PROGRAMA DE CONSCIENTIZAÇÃO E EDUCAÇÃO EM PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO DO CNPq - CONSCIENTIZA-SIN

ANEXO I

FLUXO NORTEADOR PARA ELABORAÇÃO DOS PLANOS DE AÇÃO

O processo de Conscientização e Educação em Privacidade e Segurança da Informação do CNPq é composto das seguintes etapas:

1. Definição dos Objetivos da Ação de Conscientização

É necessário definir claramente os objetivos das ações de conscientização para direcionar esforços em prol de resultados satisfatórios, visando a capacitação continuada dos agentes públicos em atividade no CNPq. Os objetivos podem ser definidos após a ocorrência de incidente de segurança na instituição, mapeamento de riscos, monitoramento de tendências ou solicitação do Comitê de Segurança da Informação (CSI). Alguns exemplos dos objetivos aplicáveis a uma ação de conscientização são:

● Advertir usuários: informar aos usuários sobre as responsabilidades e obrigações a partir do momento que estão cientes das políticas de segurança da informação da instituição;

● Educar os usuários: transmitir aos usuários conhecimentos sobre a importância de realizar uma navegação segura e da execução dos procedimentos básicos de segurança da informação;

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

2. Definição das Métricas de Alcance das Ações de Comunicação

Definir métricas e indicadores para servir como base para monitoramento e avaliação da efetividade da ação de conscientização.

As informações citadas abaixo são essenciais para saber como o plano de ação impacta os usuários internos do CNPq.

● Dados pessoais do usuário 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 podem surgir outras informações necessárias à mensuração dos resultados de acordo com cada ação a ser realizada.

3. Estruturação do Plano de Ação

3.1. Definição de Estratégias de Conscientização

A definição da estratégia aplicada às ações de conscientização é um dos pontos principais para que o plano de conscientização atinja seu objetivo. A mensagem a ser transmitida deve ser bem elaborada para um resultado satisfatório, e deve refletir o papel individual de cada agente na segurança da informação.

Nesta etapa, a melhor forma de transmitir a mensagem de conscientização deverá ser definida. A Assessoria de Comunicação Social (ACS) deverá orientar as demandas para que a informação seja transmitida ao usuário de forma didática, clara, coerente e apropriada ao contexto organizacional.

As ações de capacitação de conscientização em privacidade e segurança da informação deverão ser realizadas de forma continuada, de modo que seja estabelecida uma relação lógica entre uma e outra.

Alguns pontos significativos a serem abordados nesta fase são:

- a frequência para realizar as ações de conscientização;
- o risco que a organização pode sofrer caso determinado tema não seja abordado;
- a definição do público-alvo da ação de conscientização;
- as estratégias específicas de campanhas de conscientização aos públicos distintos; e
- a forma de comunicação a ser utilizada.

Uma variedade de estratégias para promover a conscientização em privacidade e segurança da informação pode ser utilizada, seja por meio do envio de e-mails, vídeos, palestras, cartilhas folders, webinars, eventos, mesas redondas, treinamentos, bate papo, dentre outros.

3.2. Definição de 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 Comitê de Segurança da Informação (CSI) deverá propor temas, a fim de educar os usuários internos e/ou externos quanto às boas práticas de segurança da informação adotadas pelo órgão.

Os temas de conscientização podem ser atualizados pelo CSI baseados nos registros de dados organizacionais de Segurança da Informação como monitoramento de phishings, incidentes de segurança, atualização dos procedimentos do CNPq, inclusão de novos serviços de TI, dentre outros.

Alguns dos principais temas a serem considerados, são:

- 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. Elaboração de instrumentos para Avaliação de Maturidade do CNPq em Segurança da Informação

Nessa fase vamos medir o nível de maturidade em privacidade e segurança da informação dos usuários. Para que o programa de conscientização alcance bons resultados é necessário identificar as demandas de conscientização e educação que serão atendidas através das ações propostas.

Para obter informações quanto ao nível de maturidade dos usuários do CNPq podem ser realizadas avaliações de diagnóstico do nível de maturidade por meio de instrumento adequado.

4. Elaboração de Materiais do Plano de Ação

Nessa fase, após definida a ação de conscientização a ser realizada, inicia-se 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.

Os conteúdos usados nas ações de conscientização deverão ser analisados tanto pelo Gestor de Segurança da Informação quanto pela Assessoria de Comunicação do CNPq.

5. Disponibilizar a Ação de Conscientização

Nessa etapa, a Assessoria de Comunicação é responsável pela divulgação da ação de conscientização definida durante o processo de estruturação do plano de ação de conscientização por meio de planejamento contínuo.

5.1 Avaliar a Maturidade da Ação de Conscientização do Programa

Essa etapa é fundamental para analisar o impacto da ação de conscientização nos usuários, no que se refere aos conhecimentos adquiridos no treinamento. Aqui também serão analisados os resultados das métricas pré-definidas, para verificar como a ação de conscientização atingiu o usuário final.

Um relatório, semestral ou anual, com os resultados da avaliação de maturidade do Programa deve ser elaborado para o CSI, a fim de informar as lições aprendidas com a ação, apontar erros de implementação/desenho e analisar melhorias para as próximas ações. O resultado dessa avaliação deverá ser utilizado como instrumento de gestão do Programa e auxiliar no aperfeiçoamento das próximas ações de conscientização.

6. Plataformas passíveis de serem usadas:

Avaliar a disponibilidade de plataformas para executar o plano de ação para implementação do Programa Conscientiza-SIN, de modo a permitir o monitoramento constante do nível de maturidade dos agentes públicos do órgão e criar trilhas de aprendizagem no tema privacidade e segurança da informação adaptadas aos usuários em trabalho presencial e remoto.