PLANO DE CONSCIENTIZAÇÃO, EDUCAÇÃO E TREINAMENTO EM SEGURANÇA DA INFORMAÇÃO

https://gsic.ufba.br

1 Objetivo

O plano de conscientização, educação e treinamento em Segurança da Informação da Universidade Federal da Bahia – UFBA tem o propósito de estruturar ações para treinamento, educação e conscientização de colaboradores da UFBA na temática de segurança da informação. Ademais, as informações descritas neste plano visam formar uma base para concepção, desenvolvimento e implementação de atividades e programas de conscientização eficazes e adequados à realidade da Universidade. Mais especificamente, são objetivos deste plano:

- Declarar o comprometimento da direção com conscientização e treinamento em segurança da informação em toda organização;
- Definir os papéis e responsabilidades de todos colaboradores para disseminação da cultura de segurança da informação na UFBA;
- Estabelecer ações de conscientização, educação e treinamento em segurança da informação alinhadas com as políticas, normas e procedimentos da organização, bem como respeitando a cultura organizacional;
- Medir, avaliar criticamente e melhorar continuamente as estratégias e ações adotadas, garantindo uma execução regular, atualizada, abrangente e em conformidade com as políticas, normas e procedimentos em vigor na organização.

2 Papéis e Responsabilidades

- **Núcleo de Conscientização e Educação da COSIC/STI-UFBA:** responsável por estruturar, apoiar ou executar ações de conscientização e educação em segurança da informação na UFBA, apoiando na elaboração de conteúdo, logística de realização, comunicação, promoção e realização de ações;

- **Equipe de Tratamento de Incidentes de Redes (ETIR-UFBA):** responsável por demandar e propor soluções de conscientização para mitigar os incidentes de segurança no âmbito da UFBA e apoiar o Núcleo de Conscientização e Educação na elaboração das ações de conscientização em segurança da informação;

- **Gestor de Segurança da Informação e Comunicações da UFBA (GSIC):** responsável pelo acompanhamento das ações de conscientização, pela validação do material produzido, por informar prioridades a serem executadas e pelo investimento financeiro quando necessário;

- **Central de Serviços:** responsável por orientar, auxiliar e tirar dúvidas dos usuários sobre questões de segurança da informação;

- **Consultoria Externa Especializada:** responsável por produzir itens específicos das ações de conscientização, conforme definido em plano de ação de conscientização elaborado pelo Núcleo de Conscientização;

- **Usuário:** responsável por cumprir com as políticas de segurança da informação da UFBA para que incidentes de segurança sejam minimizados ou até mesmo evitados.

3 Fluxo de Conscientização em Segurança da Informação

O processo de conscientização, educação e treinamento em segurança da informação da UFBA possui diversas fases e respectivos responsáveis, funcionando com base no fluxo da Figura 1.

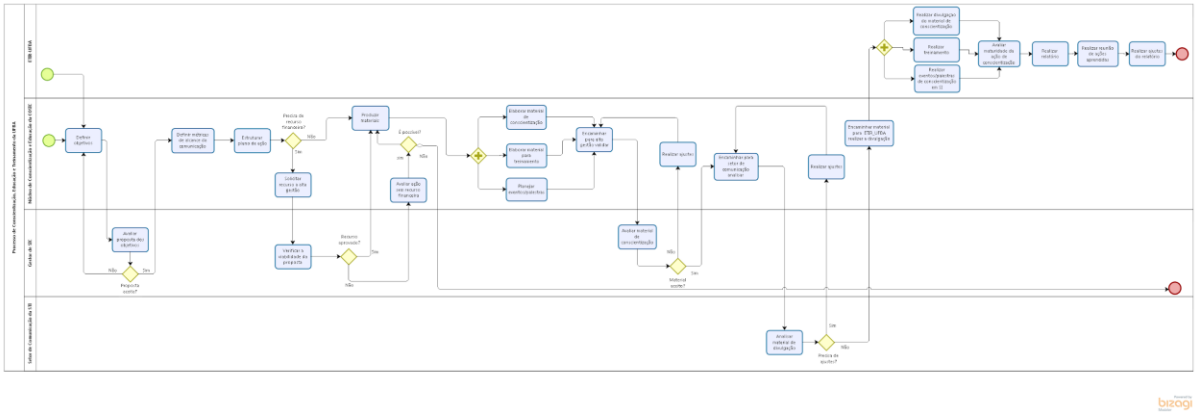

Figura 1: Fluxo de Educação, Conscientização e Treinamento da UFBA

A seguir, cada uma das etapas descritas no plano serão detalhadas.

3.1 Definir Objetivos da Ação de Conscientização

É necessário definir claramente os objetivos das ações de conscientização para que seja possível direcionar esforços em prol de resultados satisfatórios. Os objetivos podem ser definidos mediante incidente de segurança ocorrido na instituição, mapeamento de riscos, monitoramento de tendências ou solicitação da ETIR-UFBA ou GSIC. Alguns dos objetivos aplicáveis a uma ação de conscientização são:

- **Advertir usuários:** informar aos usuários internos e externos sobre as responsabilidades e obrigações a partir do momento que estão cientes das políticas de segurança da informação da instituição, advertindo-os sobre a equipe de TI responsável para manutenção e acesso aos equipamentos e recursos de rede da organização;

- **Educar os usuários:** transmitir aos usuários conhecimentos sobre a importância de realizar uma navegação segura e passar procedimentos básicos de segurança da informação como:

    - reportar incidentes de segurança da informação;
    - comunicar a equipe de TI sobre manutenção dos equipamentos de rede;
    - procedimentos de segurança da informação como, senha segura, atualização de sistemas e outros.

- **Canais de comunicação:** informar aos usuários sobre os canais de comunicação oficiais para esclarecer dúvidas ou reportar problemas.

Assim, os envolvidos estarão conscientes de suas responsabilidades com a segurança da informação mediante a políticas e normas da organização, tendo ele o compromisso de manter segura e em sigilo informações que pertençam à organização.

3.2 Definir Métricas de Alcance da Comunicação

As métricas que serão citadas a posteriori, servem como base para que seja realizado um processo de avaliação da ação de conscientização. Com o resultado dos dados obtidos, o núcleo de conscientização e educação poderá realizar ajustes e melhorias durante o processo da ação de conscientização.

Nesse momento o núcleo de conscientização e educação poderá colher algumas informações do usuário que estão tendo acesso às ações de conscientização disponibilizadas. Um exemplo para conseguir as informações desejadas pode ser através de ferramentas online que realizam monitoramento de uma determinada página *web* pré configurada ou mediante a outros recursos que o núcleo julgue necessário. As métricas citadas abaixo são essenciais para saber como o plano de ação impacta os usuários internos ou externos da UFBA. Algumas sugestões de métricas a serem usadas são:

- Dados pessoais do colaborador como, idade, sexo e cargo institucional;
- Informações da rede como IP;
- Tempo de navegação na página;
- Informações do Sistema Operacional;
- Quantidade de acessos à página;
- Recebimento de e-mail com sugestões, ajuda, dúvidas e outros.

É necessário alertar que, foram dadas sugestões de métricas para serem avaliadas, a escolha ou novas sugestões de métricas para avaliação podem surgir de acordo com cada ação a ser realizada.

3.3 Estruturar Plano de Ação

3.3.1 Definir Estratégias de Conscientização

A definição da estratégia é um dos pontos principais, pois, a partir dela que o plano de conscientização atingirá o objetivo. A mensagem a ser transmitida deve ser bem elaborada para conseguir um resultado satisfatório, nela, deve-se deixar clara a importância da segurança da informação.

Definido as estratégias, é necessário informar ao usuário que o seu aprendizado com relação às ações de conscientização tomadas pelo núcleo de conscientização e educação pode proporcionar benefícios significativos para a organização.

Nesta etapa é definida qual a melhor forma de transmitir a mensagem de conscientização. O núcleo de conscientização e educação deve se preocupar em como passar essa informação para o usuário, atentando-se para transmiti-la de forma didática, clara, coerente e de maneira apropriada com o contexto organizacional.

Logo, para estabelecer estratégias eficazes é necessário entender a forma de construção das ações. Assim, cada ação de conscientização realizada servirá como referência para as próximas ações a serem construídas, visando não somente o núcleo de conscientização e educação, como também o usuário final. Alguns pontos significativos a serem avaliados são:

- Qual a frequência para realizar as ações de conscientização?
- Qual o risco que a organização pode sofrer caso determinado tema não seja abordado?
- A quem se destina a ação de conscientização?
- Como transmitir uma mensagem de conscientização para grupos de públicos distintos?
- Qual a forma de comunicação que deve ser usada?

As estratégias de conscientização podem ser:

Envio por e-mail	- Produção de campanhas por e-mail abordando um tema específico; - Informativo de incidentes alertando os usuários da organização.
Vídeo	Vídeos possuem uma melhor interatividade com o usuário e chama mais a atenção por conter animações.
Palestras de conscientização	Realizando eventos em Segurança da Informação em que os usuários possam participar e aprender ou conhecer mais sobre os temas abordados, todos relacionados a

	segurança da informação.
Cartilhas, folders e outros	A produção de materiais impressos é uma forma de fazer com que a mensagem transmitida possa atingir públicos imensuráveis através do compartilhamento.
Webinars, participação em eventos, mesas redondas	Ações que possam ser realizadas para o envolvimento de colaboradores da organização e usuários externos, para o conhecimento e aprendizado de todos sobre a segurança da informação.
Treinamento, bate papo e outros	Aqui pode ter o envolvimento da equipe de segurança da informação e comunicações (SIC) em conjunto com a equipe de TI abordando temas relevantes para a organização em segurança da informação.

3.3.2 Definir Temas de Conscientização

Após o processo de coleta de informações necessárias para compor a ação de conscientização, é necessário definir temas de conscientização que sejam relevantes para a organização. O núcleo de conscientização deve propor temas a fim de educar os usuários internos ou externos com informações de práticas de segurança da informação já existentes como também propor temas da atualidade.

Os temas de conscientização podem ser atualizados pelo núcleo de educação mediante aos acontecimentos da organização como, incidentes de segurança, atualização dos procedimentos da universidade, inclusão de novos serviços, e outros.

Os temas de conscientização podem ser:

- Segurança da estação de trabalho;
- Segurança em dispositivos móveis;
- Vírus e códigos maliciosos;
- Segurança de senhas;
- Cópias de segurança (backup);
- Atualização de sistemas;
- Mecanismos de proteção de sistema (antivírus, antimalware, firewall);
- Golpes na Internet e fraudes eletrônicas (phishing);
- Uso seguro da Internet;
- Privacidade de informações e redes sociais.

3.3.3 Definir Avaliação de Maturidade

Nessa fase vamos medir o nível de maturidade ou capacitação em segurança da informação dos usuários. Para que o plano de conscientização alcance bons resultados é necessário identificar as demandas de conscientização, educação ou treinamento que serão realizadas através das ações propostas.

Para obter essas informações pode ser realizada uma avaliação de nível de maturidade dos usuários, realizando um questionário que pode ser através de recursos online, gerando posteriormente estatísticas para análise, dessa forma, mediante as resposta concedidas pode-se trabalhar com os resultados gerados para fortalecer ainda mais o nível de conhecimento dos usuários em relação a segurança da informação.

O questionário pode ser composto por perguntas relacionadas com o tema a ser tratado na ação de conscientização, aos procedimentos de segurança da organização e outros. A quantidade de perguntas vai depender da necessidade de informações que se deseja obter para formular a ação de conscientização. O questionário pode ser através de perguntas com envio de respostas dos usuários se verdadeiro ou falso, ou pela escolha de respostas pré-disponibilizadas. Outras formas de avaliação da maturidade podem ser elaboradas de acordo com o nível de aprimoramento das ações realizadas.

3.4 Elaborar Materiais do Plano de Ação

Nessa fase após definido a ação de conscientização a ser realizada mediante ao plano de ação discutido, o núcleo de educação e conscientização deve iniciar a elaboração dos insumos da ação de conscientização. Caso a estratégia de conscientização necessite de recursos financeiros ou assessoria externa deve ser solicitado o apoio aos responsáveis para que a execução da ação seja finalizada até as datas pré-definidas.
Após finalizado os materiais necessários para disponibilizar a ação de conscientização é necessário que o gestor de SIC avalie se as informações contidas são satisfatórias. Caso alguma modificação tenha que ser realizada, após o núcleo de conscientização realizar a alteração é necessário que o gestor de SIC faça mais uma avaliação antes de dar segmento ao fluxo da ação de conscientização.

Após a aprovação realizado pelo gestor de SIC dos materiais de conscientização, é importante que o setor de comunicação da instituição possa avaliar o material caso seja impresso, no que quesito design e até mesmo como a informação está sendo transmitida, pois os mesmos podem passar dicas importantes para melhoria do material antes que seja disponibilizado para o usuário final.

3.5 Disponibilizar a Ação de Conscientização

Nessa etapa a ETIR-UFBA é responsável pela divulgação da ação de conscientização seja ela qual for definida durante o processo de estruturação do plano de conscientização.

3.5.1 Avaliar a Maturidade da Ação de Conscientização

Essa etapa é fundamental para analisar se a ação de conscientização causou um impacto positivo nos usuários, no que se refere aos conhecimento adquiridos após disponibilizar o material para todos. Aqui também será analisado os resultados das métricas que foram pré-definidas para obter dados que procurem verificar como a ação de conscientização atinge o usuário. O resultado dessa avaliação é muito importante, em razão que pode auxiliar em melhorias nas próximas ações de conscientização a serem realizadas.

Com os resultados obtidos é importante que seja elaborado um relatório que contenham informações suficientes sobre a ação realizada. Com isso, é necessário realizar uma reunião com a ETIR-UFBA e núcleo de conscientização e educação para verificar as lições aprendidas sobre ação, discutir erros e verificar melhorias que podem ser realizadas nas próximas ações e por fim realizar ajustes necessários no relatório.

4 Disposições Finais

O núcleo de educação e conscientização da COSIC poderá realizar ajustes nesse documento sempre que julgar necessário, a fim de de mantê-lo consistente com as demandas e diretrizes da área de segurança da informação e comunicações.

5 Histórico de Revisões

Rev	Data	Descrição	Versão	Autor
01	14/01/2019	Criação do documento	1.0	Carolina Caires, Italo Valcy
02	29/01/2019	Revisão e ajustes do documento	1.1	Carolina Caires, Italo Valcy
03	05/02/2019	Revisão e ajustes do documento	1.2	Carolina Caires, Kléber Mascarenhas
04	06/06/2019	Revisão e ajustes do documento	1.3	Carolina Caires
05	10/07/2019	Revisão e ajustes do documento	1.4	Kleber Mascarenhas