INSTITUTO ÁRIA

POLÍTICA DE AQUISIÇÃO E DESENVOLVIMENTO DE SISTEMAS

Brasília/DF

POLÍTICA DE AQUISIÇÃO E DESENVOLVIMENTO DE SISTEMAS

TÍTULO I

DA POLÍTICA DE AQUISIÇÃO E DESENVOLVIMENTO DE SISTEMAS DA AUDEN

CAPÍTULO I - DO OBJETIVO

O objetivo desta política é definir requisitos de segurança da informação para aquisição, desenvolvimento, implementação e manutenção dos sistemas e serviços de informação do Instituto Ária com acesso aos ativos de informações da instituição.

A segurança deve ser integrada ao ciclo de vida de gestão de projetos, incluindo atividades como desenvolvimento, aquisição e integração de aplicativos.

Os requisitos de segurança devem ser definidos na fase inicial de um projeto e, em seguida, implementados e testados em todo o ciclo de vida do projeto para assegurar a conformidade com as políticas de segurança.

CAPÍTULO II - DO ESCOPO

Esta política se aplica a todos os sistemas e/ou serviços de informações da Faculdade com acesso aos ativos de informações da instituição, independentemente de eles serem comprados diretamente pelo negócio ou pela TI da Faculdade.

Esta política se destina ainda a colaboradores da Faculdade e a terceiros com acesso aos sistemas de informações, informações ou ativos de informações da instituição.

TÍTULO II

DA DECLARAÇÃO DA POLÍTICA DE AQUISIÇÃO E DESENVOLVIMENTO DE SISTEMAS

CAPÍTULO I - DAS FUNÇÕES E RESPONSABILIDADES

- **Segurança da informação**: responsável pela análise e aprovação de controles de segurança do novo sistema.
- **Proprietário da informação**: responsável pela gestão do ciclo do sistema de informações. Trabalha com o gestor de segurança da informação e o Depositário das informações no desenvolvimento do plano de segurança para o sistema e supervisiona a implementação de quaisquer controles de segurança do sistema em conformidade com as políticas de segurança da informação.
- **Depositário das informações**: assegura a aplicação dos controles de segurança operacionais apropriados para o sistema de informações; trabalha com o Diretor de segurança da informação na identificação, implementação e avaliação de controles de segurança comuns; participa do desenvolvimento e atualização do plano de segurança do sistema e trabalha com o proprietário do sistema de informação em quaisquer alterações no sistema. Trabalha com a Segurança da informação na avaliação do impacto à segurança de quaisquer mudanças.

CAPÍTULO II - DOS SISTEMAS DE INFORMAÇÕES/AQUISIÇÃO DE SERVIÇO/DESENVOLVIMENTO

A classificação de informações, em conformidade com a Política de classificação e utilização de ativos, deve ser realizada no início do desenvolvimento de um novo aplicativo ou de um projeto de aquisição de sistema para ajudar os proprietários de informações a fazer a seleção adequada de controles de segurança para o sistema de informações.

Para sistemas/serviços adquiridos, antes da aquisição a Segurança da informação da Faculdade, deve realizar uma análise de risco, em conformidade com a Política de segurança da informação de terceiros, para determinar o impacto do risco associado ao novo sistema ou serviço de informações.

A análise dos requisitos funcionais de segurança deve ser realizada para identificar e documentar os requisitos de proteção de cada aplicativo por meio de um processo de avaliação de riscos. Os resultados da análise devem ser documentados, revisados e aprovados pelo Proprietário das informações e pela Segurança da informação. Essa análise ajuda a

identificar os principais riscos associados ao sistema em desenvolvimento ou aquisição e determina os controles de segurança necessários para manter esses riscos em limites aceitáveis. Entre esses controles estão:

- Planejamento e projeto da segurança;
- Regras de controle de acesso;
- Controle da entrada de dados;
- Verificações de validação;
- Integridade e autenticidade de mensagens;
- Controle de dados de saída o Criptografia.

Testes e avaliação dos controles de segurança devem ser realizados para assegurar que os controles certos sejam configurados, funcionem adequadamente e sejam eficientes para o sistema de informações.

Todos os problemas relacionados à segurança considerados de “alto risco” pelo processo de análise de segurança devem ser resolvidos antes de o sistema ser colocado em ambiente de produção.

Os aplicativos devem ser testados de acordo com planos de testes documentados e predefinidos. Esses testes devem abordar vulnerabilidade a ataques, impacto de dados inadequados e eficácia de controles de segurança.

É necessário ter cuidado para evitar exposição de dados sigilosos em ambientes de teste. Os testes devem ser feitos apenas com dados fabricados que imitem as características dos dados de produção ou em cópias dos dados de produção dos quais tenham sido removidas todas as informações confidenciais. Todos os testes que usarem dados de produção devem ter autorização explícita do gestor de segurança da informação.

As atividades de desenvolvimento de aplicativos devem ser realizadas em ambientes de desenvolvimento especializados, isolados do ambiente de produção em tempo real e do ambiente de testes de aceitação. Controles de segurança da informação adequados devem

ser aplicados no ambiente de desenvolvimento para proteger do acesso não autorizado. Além disso, os funcionários de desenvolvimento não devem ter acesso ao ambiente de produção.

Os sistemas ou aplicativos de desenvolvimento de terceiros com contrato com a Faculdade devem cumprir os requisitos desta política. Além disso, os requisitos contratuais (direito de auditar, caução de código fonte, modelos de ameaças etc.) definidos pelo Departamento jurídico da Faculdade a respeito dos requisitos de segurança da informação devem ser cumpridos.

CAPÍTULO III - DA IMPLEMENTAÇÃO DE SISTEMA/SERVIÇO DE INFORMAÇÕES

Todas as implementações de sistemas ou serviços de informações devem ser feitas conforme especificado pela Política de gestão de mudanças e pela Política de gestão de configurações da Faculdade.

CAPÍTULO IV - DA MANUTENÇÃO DE SISTEMA/SERVIÇO DE INFORMAÇÕES

Todas as mudanças em sistemas ou serviços de informações devem cumprir a Política de gestão de mudanças e a Política de gestão de configurações da Faculdade.

TÍTULO III

DAS CONSIDERAÇÕES FINAIS

CAPÍTULO I - DA APLICAÇÃO DA POLÍTICA DE AQUISIÇÃO E DESENVOLVIMENTO DE SISTEMA

Esta política se aplica da seguinte maneira:

- Todos os procedimentos aplicáveis aos requisitos nesta política devem ser definidos e estabelecidos no prazo de 6 meses a partir da Data de vigência desta política.

CAPÍTULO II - DAS CONFORMIDADES E EXCEÇÕES

Todos os funcionários da Faculdade devem aderir aos requisitos definidos nesta política. Qualquer funcionário que viole esta política pode estar sujeito a ação disciplinar, incluindo até mesmo demissão.

O gestor de segurança da informação deve autorizar as exceções à presente política nos termos da estrutura da Política de tecnologia da informação da Faculdade e do Procedimento de exceção à Política de tecnologia da informação da Faculdade.

CAPÍTULO III - DAS DEFINIÇÕES

TERMO	DEFINIÇÃO
Ativo de informações	Uma informação definível independentemente do formato, que é tida como de valor para a Faculdade.
Depositário das Informações (dados)	Indivíduos identificáveis e responsáveis pela supervisão, implementação e gestão das defesas necessárias à proteção de ativos de informações de acordo com o nível classificado pelo Proprietário das informações
Proprietários das Informações (dados)	Indivíduo identificável com autoridade para tratar de ativos de informações específicos e responsabilidade para estabelecer controles para a geração, classificação, coleta, processamento, disseminação e descarte desses ativos.
Sistema de Informações	Um sistema de computador ou conjunto de componentes para obtenção, criação, armazenamento, processamento e distribuição de informações, incluindo, tipicamente, hardware e software.
Rede	Sistema contendo qualquer combinação de computadores, terminais de computador, dispositivos de exibição de áudio ou vídeo ou telefones interconectados por equipamento ou cabos de telecomunicação usado para transmitir ou receber informações.
Política	Conjunto de declarações e requisitos destinados a proteger os valores, ativos e a inteligência da empresa. As políticas servem como o fundamento para padrões, procedimentos e diretrizes relacionados.

Procedimento	Conjunto de declarações e requisitos destinados a proteger os valores, ativos e a inteligência da empresa. As políticas servem como o fundamento para padrões, procedimentos e diretrizes relacionados.
Funcionários	Funcionários, funcionários temporários, voluntários, estagiários e outras pessoas cuja conduta, durante a prestação de atividades profissionais para a organização, esteja diretamente subordinada à Faculdade, sendo pagos ou não pela instituição.
Terceiros	Qualquer entidade (como pessoa física, fornecedor, cliente, consultor, parceiros comerciais, prestadores de serviços) que não integre a instituição, mas mantenha com ela um vínculo (contratual ou informal). Terceiros não estão subordinados diretamente à instituição, mas podem ter celebrado um contrato com a Faculdade.
Usuários	Qualquer pessoa autorizada a possuir uma conta ou acessar o sistema ou os ativos de informações da Faculdade. Incluindo funcionários e terceiros.

CAPÍTULO IV - DAS CONSIDERAÇÕES FINAIS

Esta Política entrará em vigor imediatamente após sua aprovação pelo Conselho Superior. Os casos omissos serão resolvidos pelo Conselho Superior.

Conselho Superior