7º. Cabe à Comissão de Segurança da Informação:

I - Propor alterações na Política de Segurança da Informação (PSI);

II - Elaborar e promover alterações das Normas de Segurança da Informação, sempre que pertinente;

III - Propor alterações e aprovar os termos acessórios da PSI;

IV - Analisar os casos de violação da PSI, incidentes, vulnerabilidades e tentativas de burla, encaminhando-os à Reitoria da UERR, quando providências a serem autorizadas por esta forem requeridas;

V - Propor medidas relacionadas à melhoria da Segurança da Informação da UERR;

VI - Propor o planejamento e a alocação de recursos no que tange à Segurança da Informação da UERR;

VII - Aprovar a relação de responsáveis pelas informações pertencentes ou sob a guarda da UERR;

VIII - Aprovar ou reprovar o acesso a locais de rede, sítios de internet, uso de dispositivos de TI pessoais no ambiente da instituição e demais regras de uso dos recursos de TI oferecidos pela UERR aos agentes da administração.

IX - Publicar e manter atualizado o Glossário da PSI, referido no art. 3º da presente Instrução Normativa, sempre que se fizer necessário.

Art. 8. Cabe à Divisão de Tecnologia da Informação (DTI):

I - Emitir, revogar ou suspender as credenciais de acesso, sempre que solicitadas pela PROGESP;

II - Manter registros de atividades dos usuários pelo tempo correspondente a um ano permitindo controles e auditorias;

III - Formalizar orientação para a PROGESP nas políticas adequadas e aplicáveis aos usuários, cargos, funções e lotação, sempre que necessário;

IV - Apoiar as campanhas de conscientização de Segurança da Informação fornecendo os recursos de TI necessários;

V - Fomentar, sempre que possível, sistema de login unificado/centralizado para acesso aos diversos sistemas.

VI - Para os sistemas desenvolvidos internamente ou cujo desenvolvimento é mantido pela própria equipe da UERR, o login unificado é mandatório e deve ser implementado no prazo máximo de 24 (vinte quatro) meses a partir da data de publicação desta Instrução Normativa.

VII - Para os sistemas contratados, mantidos ou desenvolvidos por terceiros que já estejam em uso pela UERR, deverão ser promovidos esforços para que venham a se adequar ao sistema de login unificado já utilizado.

VIII - Para novos sistemas que venham a ser contratados de terceiros ou desenvolvidos internamente, o login unificado passa a ser pré-requisito elementar, a menos que a possibilidade de login unificado se mostre inviável.

IX - Promover campanhas com o objetivo de conscientizar os agentes da administração sobre a PSI;

X - Fomentar ações para implementar as diretrizes previstas na PSI, normas e procedimentos correlatos**;**

XI - Reportar imediatamente à Comissão de Segurança da Informação os eventos que violem, ou tentem violar, os termos da PSI, das normas ou procedimentos correlatos, ainda que por mera suspeita;

XII - Promover a criação e manutenção de diretrizes, princípios e conteúdos da PSI;

XIII - Solicitar a revogação ou suspensão das credenciais de acesso sempre que detectar a utilização inadequada das mesmas ou a reativação, conforme o caso;

XIV - Coordenar a elaboração, manutenção, implementação e testes do plano de continuidade do negócio e prevenção a desastres;

XV - Zelar para que as diretrizes e os princípios desta política sejam respeitados, informando de ofício, os incidentes e ações à Comissão de Segurança da Informação, ainda que por mera suspeita;

XVI - Responder, adequadamente, a quaisquer consultas das outras áreas sobre a aplicação da PSI, normas e procedimentos de Segurança da Informação e uso aceitável da infraestrutura de tecnologia, orientando-as sobre as melhores práticas;

XVII - Aprovar, reprovar, suspender ou promover a homologação de softwares e hardwares para o uso dos agentes da administração e divulgar lista com permissões e proibições que julgar pertinente, sob apreciação da Comissão de Segurança da Informação;

XVIII - Aprovar, reprovar, suspender ou promover diretamente a liberação do uso de dispositivos de TI pessoais dos agentes da administração no ambiente institucional e aplicar as medidas de segurança cabíveis para a preservação da infraestrutura de TI da UERR;

XIX - Aprovar e publicar a PSI, suas revisões e documentos acessórios, sob apreciação da Comissão de Segurança da Informação.

Art. 9. Cabe à PROGESP quanto aos servidores em geral:

I - Manter atualizados, no sistema informatizado de gestão de pessoas, todos os dados referentes a desligamentos, afastamentos, retornos e modificações no quadro funcional da UERR e de seus órgãos subordinados. Da mesma forma, manter o status atualizado das credenciais que precisem ser emitidas, revogadas e suspensas;

II - Apoiar as campanhas de conscientização de Segurança da Informação, em parceria com a DTI;

III - Incluir o Termo de Responsabilidade e Confidencialidade como documento obrigatório para exercício dos agentes da administração e proceder à guarda segura e adequada dos documentos assinados.

Art. 10. Cabe à PROEG quanto aos alunos de graduação:

I – Manter atualizados, no sistema acadêmico, todos os dados referentes a desligamentos, afastamentos, retornos e modificações no quadro geral de alunos de graduação da UERR. Da mesma forma, manter o status atualizado das credenciais que precisem ser emitidas, revogadas e suspensas.

Art. 11. Cabe à PROPEI quanto aos alunos de pós-graduação:

I – Manter atualizados, no sistema acadêmico, todos os dados referentes a desligamentos, afastamentos, retornos e modificações no quadro geral de alunos de pós-graduação da UERR. Da mesma forma, manter o status atualizado das credenciais que precisem ser emitidas, revogadas e suspensas.

CAPÍTULO III

Classificação da Informação, Controle e Credenciais de Acesso

Art. 12. Cabe aos responsáveis pela informação a classificação e a definição de quem possui acesso e o tipo de privilégios de acesso, sem prejuízo do disposto na legislação vigente.

Art. 13. Cabe aos chefes de divisão, diretores e pró-reitores informarem à DTI via memorando quais colaboradores do seu respectivo setor devem/possuem credenciais de acesso à determinados sistemas.

Art. 14. Cabe aos chefes de divisão, diretores e pró-reitores enviar relatório semestral à DTI informando quais colaboradores de seus respectivos setores possuem credenciais de acesso à determinados sistemas.

Art. 15. Os agentes da administração têm o dever de cumprir com o nível de segurança exigido pela classificação das informações, sob pena de responsabilidade (substituir todos os casos) conforme a gravidade do ato e os prejuízos sofridos.

Art. 16. Não é permitido o acesso ou uso de qualquer recurso de TI ou ativo da informação sem as credenciais de acesso correspondentes.

Art. 17. O agente da administração deve proteger sua identidade digital, devendo suas credenciais, senhas e acessos serem pessoais e tratados de forma segura, confidencial, intransferível, intransmissível, possuindo apenas as permissões suficientes para realização das suas atividades, com orientação nos princípios do conjunto mínimo de permissões que precisam ser atribuídos.

Art. 18. O acesso aos ambientes físicos e recursos lógicos de TI devem ser controlados e restritos às pessoas autorizadas pela DTI, conforme orientação do binômio de necessidade funcional e mais restrita permissão cabível.

Art. 19. Todas as informações criadas, acessadas, compartilhadas, manuseadas, armazenadas ou disponibilizadas ao agente da administração ou das quais tiver acesso no exercício de suas atividades, são de propriedade e/ou direito de uso exclusivo da UERR.

Parágrafo único. Todos os ativos e informações da UERR devem ser utilizados apenas para o cumprimento das atividades profissionais, dentro do padrão de conduta ética estabelecida pela UERR e às demais leis em vigor, respeitando os requisitos de sigilo profissional.

CAPÍTULO IV

Aquisição, Utilização, Controle e Descarte de Recursos de TI

Aquisição

Art. 20. Para adquirir qualquer solução, equipamento ou serviço de TI, o setor interessado deve formular o termo de referência com a supervisão da DTI para que todos os requisitos legais sejam levados em consideração, resoluções internas e questões relacionadas com a garantia da segurança das informações que serão tratadas pela solução, serviço ou equipamento.

Utilização

Art. 21. Os recursos de TI de propriedade da UERR somente poderão ser utilizados pelos agentes da Administração**.**

Art. 22. Todos os equipamentos, dispositivos e demais recursos que fizerem uso da infraestrutura de TI da UERR estarão sujeitos à PSI e às demais normas de Segurança da Informação da UERR e deverão possuir softwares de proteção instalados, a exemplo, mas não se limitando, de antivírus, anti-spyware e firewall sempre ativos e atualizados.

Art. 23. É permitido o uso de dispositivos pessoais de TI nos ambientes da UERR, desde que não haja restrição conforme seu perfil profissional e que não traga prejuízos para a UERR, sendo vedado o uso da infraestrutura de TI da UERR a partir de dispositivos pessoais, a menos que seja previamente autorizado e cadastrado para uso pela DTI.

§1º. Os agentes da administração serão integralmente responsáveis pelos conteúdos armazenados em seus dispositivos pessoais e pelos atos através deles praticados, sem ressalvas ou exceções.

§2º. Os agentes da administração poderão utilizar seus dispositivos pessoais de TI durante o expediente profissional, isto é, desde que não atrapalhe a própria concentração ou dos demais a seu redor nas atividades que devem desempenhar, não prejudique o atendimento ao público ou atrase as tarefas que lhe cabem, não violem a PSI ou gerem riscos a UERR, sob pena de responsabilidade**.**

Controle

Art. 24. São direitos da UERR, através da DTI, registrar, bloquear, permitir, suspender e limitar o uso dos recursos e dispositivos que compõem sua infraestrutura de TI.

Art. 25. A UERR, por meio da DTI, monitora todos os recursos, ambientes, dispositivos e ativos ligados à Tecnologia de Informação, tais como, mas não se restringindo, o e-mail institucional, acesso à internet, espaços físicos e utilização dos dispositivos de TI institucionais, com a finalidade de proteger seus ativos, sua reputação e conhecimento.

§1º. A UERR também registra todos os dados obtidos pelo monitoramento realizado para eventual análise forense, apuração a violações à PSI, podendo investigar fatos que comprometam seus ativos.

§2º. Da mesma forma que indicado no caput, a UERR possui a prerrogativa de registrar, inspecionar, apreender, isolar ou neutralizar dispositivos ou recursos de TI de propriedade de terceiros que pretendam adentrar em seu perímetro lógico ou físico, ou até mesmo impedir que estes o façam, com a utilização das medidas de contenção que entender cabíveis para preservar a incolumidade de sua estrutura de TI e pelo tempo que for necessário, observando os princípios de transparência, proporcionalidade e razoabilidade.

Descarte

Art. 26. O descarte de informações e ativos de TI da UERR devem ser realizados de forma segura, com a destruição, sanitização ou inutilização da mídia ou dispositivo que contém as informações, de modo que fique incapacitada de ser recuperada, adquirida ou reutilizada por terceiros.

CAPÍTULO V

Desenvolvimento, aquisição e manutenção de sistemas de informação

Art. 27. Os Sistemas de Informação adquiridos, mantidos ou desenvolvidos pela UERR deverão atender aos princípios e requisitos de Segurança da Informação, estabelecidos pela presente Instrução Normativa e demais normas em vigor.

Art. 28. As atividades de desenvolvimento, teste e homologação dos Sistemas de Informação não devem afetar o funcionamento dos sistemas em operação. Para isso, a DTI deve manter ambientes de desenvolvimento, homologação e produção separados logicamente.

Art. 29. Os dados classificados como sigilosos, mantidos pelos Sistemas de Informação, não deverão estar replicados ou acessíveis em outro ambiente, sem a competente autorização da DTI, sob o risco de vazamento de informações pessoais ou confidenciais sob a guarda da UERR.

Parágrafo único. O descumprimento desta disposição, sujeitará a responsabilização, podendo incorrer nas penas previstas em lei, conforme sua gravidade e prejuízo a UERR.

CAPÍTULO VI

Análise de conformidade e auditorias

Art. 30. À UERR é facultada a realização de análises de conformidade ou auditorias periódicas na segurança da infraestrutura de TI, seus ativos, processos e pessoas com o objetivo de detectar vulnerabilidades e demonstrar evidências do cumprimento da política e boas práticas de Segurança da Informação.

CAPÍTULO VII

Resposta a incidentes de segurança da informação

Art. 31. É de responsabilidade da DTI a implantação de uma equipe de resposta a incidentes de Segurança da Informação, de forma que as fragilidades e eventos de segurança associados aos ativos de informação sejam comunicados a Comissão de Segurança da Informação, permitindo a tomada de ação corretiva em tempo hábil e com a orientação de preservar ou restabelecer operantes os recursos de TI oferecidos.

Art. 32. A DTI tem o dever de guardar as provas produzidas pelos recursos e dispositivos de TI pelo tempo previsto de um ano, sobretudo em casos de incidente de Segurança de Informação.

CAPÍTULO VIII

Gerenciamento de riscos

Art. 33. É de responsabilidade da DTI mapear e documentar as ameaças e vulnerabilidades que resultam em risco ao negócio e à infraestrutura de tecnologia que o suporta, assim como buscar a solução adequada para cada caso.

Art. 34. É de responsabilidade da Comissão de Segurança da Informação a administração dos riscos identificados.

CAPÍTULO IX

Plano de continuidade do serviço e recuperação de desastres

Art. 35. É de responsabilidade da Comissão de Segurança da Informação coordenar a elaboração, execução, teste e renovação do Plano de Continuidade do Serviço (PCE) que tenha como objetivo minimizar o impacto na disponibilidade dos recursos críticos de TI e, consequentemente, nos processos da UERR por eles suportados.

Art. 36. É de responsabilidade da Comissão de Segurança da Informação aprovar a estratégia de continuidade do plano e fornecer subsídios para a sua implementação.

Art. 37. Independentemente da existência de um Plano de Continuidade dos Negócios ou de Plano de Recuperação de Desastres (PRD), a DTI deve estabelecer normas e procedimentos

para salvaguarda de dados com a frequência de realização conforme o grau de importância de cada informação, mantendo sempre os backups tão atualizados quanto possível.

CAPÍTULO X

Requisitos de Segurança ao Patrimônio Físico

Art. 38. Os requisitos de segurança ao patrimônio físico serão regulamentados por meio de normas e procedimentos específicos elaborados pelo Comitê de Segurança da Informação e submetidos à aprovação do Conselho Universitário.

CAPÍTULO XI

Violações da PSI e sanções

Art. 39. Todos os usuários devem noticiar às autoridades responsáveis, como também à Ouvidoria, os incidentes de Segurança da Informação que presenciarem ou tomarem conhecimento, ainda que por mera suspeita, para que providências adequadas sejam adotadas no menor tempo possível, minimizando os danos sofridos pela UERR, sem prejuízo de comunicação administrativa conforme o caso e urgência, sendo estes apurados pela Comissão de Segurança da Informação.

Art. 40. Violações da presente PSI, normas e procedimentos correlatos são passíveis de penalidades administrativas, sem prejuízo de ações legais cabíveis.

Art. 41. Casos omissos ou esclarecimentos da PSI, normas e procedimentos correlatos são de exclusiva responsabilidade da CSI e passíveis de aprovação pelo CONUNI da UERR, conforme o caso.

Art. 42. Esta Instrução Normativa entra em vigor na data de referendamento pela Reitoria da UERR. Revogam-se outras disposições em contrário.

Boa Vista-RR, 10 de novembro de 2017.

Cláudio Souza da Silva Júnior
Presidente do Comitê Gestor de Segurança
da Informação e Planejamento/UERR

Publicado no DOE Nº. 3120 em 14.11.17