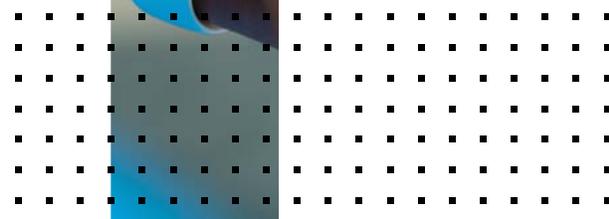


GUIA DE IMPLANTAÇÃO

# Como definir as metas e planejar seu serviço de conscientização e treinamento em Cibersegurança

Um guia sobre como criar uma equipe com conscientização cibernética



Houve um tempo em que os funcionários se ocupavam com suas tarefas diárias, ignorando ameaças potenciais para a empresa e para eles mesmos. Para eles, a equipe de segurança de TI protegia os dados, redes, dispositivos e usuários. Não demorou muito para que, hoje, os funcionários tenham se tornado alvos valiosos para cibercriminosos. É fundamental instruir os funcionários quanto aos riscos de Cibersegurança. Um ataque bem-sucedido (basta apenas um clique errado em um e-mail para isso acontecer) pode extrair milhões de dólares para os criminosos e custar para uma empresa milhões de dólares em perda na confiança da marca, sanções de conformidade, receita, valor para os acionistas e por aí vai.

**O fator humano da segurança cibernética não pode ser deixado de lado. A segurança passa a ser uma responsabilidade de todos.**

A solução de formação e conscientização em segurança deve contribuir para uma cultura de segurança geral. Seguir uma abordagem de “conformidade: o que fazer” na formação não promoverá a cultura de conscientização nem conseguirá responder ao cenário dinâmico de ameaças. É essencial que a conscientização sobre a segurança cibernética seja uma parte integrada e contínua da cultura de trabalho da empresa. Tudo começa pela pessoa em si, e todo funcionário é responsável por garantir a segurança das informações e ativos da empresa.

**Mas como você mantém seus funcionários engajados e consolida uma cultura de conscientização cibernética?**

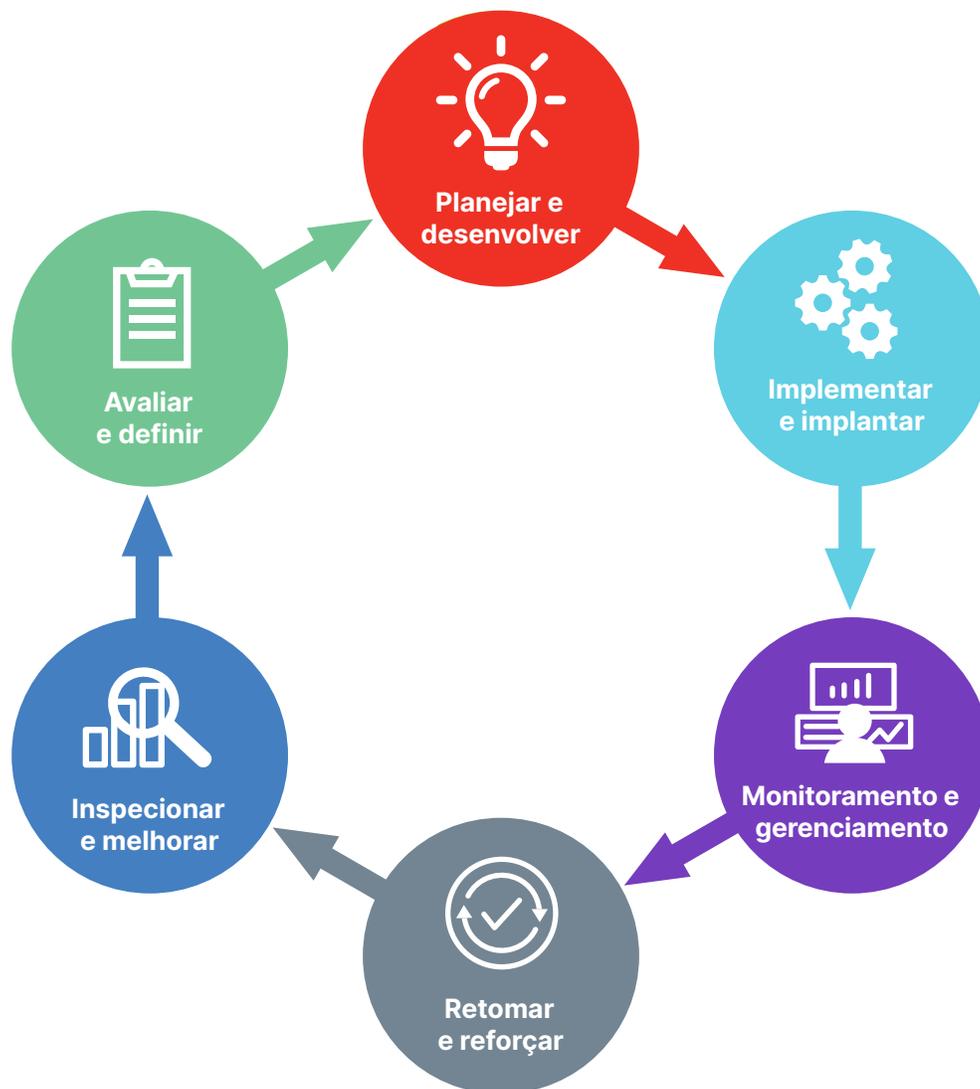


Figura 1: Um Serviço de conscientização e treinamento em Cibersegurança começa pela avaliação e definição das necessidades.

## Avalie e entenda seu parâmetro: saiba quais são seus riscos

Antes de tudo, é fundamental definir um parâmetro dos atuais riscos de segurança. Ao identificar os riscos para sua empresa, é possível elaborar um plano e avaliar se seu programa de formação está fazendo ou não a diferença nos hábitos de Cibersegurança.

A estrutura de segurança cibernética nada mais é do que um sistema de padrões, diretrizes e práticas recomendadas usado para gerenciar os riscos no cenário digital. Normalmente, essa estrutura corresponde aos objetivos de segurança e é usada para criar políticas e procedimentos que definem as práticas recomendadas aderidas pela empresa para lidar com os riscos relacionados à segurança cibernética.

Os gerentes devem fazer a seguinte pergunta: “Que resultados de Cibersegurança seriam úteis para o gerenciamento do risco de Cibersegurança?”. Há várias estruturas, como os [Princípios e ferramentas de resiliência cibernética para conselhos administrativos, do Fórum Econômico Mundial \(FEM\)](#) e a [Estrutura de Cibersegurança \(CSF\) do National Institute of Standards and Technology \(NIST\)](#), referências que podem ser usadas ao elaborar uma estrutura de segurança para sua empresa.

### Riscos de Cibersegurança para o funcionário

Recomenda-se testar os hábitos (ou a falta) de segurança do funcionário antes mesmo de incluí-lo no treinamento. Fazer isso ajuda a definir um parâmetro e, assim, entender quais as áreas problemáticas e onde concentrar os esforços de treinamento e reforço. Há várias técnicas e ferramentas que você pode implantar para entender os hábitos de segurança dos seus funcionários.

1. Comece com alguns exercícios de simulação de phishing. Registre os resultados. Inclua um treinamento de continuidade. Realize novamente os exercícios de simulação de phishing. E agora, quais são os resultados?
2. Monitore os pontos de acesso e anote quaisquer ocorrências de entradas indevidas (também conhecido como tailgating, em que os funcionários permitem que pessoas entrem nos pontos de acesso sem passar um crachá de acesso). Anote os resultados e repita o teste em intervalos predeterminados.
3. Faça uma verificação sem aviso prévio nas mesas do seu local de trabalho. Procure por dispositivos bloqueados, gavetas e documentos confidenciais. Anote os resultados e repita o teste em intervalos predeterminados.
4. Conduza uma pesquisa com perguntas básicas.

## Garanta o apoio da liderança e defina suas metas

A participação da sua equipe de liderança é essencial ao definir a missão e o princípio da sua conscientização e formação em Cibersegurança. Crie uma força-tarefa de liderança com funções e responsabilidades definidas, como a identificação de metas e objetivos para o treinamento do usuário final, o treinamento da gestão, a adoção e incorporação de estruturas e obrigações de conformidade.

Com o subsídio da diretoria, identifique os principais motivos pelos quais a empresa gostaria de adotar uma conscientização e formação em segurança em toda a organização. Comece identificando objetivos. Pense no motivo pelo qual você está implementando o treinamento e no que você espera alcançar com o treinamento dos seus funcionários. Normalmente, as metas incluem: identificar áreas problemáticas, expandir o conhecimento do funcionário, criar mudanças e reforçar as expectativas.

Suas tarefas e etapas devem obter a aprovação orçamentária e de verbas.

## Elabore seu plano de treinamento

Agora que você já conta com o apoio da diretoria e possui uma direção claramente definida, chegou a hora de elaborar seu plano de formação e conscientização.

Pode ser que você queira que seu plano aborde as seguintes questões:

- Como será o ritmo do treinamento? Como você lidará com o processo de integração, o treinamento anual, a avaliação regular e o serviço de formação como um todo?
- Precisa de uma implementação faseada com um grupo inicial de teste piloto? Como irá obter o feedback dos usuários?
- Precisa alcançar diferentes grupos, em diferentes momentos, com diferentes materiais?

- Quais assuntos devem ser abordados em sua empresa para criar um programa que atenda às demandas específicas da sua organização? Ao escolhê-los, não se esqueça dos comportamentos que gostaria de ver integrados às atividades diárias dos seus funcionários.
- Sua empresa precisa de um plano de comunicação centralizado, distribuído ou os dois? (Consulte [NIST 800-50](#), seção 3, para orientações mais detalhadas.)
- Como irá difundir todos os meios de comunicação (cartazes, imagens ou qualquer outra coisa)?
- Como irá testar os critérios de sucesso?
- Como serão estabelecidas e executadas as ações de mitigação?

## Hora de colocar em prática: chegou o momento de todos participarem

Agora está tudo pronto para apresentar seu programa de conscientização em segurança e comunicá-lo aos funcionários. O recomendado é que seus funcionários sejam avisados com antecedência de que serão inscritos na formação de conscientização em segurança, bem como que seja estipulado um prazo para que eles concluam o treinamento, com envio de lembretes. Fale sobre a importância do treinamento, seu plano de treinamento e o cronograma para toda a empresa. Fazer com que as pessoas participem é uma importante etapa para expandir a conscientização em segurança.

Selecione os assuntos sobre os quais gostaria que os membros da sua equipe aprendem mais. Você pode escolher de acordo com o teste de parâmetro, os requisitos do negócio ou eventos que estão acontecendo no mundo. Planeje o cronograma da cadência do treinamento. Defina quando serão distribuídos módulos, ativos e recursos para a equipe. Distribua-os regularmente, para que a segurança seja sempre uma prioridade.

## Monitoramento e gerenciamento

Gerencie o progresso do seu programa de conscientização sobre Cibersegurança ao monitorar o progresso dos funcionários. Quem participou do treinamento? Quem não e por quê? Quais as áreas de menor desempenho das pessoas? Consegue identificar algumas tendências que ajudem a elevar a adoção?

Além de monitorar o progresso do treinamento dos seus funcionários, você provavelmente vai querer avaliar também como os comportamentos de segurança dos funcionários melhoraram ao longo do tempo. Faça isso estabelecendo um ciclo de testes iniciais, treinamentos, novos testes e treinamento de remediação para funcionários que não estiverem em conformidade.

Ao analisar seu programa e identificar lacunas, leve em consideração os seguintes pontos enquanto implementa medidas adequadas:

- É necessário repassar as lacunas para a gerência e fazer algo em relação às questões isoladas?
- É necessário aumentar ou diminuir a frequência de distribuição do módulo de treinamento?
- Quais alterações fazer na campanha de formação para atender ao critério de sucesso?

## Retome e reforce o aprendizado

Ao monitorar seu programa, considere a eventualidade de ajustar ou adicionar novas campanhas, conforme necessário. Por exemplo, se você estiver vendo comportamentos errados ou se sua organização estiver preocupada com uma ameaça atual, considere implantar nanomódulos de aprendizagem ou micromódulos de treinamento como treinamento de remediação ou reforço de ensinamentos-chave. Distribua folhas de dicas por e-mail ou publique-as na intranet da sua empresa para serem apresentadas em intervalos regulares.

A Cibersegurança deve ser evidenciada durante todo o ano, impulsionando, assim, maior conscientização em segurança na empresa. Considere realizar campanhas associadas a vários temas, como Black Friday, o período de Natal, etc.

## Inspecionar e melhorar

O principal objetivo de qualquer implementação de programa de treinamento de conscientização em segurança é aumentar a conscientização e alterar positivamente o comportamento dos usuários para reduzir incidentes de segurança da informação.

O objetivo de um plano pós-implementação é buscar a melhoria contínua. Monitorar a conformidade, realizar avaliações formais e coletar feedbacks são práticas recomendadas que podem ser usadas para construir essa melhoria contínua dentro da sua organização.

A Publicação Especial NIST 800-50, seção 6.2, destaca as ferramentas e táticas para a realização de avaliações formais e a coleta de feedback, incluindo:

- Concepção de uma estratégia de feedback
- Realização de pesquisas
- Elaboração de relatórios de status
- Realização de entrevistas
- Anotações
- Implementação de grupos de foco
- Coleta e comparação de métricas (comparação com o parâmetro)

A publicação também destaca vários indicadores de sucesso do programa de formação de conscientização em segurança, como:

- Há o apoio para a distribuição de módulos e de ativos de conscientização.
- A equipe executiva está integrada com o envio de mensagens ao pessoal sobre segurança de TI.
- As métricas indicam uma lacuna cada vez menor entre a conscientização que já existe e as necessidades identificadas, aumento da porcentagem de usuários que têm acesso a materiais de conscientização, etc.
- Os gerentes estão empenhados no processo, inscrevendo-se no respectivo treinamento de conscientização e completando-o, e encorajando os outros a fazê-lo também.
- As contribuições de segurança estão sendo reconhecidas através de prêmios, concursos, etc.
- As principais figuras (gerentes, administradores de segurança da informação, coordenadores de formação e outros) parecem estar motivadas.

Verifique se a implementação deu certo ou não com base nos indicadores de sucesso. Se você ver que não deu certo, use os indicadores para verificar onde é possível fazer melhorias. As melhorias contínuas e as mudanças quantificáveis no comportamento devem sempre ser metas de qualquer programa de conscientização e formação em segurança da informação de sucesso.

