MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL RURAL DO SEMI-ÁRIDO
CONSELHO UNIVERSITÁRIO

RESOLUÇÃO CONSUNI/UFERSA Nº 015/2017, de 15 de dezembro de 2017.

Regulamenta a Política de Segurança da Informação e Comunicação da UFERSA.

O Presidente do **CONSELHO UNIVERSITÁRIO** da **UNIVERSIDADE FEDERAL RURAL DO SEMI-ÁRIDO - UFERSA,** no uso de suas atribuições legais e com base na deliberação deste Órgão Colegiado em sua **10ª Reunião Ordinária de 2017**, em sessão realizada no dia 08 de dezembro de 2017,

CONSIDERANDO o Decreto Nº 3.505, de 13 de junho de 2000 que Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal;

CONSIDERANDO a Instrução Normativa DSIC/GSI/PR nº 1, de 13 de junho de 2008 que Disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências;

CONSIDERANDO a norma ABNT NBR ISO/IEC 27001 de 2006, que normatiza os sistemas de gestão de segurança da informação;

CONSIDERANDO a Lei 12527, de 18 de novembro de 2011 – Lei de acesso à informação;

CONSIDERANDO a Lei nº 9.983, de 14 de julho de 2000: Altera o Decreto Lei no 2848/40 – Código Penal, sobre tipificação de crimes por computador contra a Previdência Social e a Administração Pública;

CONSIDERANDO a Lei nº 9.610, de 19 de fevereiro de 1998, que altera, atualiza e consolida a legislação sobre direitos autorais;

CONSIDERANDO a Lei nº 8.159, de 08 de janeiro de 1991, dispõe sobre a política nacional de arquivos públicos e privados e dá outras providências e alterações legais;

CONSIDERANDO o Decreto nº 7.724 de 16/05/2012, que regulamenta a Lei 12.527, de 18/11/2011 – Dispõe sobre o acesso a informações;

CONSIDERANDO o Decreto nº 4.553, de 27 de dezembro de 2002, que dispõe sobre a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse de segurança da sociedade e do Estado, no âmbito da Administração Pública Federal, e dá outras providências;

CONSIDERANDO o Decreto nº 1.171, de 24 de junho de 1994 que aprova o Código de Ética Profissional do Servidor Público Civil do Poder Executivo Federal e outras providências;

CONSIDERANDO a EMENDA REGIMENTAL Nº 1, de 13 setembro de 2012, que cria o Comitê Gestor de Tecnologia da Informação da UFERSA;

CONSIDERANDO a Decisão CONSUNI/UFERSA Nº 42/2016, de 29 de fevereiro de 2016, que cria a Política de Segurança da Informação e Comunicação da UFERSA,

R E S O L V E:

Art. 1º Regulamentar e definir a Política de Segurança da Informação e Comunicação (POSIC) no âmbito da Universidade Federal Rural do Semi-Árido – UFERSA.

CAPÍTULO I
DOS CONCEITOS E DAS DEFINIÇÕES

Art. 2º Para efeito desta POSIC, deve-se considerar:

I. Acesso Lógico: acesso a redes de computadores, sistemas e estações de trabalho por meio de autenticação;

II. Acesso Remoto: ingresso, por meio de uma rede, aos dados de um computador fisicamente distante da máquina do usuário;

III. Ambiente Computacional de Produção: conjunto de recursos computacionais que está a serviço dos colaboradores da Instituição para lidar com os dados reais do negócio, dados utilizados nas tarefas diárias e cujas informações possuem valores legais e são utilizadas pela Instituição. Por possuir dados reais, é considerado ambiente crítico para a Segurança da Informação da Instituição e, por isso, seu acesso físico e lógico deve ser limitado;

IV. Ambiente Computacional de Homologação: conjunto de recursos computacionais no qual são feitos os testes de um sistema e no qual um grupo restrito de colaboradores tem acesso para validação de funções de um sistema. Possui cópias dos dados do Ambiente computacional de Produção;

V. Ambiente Computacional de Desenvolvimento: ambiente computacional no qual os desenvolvedores criam ou alteram sistemas e funcionalidades. Pode possuir dados reais e funções incompletas, por isso seu acesso é restrito às equipes técnicas de desenvolvimento de software;

VI. Ameaça: conjunto de fatores internos ou externos ou causa potencial de um incidente, que pode resultar em dano para um sistema ou para a organização aproveitando-se ou não de uma vulnerabilidade;

VII. Análise/avaliação de riscos: processo completo de análise e avaliação de riscos;

VIII. Ativos de informação e comunicação: patrimônio composto pelos meios de armazenamento, transmissão e processamento, pelos sistemas de informação, por todos os dados e informações gerados, manipulados, transmitidos ou descartados nos processos da Instituição, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso;

IX. Ativo Sigiloso: qualquer bem tangível ou intangível que possa conter informações sigilosas que, se acessadas por pessoas não autorizadas, podem causar danos significativos à organização;

X. Autenticação: ato de confirmar que algo ou alguém é autêntico, ou seja, uma garantia de que qualquer alegação de ou sobre um objeto é verdadeira;

XI. Autenticidade: propriedade que certifica a produção expedição, modificação e destruição da informação por determinada pessoa, sistema, órgão ou entidade;

XII. Bloqueio de acesso: processo que tem por finalidade suspender temporariamente o acesso;

XIII. Ciclo de vida da informação: engloba o período desde a criação, o armazenamento, a consulta, o manuseio, o transporte até o descarte das informações dentro das regras de negócio da organização;

XIV. Classificação da informação: atribuição, pela autoridade competente, de grau de sigilo dado à informação, documento, material, área ou instalação;

XV. Comunicação: transmissão de informações entre pessoas, equipamentos ou qualquer outro ente, em que haja uma mensagem (informação ou dado), um transmissor (o que emite a mensagem), um receptor (que recebe a mensagem), um meio (por onde tramita a mensagem), seguindo um determinado protocolo (conjunto de procedimentos e linguagens necessários ao entendimento da mensagem);

XVI. Confidencialidade: disponibilidade da informação apenas à pessoa, sistema, órgão ou entidades autorizados;

XVII. Contingência: descrição de medidas a serem tomadas por uma empresa, incluindo a ativação de processos manuais, para fazer com que seus processos vitais voltem a funcionar plenamente, ou num estado minimamente aceitável, o mais rápido possível, evitando assim uma paralisação prolongada que possa gerar maiores prejuízos à corporação;

XVIII. Controle de Acesso: conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso aos ativos da informação e comunicação;

XIX. Cópia de Segurança (Backup): copiar dados em um meio separado do original, de forma a protegê-los de qualquer eventualidade. Essencial para dados importantes;

XX. Dado: representação de uma informação, instrução, ou conceito, de modo que possa ser armazenado e processado por um computador;

XXI. Disponibilidade: propriedade de que a informação esteja acessível e utilizável a quem lhe é dada permissão;

XXII. Gestor da Informação: pessoa responsável pela administração de informações geradas em seu processo de trabalho e/ou sistemas de informação relacionados às suas atividades;

XXIII. Incidente: concretização de evento iniciado por uma ou mais ameaças que comprometa o ciclo de vida da informação;

XXIV. 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 veiculado;

XXV. Informação sigilosa: informação submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado, e aquelas abrangidas pelas demais hipóteses legais de sigilo;

XXVI. Integridade: propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;

XXVII. Perfil de acesso: conjunto de regras que limitam ou permitem o acesso de um usuário a um recurso computacional;

XXVIII. Plano de Contingência: Descreve as medidas a serem tomadas por uma empresa ou órgão público, incluindo a ativação de processos manuais, para fazer com que seus processos críticos voltem a funcionar plenamente, ou num estado minimamente aceitável, o mais rápido possível, evitando assim uma paralisação prolongada;

XXIX. Protocolo: convenção ou padrão que controla e possibilita uma conexão, comunicação ou transferência de dados entre dois sistemas computacionais. Método padrão que permite a comunicação entre processos, conjunto de regras e procedimentos para emitir e receber dados numa rede;

XXX. Quebra de segurança: ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação e das comunicações;

XXXI. Risco: probabilidade de que uma ameaça explore uma vulnerabilidade e gere um incidente com impacto negativo no negócio da organização;

XXXII. Recurso Computacional: equipamento, sistema de informação, dados, meios de armazenamento, meio de transmissão, conectividade de rede, espaço físico e outros elementos físicos e lógicos que permitem a existência coerente de sistemas que dão suporte ao ciclo de vida da informação;

XXXIII. Salvaguarda das informações: propriedade de que as informações críticas deverão ter um número de cópias de segurança/backup compatível com a capacidade/necessidade de recuperação de um incidente;

XXXIV. Sistema de informação: conjunto de meios de comunicação, computadores e redes de computadores, assim como dados e informações que podem ser armazenados, processados, recuperados ou transmitidos por serviços de telecomunicações, inclusive aplicativos, especificações e procedimentos para sua operação, uso e manutenção;

XXXV. Segurança da informação: conjunto de fatores ou características necessárias para que o ciclo de vida da informação ocorra sem incidentes;

XXXVI. Usuário: técnico-administrativo, professor, aluno, consultor, terceirizado, estagiário ou qualquer pessoa autorizada a utilizar os sistemas de informação;

XXXVII. Vulnerabilidade: fragilidade nos recursos computacionais que pode ser explorada para expor, corromper, ocultar informações ou danificar de alguma forma o ciclo de vida da informação.

CAPÍTULO II
DOS PRINCÍPIOS

Art. 3º A POSIC obedecerá à legislação vigente no país, o arcabouço legal que rege a Administração Pública Federal e às normas institucionais, seu Regimento e seus regulamentos.

Art. 4º Esta POSIC e suas ações são norteadas de modo a garantir os seguintes princípios:

I. As regras de segurança dos ativos de informação e comunicação devem ser precisas, concisas e de fácil entendimento;
II. Transparência no trato da informação, observados os critérios legais;
III. Garantia do direito pessoal e coletivo à intimidade e ao sigilo da correspondência e das comunicações individuais, sem comprometimento dos ativos de informação e comunicação;
IV. A proteção dos dados, informações e conhecimentos produzidos, na UFERSA, classificados como sigilosos.

CAPITULO III
DAS DIRETRIZES E ESTRATÉGIAS GERAIS

Art. 5º Todos os ativos de informação e comunicação são considerados parte do patrimônio da UFERSA e devem ser protegidos.

Art. 6º Na proteção dos ativos de informação e comunicação, da UFERSA, deve ser considerado todo o ciclo de vida da informação, bem como estratégias de recuperação de incidentes, propositais ou acidentais, inclusive desastres naturais.

Art. 7º Todas as informações presentes nos ativos de informação e comunicação da UFERSA, devem ser classificadas e tratadas de acordo com seu grau de sigilo.

Art. 8º As regras, normas e padrões de segurança da informação devem ser os mesmos para todos os setores e campi da Instituição.

Art. 9° Todos os ativos de informação e comunicação estão sujeitos a monitoração e auditoria, e os registros assim obtidos poderão ser utilizados para detecção de violações desta POSIC e demais regulamentações em vigor.

CAPITULO IV
DO TRATAMENTO DOS ATIVOS

Art. 10. Com relação ao Tratamento dos Ativos, que envolve a Identificação, Classificação, Manipulação e Conservação dos Ativos, devem ser considerados os seguintes aspectos:

I. Todo Ativo Custodiado ou de propriedade desta instituição deve ser inventariado e protegido segundo as Diretrizes descritas nesta política e nas demais regulamentações em vigor;
II. Todo Ativo de Informação custodiado ou de propriedade desta instituição deve ser classificado quanto aos aspectos de confidencialidade, integridade, autenticidade, não- repúdio e disponibilidade, de forma explícita ou implícita. Esse processo de classificação deve ser implementado e mantido em conformidade com a legislação vigente, visando estabelecer os controles de segurança necessários a cada Ativo de Informação;

III. Todo Ativo Custodiado ou de propriedade desta instituição deve ser cedido somente mediante autorização formal. Essa autorização deve observar a classificação do ativo e a legislação vigente na UFERSA.

CAPITULO V
DO CONTROLE DE ACESSO

Art. 11. Com relação ao Controle de Acesso, que envolve o Acesso Lógico e Físico aos Ativos, devem ser considerados os seguintes aspectos:

I. Todo uso dos Ativos deve ser autorizado pelo Gestor imediato do solicitante, mediante solicitação ao setor responsável pelo ativo;

II. Todo uso dos Ativos deve ser controlado e limitado ao mínimo necessário para o cumprimento das atividades de cada usuário. Qualquer outra forma de uso deve ser previamente autorizada formalmente pelo chefe imediato;

III. Sempre que houver a admissão, mudança das atribuições ou desligamento de servidor desta instituição, será responsabilidade da respectiva chefia imediata notificar ao setor responsável pelos Ativos utilizados por esse membro. O setor responsável pelos Ativos deverá providenciar os ajustes necessários dos privilégios de acesso, do servidor em questão, aos respectivos Ativos; e,

IV. Todo ambiente deve ser classificado e protegido com mecanismos adequados de segurança de acordo com a criticidade e o sigilo dos Ativos que são mantidos naquele local.

CAPITULO VI
DA AUDITORIA E CONFORMIDADE

Art. 12. Com relação à Auditoria e Conformidade devem ser considerados os seguintes aspectos:

I. Todo uso de Ativo, sempre que possível, deve gerar trilhas de auditoria que devem ser mantidas para efeito de análise segundo as diretrizes descritas nesta política e as demais regulamentações em vigor; e,

II. Todo uso de Ativo é passível de monitoramento e auditoria e, sempre que possível, deve ser analisado em busca de indícios de descumprimento desta política e das demais regulamentações em vigor.

CAPITULO VII
DA GESTÃO DE CONTINUIDADE

Art. 13. Com relação à Gestão de Continuidade, que envolve o Backup, Plano de Contingência, Testes, Treinamentos e Documentação de procedimentos, devem ser considerados os seguintes aspectos:

I. Deve ser estabelecida a gestão de continuidade no âmbito da UFERSA, com o objetivo de minimizar os impactos de falhas fortuitas dos Ativos que suportam as operações desta instituição;

II. Deve ser elaborado um plano de contingência para o restabelecimento das operações críticas interrompidas por falhas fortuitas dos Ativos desta instituição;

III. Todo Ativo de Informação e Comunicação da UFERSA, seja eletrônico ou não, deve ser armazenado em meio que ofereça salvaguarda adequada e segurança;

IV. Todo Ativo de informação e Comunicação da UFERSA, se eletrônico, deve dispor de Cópia de Segurança atualizada regularmente e com frequência adequada; e,

V. Toda Cópia de Segurança deve, sempre que possível, ser mantida em lugar seguro e diferente do lugar onde o respectivo Ativo de Informação está localizado. O lugar escolhido deve garantir a segurança da cópia, caso alguma ameaça a que está sujeito o respectivo Ativo de Informação se concretize.

CAPITULO VIII
DA GESTÃO DE RISCO

Art. 14. Com relação à Gestão de Risco, que envolve o Inventariamento dos Ativos, Análise, Avaliação, Tratamento, Aceitação, Comunicação e Monitoramento dos Riscos, devem ser considerados os seguintes aspectos:

I. Os riscos associados aos Ativos devem ser avaliados e, se possível, minimizados;

II. Toda ação de segurança da informação deve ser feita com base na avaliação da criticidade
dos Ativos; e

III. Toda ação de segurança da informação deve respeitar a legislação vigente na UFERSA.

CAPITULO IX
DAS COMPETÊNCIAS E RESPONSABILIDADES

Art. 15. A Segurança da Informação assim como hábitos, posturas éticas, responsabilidade e cuidados com os ativos de informação devem ser responsabilidade de todos os usuários, de todos os setores da Instituição, não apenas da área e/ou profissionais de Tecnologia da Informação e comunicação (TIC).

Art. 16. Cabe a todos os usuários comunicar à Superintendência de Tecnologia da Informação e Comunicação da UFERSA (SUTIC) e/ou ao Comitê Gestor de Tecnologia da Informação da UFERSA (CGTI) e/ou ao Comitê de Governança Digital (CGD) a ocorrência de incidentes, a identificação de ameaças e vulnerabilidades, assim como qualquer transgressão desta POSIC.

Art. 17. A SUTIC é o setor primário de execução e verificação desta POSIC e, para tanto, deve ser suprida dos recursos materiais e humanos pela Instituição.

Art. 18. Cabe ao CGTI e ao CGD quanto à POSIC, homologar ações e processos da Instituição quanto à sua adequação, sugerir instrumentos complementares, realizar adequações e julgar infrações.

Art. 19. O CONSUNI é a entidade recursal ao julgamento de infrações à POSIC.

CAPITULO X
DAS PENALIDADES

Art. 20. O descumprimento ou violação da POSIC e demais normas e procedimentos estabelecidos relativos a ela, implicará penalidades, obedecidos aos ritos legais e em conformidade com o Regimento Geral da UFERSA.

Art. 21. Uma vez que a violação represente afronta à Legislação vigente no país, caracterizando crime ou contravenção, obriga-se a Administração Superior, a tomar as providências necessárias para que se cumpram as Leis.

CAPITULO XI
DA COMPOSIÇÃO E ATUALIZAÇÃO

Art. 22. A regulamentação da POSIC será composta deste documento, de demais Regulamentações, Normas, Portarias, Decisões, Instruções e outros documentos legalmente constituídos que a ela se refiram, emitidos ou homologados pelo CONSUNI.

Art. 23. Esta política e os instrumentos normativos gerados a partir dela devem ser revisados sempre que necessário, ou no mínimo, a cada 3 (três) anos.

CAPITULO XII
DA VIGÊNCIA

Art. 24. A regulamentação desta POSIC entrará em vigor na data de sua publicação, revogando-se as demais disposições em contrário.

Mossoró-RN, 15 de dezembro de 2017.

José de Arimatea de Matos
Presidente