Universidade Federal do Pampa
Conselho Universitário

RESOLUÇÃO Nº 83, DE 30 DE OUTUBRO DE 2014

O CONSELHO UNIVERSITÁRIO da Universidade Federal do Pampa, em sessão de 30/10/2014, no uso das atribuições que lhe são conferidas pelo Artigo 19, Inciso XVII do Estatuto da Universidade e considerando a Lei 9.394, de 20 de dezembro de 1996, a Resolução do CNE/CES 01, de 03 de abril de 2001, e a Resolução CNE/CES 24, de 18 de dezembro de 2002,

RESOLVE:

INSTITUIR A ESTRUTURA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES (ESIC).

CAPÍTULO I
DOS OBJETIVOS

Art. 1º São objetivos da Estrutura de Segurança da Informação e Comunicações (ESIC):

I. definir um Plano de Segurança da Informação e Comunicações (SIC) para a UNIPAMPA;

II. auxiliar a alta administração na priorização de ações e investimentos com vistas à correta aplicação de mecanismos de proteção, tendo como base as exigências estratégicas e as necessidades operacionais prioritárias da Instituição e as implicações que o nível de segurança pode trazer ao cumprimento dessas exigências;

III. planejar medidas de proteção e balancear os custos na aplicação de controles, de acordo com a análise dos riscos e impactos relacionados a possíveis falhas de segurança;

IV. registrar e tratar incidentes de SIC;

V. capacitar regularmente os membros da Estrutura da ESIC, com as especialidades das disciplinas relacionadas à SIC de acordo com suas funções.

CAPÍTULO II
DA COMPOSIÇÃO

Art. 2º Compõem a ESIC:

I. Gestor de Segurança da Informação e Comunicações (GSIC);

II. Comitê de Segurança da Informação e Comunicações (CSIC);

III. Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR).

~~Art. 3º Compõem o CSIC:~~

~~I. Vice-Reitor;~~

~~II. Gestor de Segurança da Informação e Comunicações;~~

~~III. Diretor do Núcleo de Tecnologia da Informação e Comunicações;~~

~~IV. Responsável pela consultoria jurídica;~~

~~V. Pró-Reitor de Gestão de Pessoal;~~

~~VI. Pró-Reitor de Planejamento ou representante de infraestrutura;~~

~~VII. um representante do Comitê Gestor de Tecnologia da Informação e Comunicações (CGTIC~~). (Alterado pela Resolução 220, de 25 de outubro de 2018)

Art. 3º Compõem o CSIC:

I. Reitor como Gestor de Segurança da Informação e Comunicações;

II. Diretor da Diretoria de Tecnologia da Informação e Comunicações;

III. Coordenador de Governança de TI da DTIC;

IV. Pró-Reitor de Extensão;

V. Pró-Reitor de Graduação;

VI. Pró-Reitor de Pesquisa, Pós-Graduação e Inovação;

VII. Pró-Reitor de Planejamento e Infraestrutura;

VIII 5 Diretores de Campus.

CAPÍTULO III
DAS COMPETÊNCIAS

Art. 4º Cabe ao Gestor de Segurança da Informação e Comunicações:

I. promover a cultura de segurança da informação e comunicações;

II. acompanhar as investigações e as avaliações dos danos decorrentes de incidentes de segurança;

III. propor recursos necessários às ações de SIC;

IV. coordenar o CSIC e a ETIR;

V. comunicar ao CSIC os resultados e outras informações pertinentes;

VI. realizar e acompanhar estudos de novas tecnologias quanto a possíveis impactos na SIC;

VII. manter contato permanente com o Departamento de Segurança da Informação e Comunicações (DSIC) do Gabinete de Segurança Institucional (GSI) da Presidência da República e com o Centro de Atendimento a Incidentes de Segurança (CAIS) da Rede Nacional de Pesquisa (RNP) para o trato de assuntos relativos à segurança da informação e comunicações;

VIII. propor normas relativas à SIC;

IX. promover a melhoria contínua nos processos e controles de SIC;

X. desenvolver um Plano de Conscientização em Segurança da Informação e Comunicações a fim de que todos os servidores da UNIPAMPA tenham ciência do assunto.

Art. 5º O Comitê de Segurança da Informação e Comunicações (CSIC) deve atender as disposição das normas:

I. Instrução Normativa GSI 01, de 13 de Junho de 2008;

II. Instrução Normativa GSI 02, de 05 de fevereiro de 2013;

III. Instrução Normativa GSI 03, de 06 de março de 2013;

IV. do Gabinete de Segurança Institucional da Presidência da República e das demais instruções normativas e normas complementares expedidas pelo GSI.

Parágrafo único. O Comitê possui caráter consultivo, propositivo e de apoio, estando vinculado diretamente à Reitoria da Universidade, sem subordinação hierárquica às demais pró-reitorias e direções de Campus.

Art. 6º Cabe ao CSIC:

I. normatizar e supervisionar a SIC no âmbito da UNIPAMPA;

II. constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre a SIC e realizar verificações de conformidade;

III. propor alterações na Política de Segurança da Informação e Comunicações (POSIC);

IV. solicitar apurações quando da suspeita de ocorrências de incidentes de SIC;

V. avaliar, revisar e analisar criticamente a POSIC e suas normas complementares, visando a sua aderência aos objetivos institucionais da UNIPAMPA e às legislações vigentes;

VI. dirimir eventuais dúvidas e deliberar sobre assuntos relativos à POSIC;

VII. aprovar o plano de investimentos em SIC;

VIII. monitorar e avaliar periodicamente o Plano de SIC, assim como determinar os ajustes cabíveis;

IX. definir e atualizar seu Regimento Interno;

X. instituir normas e procedimentos complementares a essa POSIC.

§1º O Comitê deve encaminhar ao CONSUNI as proposições com relação à POSIC e a outras normas relacionadas, visando garantir a representatividade da área técnica, administrativa e acadêmica.

§2º Após a aprovação, as Normas e Políticas devem ser publicadas no âmbito da Universidade, tornando-se de efeito imediato.

Art. 7º Cabe à ETIR:

I. facilitar e coordenar as atividades de tratamento e resposta a incidentes de segurança;

II. coordenar, executar e acompanhar a análise dos sistemas comprometidos buscando causas, danos e responsáveis;

III. coordenar, executar e acompanhar a avaliação, auditoria e testes das condições de segurança da rede corporativa;

IV. apoiar o desenvolvimento de um Plano de Conscientização em Segurança da Informação e Comunicações a fim de que todos os servidores da UNIPAMPA tenham ciência do assunto;

IV. manter em condições adequadas de segurança o acervo de informações relativas aos incidentes da rede corporativa;

V. participar da definição e acompanhar os indicadores de incidentes na rede corporativa;

VI. prestar assessoria técnica na elaboração de políticas, normas, pareceres e na especificação técnica de produtos e equipamentos em relação à segurança da informação e comunicação;

VII. agir proativamente com o objetivo de evitar que ocorram incidentes de segurança, divulgando práticas e recomendações de SIC e avaliando condições de segurança de redes por meio de verificações de conformidade;

IX. realizar ações reativas que incluem recebimento de notificações de incidentes, orientação de equipes no reparo a danos e análise de sistemas comprometidos, buscando causas, danos e responsáveis;

X. analisar e executar as ações necessárias para tratar incidentes de segurança;

XI. obter informações quantitativas acerca dos incidentes ocorridos que descrevam sua natureza, causas, data de ocorrência, frequência e custos resultantes;

XII. cooperar com outras equipes de Tratamento e Resposta a Incidentes;

XIII. participar em fóruns, redes nacionais e internacionais relativos à SIC;

XIV. executar outras atividades correlatas que lhe forem demandadas.

CAPÍTULO IV
DAS DIRETRIZES ESPECÍFICAS

Art. 8º Para cada uma das diretrizes constantes das seções deste capítulo, tais como o uso de recursos computacionais, da rede e política de e-mail, senhas e também o controle de circulação de pessoas e veículos devem ser elaboradas normas táticas específicas, manuais e procedimentos.

Seção I
Do Tratamento das Informações

Art. 9º Todo ativo de informação deve possuir um responsável explicitamente identificado.

Art. 10 Os ativos de informação da Instituição devem ser identificados, classificados de acordo com seu grau de severidade e documentados.

Art. 11 Seja qual for a forma ou o meio pelo qual a informação seja apresentada ou compartilhada, deve ser sempre protegida adequadamente de acordo com a POSIC.

Art. 12 Toda informação criada, manuseada, armazenada, transportada ou descartada deve ser classificada quanto aos aspectos de confidencialidade, integridade e disponibilidade, de forma explícita ou implícita.

Art. 13 A classificação e o tratamento de informação são:

I. norteados pela legislação específica que disponha sobre a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado, no âmbito da Administração Pública Federal (APF);

II. implementados e mantidos em conformidade com a legislação vigente, visando estabelecer os controles de segurança necessários a cada informação custodiada ou de propriedade da UNIPAMPA ao longo do seu ciclo de vida.

Seção II
Do Tratamento de Incidentes de Segurança da Informação

Art. 14 Os incidentes de segurança da informação devem ser registrados e gerenciados.

Art. 15 Deve ser definida uma equipe para tratamento e resposta aos incidentes em redes computacionais, segundo critérios a serem definidos pela área de Segurança da Informação, a fim de receber, analisar e responder às notificações e atividades relacionadas aos incidentes de segurança em redes computacionais na Instituição.

Seção III
Da Gestão de Riscos e Continuidade

Art. 16 Deve ser adotada a gestão de riscos de segurança da informação, segundo critérios a serem definidos pela ESIC, para a identificação e implementação das medidas de proteção necessárias à mitigação ou eliminação dos riscos.

Art. 17 Deve ser adotada a gestão de continuidade de negócios em segurança da informação, segundo critérios a serem definidos pela ESIC, visando minimizar os impactos decorrentes de falhas, desastres ou indisponibilidades significativas, através de ações de prevenção, resposta e recuperação dos ativos que sustentam os processos críticos da Instituição.

Seção IV
Do Controle de Acesso

Art. 18 Todo acesso à informação que não seja de domínio público se dá através de mecanismos de identificação e controle de acesso.

§1º Qualquer mudança funcional implica na revisão dos direitos de acesso à informação;

§2º O usuário deve ter pleno conhecimento das diretrizes, responsabilidades, limitações e penalidades relacionadas à utilização dos recursos de informação, inclusive por ocasião da mudança de atividades.

Art. 19 O ambiente que contenha ativos de informação deve ser protegido de acordo com sua severidade.

Art. 20 No gerenciamento de operações e comunicações deve-se garantir a operação segura e correta dos recursos de processamento da informação e das comunicações.

Seção V
Da Aquisição, do Desenvolvimento e da Manutenção de Sistemas

Art. 21 A ESIC deve estabelecer critérios e metodologia de segurança para desenvolvimento de sistemas de informação, de forma a abranger todas as fases do ciclo de vida dos sistemas.

Parágrafo único. O desenvolvimento de sistemas de informação deve ser realizado com base em uma Metodologia de Desenvolvimento de Sistemas alinhada em requisitos de segurança reconhecidos.

Art. 22 O processo de aquisição de sistemas e aplicações corporativas deve atender requisitos de segurança previstos em norma específica.

Parágrafo único. Todos os sistemas de informação adquiridos ou desenvolvidos devem respeitar as diretrizes da POSIC.

Seção VI
Da Segurança da Informação em Recursos Humanos

Art. 23 A ESIC deve assegurar que alunos, professores, técnico-administrativos, fornecedores e terceiros entendam suas responsabilidades e estejam de acordo com os seus papéis, reduzindo o risco da ocorrência de incidentes de segurança no âmbito da Universidade, utilizando para tal as seguintes metas:

I. definir papéis e responsabilidades;

II. definir termos e condições de execução de atividades no âmbito da Universidade;

III. conscientizar, educar e qualificar em Segurança da Informação;

IV. definir processos disciplinares;

V. conceder e restringir acesso aos ativos de informação;

VI. definir processos para devolução de ativos e revogação de privilégios.

Art. 24 Esta Resolução entra em vigor na data da sua aprovação.

ULRIKA ARNS
Reitora