Política de Segurança da Informação e Comunicações (POSIC)

Versão 1.0 (outubro 2018)

CAPÍTULO I DAS DISPOSIÇÕES PRELIMINARES

Art. 1º Fica estabelecida a Política de Segurança da Informação e Comunicações da Universidade do Estado de Santa Catarina (POSIC/UDESC), 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 UDESC 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 UDESC, 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;

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 UDESC;

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 UDESC.

CAPÍTULO II DOS PRINCÍPIOS E DO ESCOPO

Art. 3º A Segurança da Informação e Comunicações da UDESC 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 UDESC 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 UDESC.

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 UDESC;

II. Assessorar o Comitê de Gestor de Tecnologia da Informação e Comunicação (CGTIC) em matérias relativas à 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 UDESC:

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 UDESC 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;

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

III. Promover cultura de segurança da informação e comunicações;

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

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

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

VII. Manter contato permanente com o COSIC e o CGTIC 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 UDESC.

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 CGTIC ouvido o COSIC.

Referência Legais e Normativas

1.Instrução Normativa nº 01 do Gabinete de Segurança Institucional, de 13 de junho de 2008.
2. NBR ISO-IEC 27001:2006. 6.
3. NBR ISO-IEC 27002:2007.
4. e-PING - Padrões de Interoperabilidade de Governo Eletrônico, de 16 de dezembro de 2008.