1. Propósito

Determinar as práticas referentes aos processos de aquisição e desenvolvimento interno de sistemas.

2. Escopo

Esta norma trata de pontos relevantes em relação a qualquer software utilizado pela ALCE, seja ele software básico ou de apoio, adquirido de terceiros ou desenvolvido internamente.

3. Política

3.1. Responsabilidade

É de responsabilidade da Área de Tecnologia o recebimento de requisições de soluções tecnológicas, ficando sob sua responsabilidade a avaliação das demandas, viabilidade tecnológica e econômico-financeira e aquisição de sistemas de acordo com esta norma.

É vedado a outras áreas da ALCE a contratação direta de sistemas e/ou soluções tecnológicas sem que o processo de avaliação aprovado pela Área de Tecnologia da Informação.

3.2. Perfis de Acesso

As soluções adquiridas ou desenvolvidas internamente devem dispor de recursos para aplicar a Norma de Controle de Acesso a Sistemas e Informações.

3.3. Trilhas de Auditoria

Os sistemas devem manter um registro de usuários que realizaram acesso e ações realizadas, permitindo a identificação de usuários responsáveis por ações críticas no sistema e comprovação dos acessos realizados.

3.4. Validação de Entrada de Dados e Falhas de Código

Todos os aplicativos de negócio, que armazenem ou processem informações sigilosas da ALCE ou de sua responsabilidade ou que estejam publicamente acessíveis via Internet devem, obrigatoriamente, ser protegidos quanto ao fornecimento de dados inválidos pelo usuário ou eventuais falhas de código que possam gerar ações imprevistas e possíveis incidentes de segurança.

3.5. Armazenamento e transmissão de informações sigilosas

As informações sigilosas, assim eleitas conforme a Norma de Classificação de Informações em vigor, devem ser protegidas ao serem armazenadas, ou ao transitarem entre funcionalidades da mesma aplicação ou entre aplicações distintas.

3.6. Isolamento de recursos considerados críticos

Aplicações consideradas críticas, onde eventuais incidentes de segurança possam impactar a operação ou causar prejuízos financeiros, legais ou à imagem da ALCE, devem ser adequadamente isoladas e protegidas visando minimizar a probabilidade de ocorrência de problemas bem como seu impacto caso venham a acontecer.

4. Sanções

Qualquer colaborador que violar esta norma estará sujeito a ações disciplinares, conforme previsto no NC-013 - Manual de Sanções Administrativas.

5. Aprovação

Este documento foi aprovado em 16/08/2013 pela Presidência e é válido a partir da data de sua publicação para todos os colaboradores que utilizam recursos computacionais.

6. Definições

7. Histórico de Revisão

01/06/2012 – Criação da Norma