INSTITUTO ÁRIA

POLÍTICA DE CONSCIENTIZAÇÃO E TREINAMENTO SOBRE A SEGURANÇA DE TECNOLOGIA DA INFORMAÇÃO

Brasília/DF

POLÍTICA DE CONSCIENTIZAÇÃO E TREINAMENTO SOBRE A SEGURANÇA DE TECNOLOGIA DA INFORMAÇÃO

TÍTULO I

DA POLÍTICA DE CONSCIENTIZAÇÃO E TREINAMENTO SOBRE A SEGURANÇA DE TECNOLOGIA DA INFORMAÇÃO DA AUDEN

CAPÍTULO I - DO OBJETIVO

O objetivo desta política é fornecer os requisitos do programa de conscientização e treinamento sobre segurança do Instituto Ária. Este documento fornece um esboço do programa e descreve quais atividades são necessárias para ele que seja corretamente implantado.

CAPÍTULO II - DO ESCOPO

Esta política define as exigências do programa desenvolvido para garantir que os usuários da Faculdade estejam adequadamente cientes e treinados dentro dos conceitos e práticas de segurança da informação que são exigidos para proteger corretamente os ativos de informações e sistemas de informação da instituição.

Esta política se destina a funcionários da Faculdade e a terceiros com acesso aos sistemas de informação, redes ou ativos de informações da instituição,

CAPÍTULO III - DAS DEFINIÇÕES

TERMO	DEFINIÇÃO
Ativo de informações	Uma informação definível independentemente do formato, que é tida como de valor para a Faculdade.
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
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.

TÍTULO II

DA DECLARAÇÃO DA POLÍTICA DE AQUISIÇÃO E DESENVOLVIMENTO DE SISTEMAS

CAPÍTULO I - DAS FUNÇÕES E RESPONSABILIDADES

O gestor de segurança é responsável por administrar esta política. Ele trabalhará juntamente com outras partes interessadas da Faculdade para definir os procedimentos e sistemas adequados para desenvolver e oferecer conteúdos de conscientização sobre segurança, além de documentações e certificados.

O gestor (ou seu representante) é responsável por definir o treinamento para os usuários e por monitorar a conformidade. Os usuários devem realizar o treinamento definido. Não concluir todo o treinamento atribuído ao usuário será considerado uma violação desta política. As violações serão comunicadas ao gestor direto do usuário e um cronograma será fornecido definindo quando a violação deverá ser solucionada. O usuário e seu gestor direto têm a responsabilidade de garantir que as ações corretivas (que podem envolver o

Departamento jurídico e o RH) para solucionar as violações sejam tomadas. Além disso, deixar de solucionar a violação dentro do tempo determinado pode resultar na suspensão do acesso do usuário aos sistemas de informação da Faculdade até que as ações corretivas sejam realizadas.

CAPÍTULO II - DA DECLARAÇÃO DA POLÍTICA

Os controles de segurança de TI são um componente fundamental para a estrutura de segurança da informação da Faculdade, mas só podem proteger os ativos de informações quando todos os usuários demonstram um alto nível de conhecimento de segurança desses controles. A conscientização sobre segurança se refere à transmissão de conceitos de segurança, de diferentes maneiras, com o objetivo de fazer com que os usuários dos sistemas de informação da Faculdade estejam mais cientes sobre o assunto e possam proteger de maneira adequada os ativos de informações e sistemas de informação da empresa. Este programa inclui as atividades específicas de treinamento, além de materiais de acompanhamento usados para ensinar os usuários dos sistemas de informação da instituição sobre segurança e sua aplicabilidade nas tarefas e serviços que desempenham. Este programa contínuo é adaptável e considera as alterações sofridas no ambiente de computação, na equipe de funcionários e as ameaças que podem pôr em risco a segurança da Faculdade.

CAPÍTULO III - DO CONTEÚDO DO TREINAMENTO DE CONSCIENTIZAÇÃO SOBRE SEGURANÇA

O gestor de segurança (ou seu representante) fornecerá o treinamento adequado de conscientização de segurança a todos os usuários dos sistemas de informação da Faculdade. Este treinamento pode abranger tópicos gerais, para todos os usuários, e conteúdo específico de conscientização de segurança para determinadas funções. O treinamento deve abordar tópicos sobre a proteção adequada dos ativos e sistemas de informação da instituição.

O conteúdo específico deve ser definido com base nas necessidades e considerar os requisitos jurídicos, regulatórios e/ou contratuais. Todo o programa de conscientização sobre segurança deve ser avaliado e aprovado pelo gestor de segurança ou pessoa indicada.

CAPÍTULO IV - DO TREINAMENTO OBRIGATÓRIO DE CONSCIENTIZAÇÃO SOBRE SEGURANÇA

O treinamento de conscientização sobre segurança é obrigatório para todos os usuários que precisam de acesso aos ativos e sistemas de informação da Faculdade. O treinamento de conscientização sobre segurança deve ser concluído dentro de 30 (trinta) dias após o usuário receber o acesso inicial ao sistema ou rede de informações da instituição (com ao menos um treinamento obrigatório por ano).

Para usuários que já contam com o acesso, o treinamento de conscientização sobre segurança deve ser feito anualmente.

CAPÍTULO V - DO OFERECIMENTO DO TREINAMENTO DE CONSCIENTIZAÇÃO SOBRE SEGURANÇA

O treinamento de conscientização sobre segurança deve ser oferecido de forma eficiente. O uso de treinamentos via Web pode ser considerado.

CAPÍTULO VI - DO TREINAMENTO DE CONSCIENTIZAÇÃO SOBRE SEGURANÇA ESPECÍFICO POR FUNÇÃO

A Faculdade deverá oferecer treinamentos de conscientização sobre segurança específicos para funções que exijam um treinamento adicional por conta do acesso necessário para a responsabilidade da função. O gestor de segurança (ou seu representante) determinará a necessidade, o conteúdo e o público-alvo dos diferentes tipos de treinamento.

CAPÍTULO VII - DA DOCUMENTAÇÃO DO TREINAMENTO DE CONSCIENTIZAÇÃO SOBRE SEGURANÇA

O gestor de segurança da informação, o departamento de recursos humanos e a Direção Geral da Facudade devem garantir que a documentação mantida evidencie a conformidade com esta política. Registros de treinamentos individuais devem ser retidos de acordo com a Política de retenção da Faculdade.

CAPÍTULO VII - DA AVALIAÇÃO DO PROGRAMA DE CONSCIENTIZAÇÃO SOBRE SEGURANÇA

O gestor de segurança (ou seu representante) também será responsável por:

- Facilitar o treinamento contínuo de segurança para os usuários do sistema de informações da Faculdade;
- Atualizar sobre as mais recentes práticas recomendadas de segurança;
- Compartilhar informações atuais relacionadas à segurança incluindo novas ameaças, vulnerabilidades e incidentes.

O gestor de segurança (ou seu representante) deve garantir que o treinamento de conscientização sobre segurança seja mantido atualizado. Além disso, deve monitorar a conformidade dos usuários com o programa de treinamento de conscientização sobre segurança da instituição, ajustando o programa para poder solucionar quaisquer problemas.

O gestor de segurança ou pessoa indicada deve avaliar anualmente o conteúdo de conscientização de segurança e trabalhar com os recursos humanos e com a Diretoria Geral para revisar o conteúdo, se necessário.

TÍTULO IV

DAS CONSIDERAÇÕES FINAIS

CAPÍTULO I - DA APLICAÇÃO DA POLÍTICA DE CONSCIENTIZAÇÃO E TREINAMENTO SOBRE A SEGURANÇA DE TECNOLOGIA DA INFORMAÇÃO

Após a data deste documento, todos os novos usuários devem receber o treinamento inicial no prazo de 30 dias a contar da data de aprovação do presente documento.

Todos os usuários atuais devem concluir o treinamento de conscientização sobre segurança em no máximo 6 meses após a 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 deverá fornecer as autorizações para todas 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 instituição.

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