MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL DE SANTA MARIA

RESOLUÇÃO N. 009/2013

Aprova o Regulamento da Política de Segurança da Informação e Comunicações – PoSIC da Universidade Federal de Santa Maria.

O REITOR DA UNIVERSIDADE FEDERAL DE SANTA MARIA, no uso de suas atribuições legais e estatutárias e considerando:

– a necessidade de instituir diretrizes e princípios de Segurança da Informação e Comunicações (SIC), com o propósito de limitar a exposição ao risco a níveis aceitáveis e garantir a disponibilidade, a integridade, a confidencialidade e a autenticidade (DICA) das informações que suportam os objetivos estratégicos da Universidade Federal de Santa Maria; e

– o Parecer n. 038/2013 da Comissão de Legislação e Regimentos (CLR), aprovado na 745ª Sessão do Conselho Universitário, de 27 de março de 2013, referente ao Processo n. 23081.002079/2013-89.

RESOLVE:

Art. 1º Aprovar o Regulamento da Política de Segurança da Informação e Comunicações (PoSIC), no âmbito da Universidade Federal de Santa Maria.

Art. 2º Esta resolução entrará em vigor na data de sua assinatura, revogadas as disposições em contrário.

GABINETE DO REITOR DA UNIVERSIDADE FEDERAL DE SANTA MARIA, aos dois dias do mês de abril do ano dois mil e treze.

Felipe Martins Müller,
Reitor.

MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL DE SANTA MARIA

REGULAMENTO DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES – PoSIC

CAPÍTULO I
DO OBJETIVO

Art. 1º A Política de Segurança da Informação e Comunicações – PoSIC tem por objetivo instituir diretrizes e princípios de Segurança da Informação e Comunicações (SIC) no âmbito da Universidade Federal de Santa Maria, com o propósito de limitar a exposição ao risco a níveis aceitáveis e garantir a disponibilidade, a integridade, a confidencialidade e a autenticidade (DICA) das informações que suportam os objetivos estratégicos da Instituição.

CAPÍTULO II
DA REFERÊNCIA NORMATIVA

Art. 2º São referências normativas básicas para elaboração desta política:

I – Associação Brasileira de Normas Técnicas. ABNT NBR ISO/IEC 17799:2005 (27002). Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação;

II – Constituição da República Federativa do Brasil, de 1988;

III – Decreto n. 1.171, de 22 de junho de 1994, que dispõe sobre o Código de Ética Profissional do Servidor Público Civil, do Poder Executivo Federal;

IV – Decreto n. 3505, de 13 de junho de 2000, que institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal;

V – Decreto n. 4.553, de 27 de dezembro de 2002, que dispõe 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;

VI – Instrução Normativa GSI n. 01, de 13 de junho de 2008, que disciplina a Gestão de Segurança da Informação e Comunicações, na Administração Pública Federal, direta e indireta e demais normas complementares; e

VII – Lei n. 8.112, de 11 de dezembro de 1990, que dispõe sobre o regime jurídico dos servidores públicos civis da União, das autarquias e das fundações públicas federais.

CAPÍTULO III
DA ABRANGÊNCIA

Art. 3º A Política de Segurança da Informação e Comunicações – PoSIC e suas normas complementares aplicam-se a todas as unidades e subunidades da UFSM, bem como aos docentes, discentes, técnico-administrativos em educação, colaboradores terceirizados, estagiários e a quem de alguma forma tenha acesso aos ativos de informação da Instituição.

CAPÍTULO IV
DOS PRINCÍPIOS

Art. 4º O conjunto de documentos que compõe esta PoSIC deverá ser orientado pelos seguintes princípios:

I – Menor privilégio: Usuários e sistemas devem ter a menor autoridade e o mínimo acesso aos recursos necessários para realizar uma determinada tarefa;

II – Segregação de função: Funções de planejamento, execução e controle devem ser segregadas de forma a reduzir as oportunidades de modificação, o uso indevido, e a não autorização ou não intencionalidade dos ativos;

III – Auditabilidade: Todos os eventos significantes de sistemas e processos devem ser rastreáveis até o evento inicial;

IV – Mínima dependência de segredos: Os controles deverão ser efetivos ainda que a ameaça saiba de suas existências e como eles funcionam;

V – Controles automáticos: Sempre que possível, controles de segurança automáticos deverão ser utilizados, especialmente os controles que dependem da vigilância humana e do comportamento humano;

VI – Resiliência: Os sistemas e processos devem ser projetados para que possam resistir ou realizar a recuperação dos efeitos de um desastre;

VII – Defesa em profundidade: Os controles devem ser desenhados em camadas de tal forma que quando uma camada de controle falhar, exista um tipo diferente de controle em outra camada para prevenir a brecha de segurança;

VIII – Exceção aprovada: Exceções à PoSIC deverão sempre ter aprovação superior;

IX – Substituição da segurança em situações de emergência: Os controles somente devem ser desconsiderados de formas predeterminadas e seguras, sendo que deve sempre existir procedimentos e controles alternativos para minimizar o nível de risco em situações de emergência; e

X – Esta PoSIC deverá estar, também, em conformidade com os princípios constitucionais e administrativos que regem a Administração Pública Federal, bem como aos demais dispositivos legais aplicáveis.

CAPÍTULO V
DAS DIRETRIZES GERAIS

Art. 5º As diretrizes de SIC devem considerar, prioritariamente, os requisitos legais, os objetivos estratégicos, e a estrutura e finalidade da UFSM.

Art. 6º Os custos associados à Gestão da SIC deverão ser compatíveis com os custos dos ativos que se deseja proteger.

Art. 7º A Gestão de SIC deve suportar a tomada de decisões, bem como realizar a gestão de conhecimento e de recursos por meio da utilização eficiente e eficaz dos ativos, possibilitando alcançar os objetivos estratégicos da UFSM, assim como, otimizar seus investimentos.

Art. 8º As normas e procedimento de SIC da UFSM devem considerar, subsidiariamente, normas e padrões aceitos no mercado como referência nos processos de gestão e governança de SIC.

Art. 9º São normas e padrões relacionados à gestão de ativos:

I – Os ativos de informação da Instituição são elementos fundamentais para a consecução dos objetivos estratégicos, portanto ações de segurança específicas deverão garantir a proteção adequada dos mesmos, sendo que os níveis de proteção deverão variar de acordo com a criticidade do ativo para a Instituição;

II – Os ativos de informação devem ter controles de segurança implementados independentemente do meio em que se encontram e deverão ser protegidos contra divulgação não autorizada, modificações, remoção ou destruição, de forma a evitar incidentes de segurança que possam danificar a imagem da instituição e interromper suas operações;

III – As pessoas, que, de alguma maneira tenham acesso aos ativos de informação da instituição, devem ser periodicamente conscientizadas, capacitadas e sensibilizadas em assuntos de segurança e de tratamento da informação, de forma a garantir o entendimento e a prática efetiva da SIC; e

IV – Os processos e atividades que sustentam os serviços críticos disponibilizados pela UFSM devem ser protegidos de forma a garantir a disponibilidade, a integridade, a confidencialidade e a autenticidade (DICA) das informações.

Art. 10. A gestão de riscos tem como objetivo reduzir as vulnerabilidades, evitar as ameaças, minimizar a exposição aos riscos e atenuar os impactos associados aos ativos da organização, sendo que deverá ser estabelecido processo que possibilite a identificação, a quantificação, a priorização, o tratamento, a comunicação e a monitoração periódica dos riscos.

Art. 11. São normas e padrões relacionados à gestão de operações e comunicações:

I – Dada a importância estratégica que os recursos de processamento da informação têm para a consecução dos objetivos da UFSM, ações de segurança deverão garantir a operação segura e correta desses recursos;

II – As interfaces com terceiros são importantes canais de informação que, sem um nível de segurança adequado, poderão levar a Instituição a uma elevada exposição a riscos tendo como objetivo de reduzir os riscos associados, o gerenciamento dos serviços terceirizados deverá manter os níveis apropriados de segurança da informação e da entrega dos serviços;

III – A troca de informações, tanto internamente, quanto externamente, deverão ser reguladas de forma a manter o nível adequado da segurança; e

IV – As operações deverão ser adequadamente monitoradas visando detectar o mais breve possível atividades não autorizadas.

Art. 12. São normas e padrões relacionados ao controle de acessos:

I – Com o objetivo de evitar a quebra de segurança, devem ser instituídas normas ou procedimentos que garantam o controle de acesso às informações e instalações;

II – A concordância expressa e por escrito aos preceitos desta PoSIC é condição necessária para o acesso aos ativos de informação da UFSM; e

III – Devem ser instituídas normas e procedimentos que garantam a segurança da informação em ambientes de computação móvel e de trabalho remoto, considerando que ambientes de computação móvel e de trabalho remoto são necessários para a consecução das atividades da UFSM e que podem consistir em pontos fracos do sistema de gestão de segurança.

Art. 13. Com relação à gestão de incidentes de segurança da informação, os mesmos devem ser identificados, monitorados, comunicados e devidamente tratados, em tempo hábil, de forma a garantir a continuidade das atividades e a não intervenção no alcance dos objetivos estratégicos da UFSM.

Art. 14. Com relação à gestão de continuidade do negócio, ressalta-se que a interrupção das atividades da UFSM leva à suspensão de serviços críticos prestados ao

cidadão e poderá resultar em grave dano à imagem da organização, portanto, deverão ser instituídas normas e procedimentos que estabeleçam a Gestão de Continuidade do Negócio para minimizar os impactos decorrentes de eventos que causem a indisponibilidade sobre os serviços da UFSM, além de recuperar perdas de ativos de informação a um nível estabelecido, por intermédio de ações de prevenção, resposta e recuperação.

CAPÍTULO VI
DA CONFORMIDADE

Art. 15. O cumprimento desta política de segurança deverá ser avaliado periodicamente por meio de verificações de conformidade realizadas pela Administração Superior, que poderá solicitar o apoio de entidades externas e independentes.

Art. 16. Os controles de SIC devem ser analisados criticamente e verificados em períodos regulares, tendo por base as conformidades com políticas, padrões, normas, ferramentas, manuais de procedimentos e outros documentos pertinentes.

Art. 17. De forma a obter o absoluto cumprimento destes instrumentos legais e normativos, devem ser instituídos processos de análise e tratamento de conformidade, visando garantir o atendimento das leis, regulamentos e normas que regem as atividades no âmbito da Administração Pública Federal.

CAPÍTULO VII
DAS RESPONSABILIDADES

Art. 18. É de responsabilidade da Administração Superior desta Instituição prover a orientação e o apoio necessários às ações de SIC, de acordo com os objetivos estratégicos e com as leis e regulamentos pertinentes.

Art. 19. É de responsabilidade dos demais gestores zelar pelo cumprimento das diretrizes desta política no âmbito de suas áreas de atuação.

Art. 20. É de responsabilidade de todos que têm acesso aos ativos de informação da UFSM manter níveis de segurança da informação adequados, segundo preceitos desta política e de suas normas complementares.

Art. 21. Deverá ser instituído, por portaria específica, o Comitê Gestor de Segurança da Informação e Comunicações (CGSIC) da UFSM.

Art. 22. Os membros do Comitê deverão receber regularmente capacitação especializada em segurança da informação e comunicações.

Art. 23. São atribuições e forma de funcionamento do Comitê Gestor de Segurança da Informação e Comunicações:

I – assessorar na implementação das ações de SIC;

II – promover a cultura de segurança da informação e comunicações;

III – constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre a SIC;

IV – propor alterações na PoSIC;

V – elaborar instruções normativas complementares relativas à SIC;

VI – dirimir eventuais dúvidas sobre assuntos relativos à PoSIC;

VII – acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança;

VIII – propor à Administração Superior investimentos em ações de segurança da informação e comunicações;

IX – realizar e acompanhar estudos e novas tecnologias, quanto a possíveis impactos na segurança da informação e comunicações; e

X – regular os processos de gestão relacionados a SIC.

Art. 24. Os níveis adequados de segurança dos ativos de informação deverão ser garantidos pelos seus usuários diretamente responsáveis.

CAPÍTULO VIII
DAS PENALIDADES

Art. 25. Ações que violem a PoSIC ou que quebrem os controles de segurança da informação e comunicações serão passíveis de sansões civis, penais e administrativas, conforme a legislação em vigor, que podem ser aplicadas isoladamente ou cumulativamente.

Art. 26. Para apurar as ações que constituem em quebra das diretrizes impostas por esta PoSIC, deverá ser elaborado um processo disciplinar específico.

CAPÍTULO IX
DA ATUALIZAÇÃO

Art. 27. Esta PoSIC, bem como os documentos gerados a partir dela, deverão ser revisados e atualizados sempre que houver alterações na legislação específica.

CAPÍTULO X
DA VIGÊNCIA

Art. 28. Esta Política entra em vigor na data de sua publicação.

CAPÍTULO XI
DAS DISPOSIÇÕES GERAIS

Art. 29. Esta PoSIC, bem como as normas e procedimentos de SIC associados, deverão ter ampla divulgação, de forma a garantir que todos entendam suas responsabilidades e ajam de acordo com os preceitos desta Política.

ANEXO I
DOS CONCEITOS E DEFINIÇÕES

São conceitos e definições utilizados na elaboração desta política:

I – Acesso: ato de ingressar, transitar, conhecer ou consultar a informação, bem como a possibilidade de usar os ativos de informação de um órgão ou entidade [NC07/IN01/DSIC/GSIPR, 2010, p. 2];

II – Ameaça: conjunto de fatores externos ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização;

III – Ativo: tudo aquilo que possui valor para o órgão ou entidade da Administração Pública Federal;

IV – Ativos de Informação: os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso [NC04/IN01/DSIC/GSIPR, 2009, p. 2];

V – 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 [IN01/DSIC/GSIPR, 2008, p. 2];

VI – Capacitação em SIC: saber o que é segurança da informação e comunicações aplicando em sua rotina pessoal e profissional, servindo como multiplicador sobre o tema, aplicando os conceitos e procedimentos na Organização como gestor de SIC [DSIC/GSIPR];

VII – Capacitação: visa a aquisição de conhecimentos, capacidades, atitudes e formas de comportamento exigidos para o exercício das funções;

VIII – Comitê Gestor de Segurança da Informação e Comunicações: grupo de pessoas com a responsabilidade de assessorar e coordenar a implementação das ações de segurança da informação e comunicações [NC03/IN01/DSIC/GSIPR];

IX – Confidencialidade: propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizado e credenciado [IN01/DSIC/GSIPR, 2008, p. 2];

X – Conscientização em SIC: saber o que é segurança da informação e comunicações aplicando em sua rotina pessoal e profissional, além de servir como multiplicador sobre o tema [DSIC/GSIPR];

XI – Continuidade de Negócios: capacidade estratégica e tática de um órgão ou entidade de se planejar e responder a incidentes e interrupções de negócios, minimizando seus impactos e recuperando perdas de ativos da informação das atividades críticas, de forma a manter suas operações em um nível aceitável, previamente definido [NC06/IN01/DSIC/GSIPR, 2009, p.3];

XII – Controle de Acesso: conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso [NC07/DSIC/GSIPR, 2010, p. 3];

XIII – Disponibilidade: propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade [IN01/DSIC/GSIPR, 2008,p. 2];

XIV – Evento: ocorrência identificada de um sistema, serviço ou rede, que indica uma possível violação da política de segurança da informação ou falha de controles, ou uma situação previamente desconhecida, que possa ser relevante para a segurança da informação. [ISO/IEC TR 18044:2004];

XV – Gestão de Riscos de Segurança da Informação e Comunicações: conjunto de processos que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação, e equilibrá-los com os custos operacionais e financeiros envolvidos [NC04/IN01/DSIC/GSIPR, 2009, p.2];

XVI – Gestão de Segurança da Informação e Comunicações: ações e métodos que visam à integração das atividades de gestão de riscos, gestão de continuidade do negócio,

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 e comunicações [IN01/DSIC/GSIPR, 2008, p. 2];

XVII – Gestor de Segurança da Informação e Comunicações: é responsável pelas ações de segurança da informação e comunicações no âmbito do órgão ou entidade da APF [IN01/DSIC/GSIPR, 2008, p. 2];

XVIII – Incidente de segurança: é qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores [NC05/IN01/DSIC/GSIPR, 2009, p. 3];

XIX – Integridade: propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental [IN01/DSIC/GSIPR, 2008, p. 2];

XX – Nível de Segurança Adequado: será estabelecidos em documentos complementares a esta PoSIC;

XXI – Política de Segurança da Informação e Comunicações (PoSIC): documento aprovado pela autoridade responsável do órgão ou entidade da Administração Pública Federal – APF, com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da segurança da informação e comunicações [NC03/IN01/DSIC/GSIPR, 2009, p. 2];

XXII – Terceiro: pessoa, não integrante do órgão ou entidade da APF, envolvida com o desenvolvimento de atividades, de caráter temporário ou eventual, exclusivamente para o interesse do serviço, que poderão receber credencial especial de acesso [NC07/DSIC/GSIPR, 2010, p. 3];

XXIII – Proprietário da Informação: pessoa ou setor que produz a informação;

XXIV – Quebra de Segurança: ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação e das comunicações [IN01/DSIC/GSIPR,2008, p. 2];

XXV – Riscos de Segurança da Informação e Comunicações: potencial associado à exploração de uma ou mais vulnerabilidades de um ativo de informação ou de um conjunto de tais ativos, por parte de uma ou mais ameaças, com impacto negativo no negócio da organização [NC04/IN01/DSIC/GSIPR, 2009, p.3];

XXVI – Segurança da Informação e Comunicações: ações que objetivam viabilizar e assegurar à disponibilidade, a integridade, a confidencialidade e a autenticidade das informações [IN01/DSIC/GSIPR, 2008, p. 2];

XXVII – Segurança de Operações e Comunicações: responsável pela manutenção do funcionamento de serviços, sistemas e da infraestrutura que os suporta;

XXVIII – Usuário: servidores, terceirizados, colaboradores, consultores, auditores e estagiários que obtiveram autorização do responsável pela área interessada para acesso aos ativos de informação de um órgão ou entidade da APF, formalizada por meio da assinatura do Termo de Responsabilidade [NC07/DSIC/GSIPR, 2010, p. 3]; e

XXIX – Vulnerabilidade: conjunto de fatores internos ou causa potencial de um incidente indesejado, que podem resultar em risco para um sistema ou organização, os quais podem ser evitados por uma ação interna de segurança da informação NC04/IN01/DSIC/GSIPR, 2009, p.3].