Universidade Federal de Santa Catarina

Política de Segurança da Informação e Comunicações (POSIC)

Documento elaborado pelo Comitê de Segurança da Informação e Comunicação (COSIC) instituído pela Portaria No. 1754/2015/GR – 09/10/2015.

Integrantes do COSIC:

Ricardo Alexandre Reinaldo de Moraes – campus Araranguá

Jean Everson Martina – Departamento de Informática e Estatística/CTC

Joni da Silva Fraga – Departamento de Automação e Sistemas/CTC

Káthia Regina Lemos Jucá – Coordenadoria de Certificação Digital da Sala Cofre - CCD/PROPLAN

Rodrigo Gonçalves – SeTIC/PROPLAN

Carlos Alberto Moresco – SeTIC/PROPLAN

Aprovações

Data de Aprovação pelo COSIC: 25/04/2016

Data de Aprovação pelo COTIC: 02/05/2016

Data de encaminhamento ao CUn: xx/xx/2016

Data de Aprovação pelo CUn: xx/xx/xxxx

Data de Publicação: xx/xx/xxxx

Ciclo de Revisões: Bianual

CAPÍTULO I

DAS DISPOSIÇÕES PRELIMINARES

Art. 1º Fica estabelecida a Política de Segurança da Informação e Comunicações da Universidade Federal de Santa Catarina (POSIC/UFSC), contendo os princípios, objetivos e diretrizes a serem observadas no âmbito desta Universidade.

Parágrafo único. Servidores, estudantes, colaboradores e quaisquer pessoas que tenham acesso a informações da UFSC sujeitam-se às diretrizes, normas e procedimentos de segurança da informação e comunicações da Política de que trata este documento, e são responsáveis por garantir a segurança das informações a que tenham acesso.

Art. 2º Para os efeitos deste documento, entende-se por:

I. Política de segurança da informação e comunicações (POSIC): recomendações e regras com o propósito de estabelecer critérios para o adequado manuseio, armazenamento, transporte e descarte de informações no âmbito da UFSC, através do desenvolvimento de Diretrizes, Normas, Procedimentos e Instruções destinadas, respectivamente, aos níveis estratégico, tático e operacional;

II. Princípios de segurança da informação e comunicações: princípios que visam a implementação das propriedades de confidencialidade, integridade, disponibilidade e autenticidade que regem a segurança da informação, de acordo com o art. 3° do Decreto n° 3.505, de 13 de junho de 2000;

III. COSIC: Comitê de Segurança da Informação e Comunicação, que foi instituído com o objetivo de complementar o arcabouço da governança da Tecnologia da Informação e Comunicação no que tange à segurança da informação;

IV. Grupo Gestor de Segurança da Informação e Comunicações: instância executiva responsável pela implementação da POSIC da UFSC;

V. Disponibilidade: é a garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes, sempre que necessário.

VI. Integridade: é a garantia de que a informação não é modificada ou destruída de maneira não autorizada ou acidental. Salvaguardando a exatidão e correção da informação e dos métodos de processamento;

VII. Confidencialidade: é a garantia de que a informação é acessível somente a pessoas físicas, sistemas, órgãos ou entidades autorizadas e credenciadas;

VIII. Autenticidade: é a propriedade que responsabiliza e garante a associação da informação produzida, expedida, modificada ou destruída a determinada pessoa física, ou a um sistema, órgão ou entidade;

IX. Ativos: é tudo que manipula, processa ou corresponde à informação, tais como base de dados, arquivos, documentação do sistema, manuais, material de treinamento, procedimentos de suporte ou operação, planos de continuidade, procedimentos de recuperação, softwares, sistemas, ferramentas de desenvolvimento e utilitários, estações de trabalho, servidores, equipamentos de comunicação e outros;

X. Termo de responsabilidade: acordo entre partes que visa manter as propriedades de segurança das informações, atribuindo responsabilidades aos usuários, colaboradores e administrador de serviços quanto ao sigilo e a correta utilização dos ativos e das informações de propriedade ou custodiados pela UFSC.

CAPÍTULO II

DOS PRINCÍPIOS E DO ESCOPO

Art. 3º A Segurança da Informação e Comunicações da UFSC abrange aspectos físicos, tecnológicos e humanos da organização e orienta-se pelos seguintes princípios:

I. garantia da integridade, da autenticidade e da disponibilidade das informações;

II. proteção adequada das informações de acordo com a necessidade de restrição de acesso;

III. planejamento das ações para manter a segurança da informação;

IV. transparência das informações públicas de acordo com a legislação vigente.

Art. 4º A Política de Segurança da Informação e Comunicações deve ser aplicada em toda a Universidade e abrange:

I. aspectos estratégicos, estruturais e organizacionais;

II. requisitos de segurança humana, física e lógica que sustentam os procedimentos, os processos de negócio e dos ativos da informação utilizados nos serviços oferecidos pela UFSC.

CAPÍTULO III

DOS DEVERES E DAS RESPONSABILIDADES

Art. 5º O COSIC tem por finalidade:

I. elaborar, avaliar e rever periodicamente a POSIC – em consonância com o Plano Diretor de Tecnologia da Informação e Comunicação (PDTI) da UFSC;

II. assessorar o Comitê de Tecnologia da Informação e Comunicação (COTIC) em matérias relativas a Segurança da Informação e Comunicações;

III. manifestar-se sobre matérias de segurança da informação que lhe sejam submetidas;

IV. propor e revisar as normas e procedimentos inerentes à segurança da informação e avaliar regularmente a sua aplicação;

V. propor ações permanentes de divulgação, treinamento, educação e conscientização sobre políticas, normas e procedimentos que promovam a segurança da informação.

Art. 6. É dever dos servidores, estudantes, colaboradores e quaisquer pessoas que tenham acesso a informação da UFSC:

I. zelar por suas credencias pessoais de acesso, responsabilizando-se pelo seu uso;

II. respeitar as políticas de segurança da informação. O acesso às informações deve ser permitido exclusivamente para pessoas devidamente autorizadas;

III. utilizar os ativos e as informações somente para o desempenho das suas atividades administrativas, de ensino, pesquisa e extensão;

IV. aceitar o Termo de Responsabilidade (TR), atestando o conhecimento da existência de políticas de segurança desta Universidade;

V. colaborar com o grupo gestor de segurança da informação e comunicações, informando possíveis anomalias referentes a segurança da informação de que tenham ciência ou suspeita;

Art. 7. O grupo gestor de segurança da informação e comunicações será composto pelo gestor de segurança da informação e equipe, que devem atender as seguintes atribuições:

I. Desenvolver ações para a melhoria contínua da segurança dos serviços e sistemas de TIC da UFSC em conformidade com:

   a. Leis e normas nacionais e internacionais;

   b. Políticas e normas institucionais.

II. Propor normas e procedimentos associados a segurança dos Ativos;

III. Promover a aplicação de políticas, normas e procedimentos associados a segurança dos Ativos;

IV. Promover cultura de segurança da informação e comunicações;

V. Propor recursos necessários às ações de segurança da informação e comunicações;

VI. Acompanhar as investigações e as avaliações dos incidentes de segurança;

VII. Promover e acompanhar estudos de novas tecnologias, quanto a possíveis impactos na segurança da informação e comunicações;

VIII. Manter contato permanente com o COSIC e o COTIC para o trato de assuntos relativos à segurança da informação e comunicações;

CAPÍTULO IV

DAS SANÇÕES E PENALIDADES

Art. 8. Em caso de descumprimento de termos estabelecidos por este documento, serão aplicadas as sanções e penalidades previstas na legislação vigente e nas regulamentações internas da UFSC.

CAPÍTULO V

DAS DISPOSIÇÕES FINAIS

Art. 9. A POSIC deverá ser publicada e amplamente divulgada, garantindo que a comunidade universitária tenha conhecimento da mesma.

Art. 10. Os Instrumentos normativos gerados a partir da POSIC, incluindo a própria POSIC devem ser revisados sempre que se fizer necessário, não excedendo o período máximo de 02 (dois) anos.

Art. 11. Os casos omissos neste documento serão analisados pelo COTIC ouvido o COSIC.

Referência Legais e Normativas

1. Art. 6° da Lei n° 10.683, de 28 de maio de 2003.
2. Art. 8° do Anexo I do Decreto n° 5.772, de 8 de maio de 2006.
3. Decreto n° 3.505, de 13 de junho de 2000.
4. Instrução Normativa n° 01 do Gabinete de Segurança Institucional, de 13 de junho de 2008.
5. NBR ISO-IEC 27001:2006.
6. NBR ISO-IEC 27002:2007.
7. Decreto n° 1048, de 21 de janeiro de 1994.
8. Decreto de 18 de outubro de 2000 - Governo Eletrônico.
9. Decreto n° 4553, de 27 de dezembro de 2002.
10. Art 5° Inciso III da Instrução Normativa n° 04 da Secretaria de Logística e Tecnologia da Informação/MPOG, de 19 de maio de 2008.
11. e-PING - Padrões de Interoperabilidade de Governo Eletrônico, de 16 de dezembro de 2008.
12. Lei 12.527, de novembro de 2011.