

COMO FAZER UM

PROGRAMA DE CONSCIENTIZAÇÃO

ORIENTADO A DADOS EM

6 PASSOS



SUMÁRIO

COMO FAZER UM PROGRAMA DE CONSCIENTIZAÇÃO ORIENTADO A DADOS EM 6 PASSOS	04
1. IDENTIFIQUE SEU PÚBLICO	06
2. ENTENDA SEU AMBIENTE	08
Principais riscos associados ao fator humano	
Entender os objetivos legais, regulatórios ou de auditoria	
Nível de maturidade de conscientização	
Canais de comunicação disponíveis	
3. DEFINA A ESTRATÉGIA E OBJETIVOS	10
Obtenha patrocínio	
Faça alianças	
Defina Papéis e responsabilidades	
Recursos disponíveis	
Estabeleça um plano de trabalho	
4. ESTABELEÇA MÉTRICAS	12
Métricas de Risco	
Métricas de Engajamento	
5. ENGAJE E TREINE	14
Cultura da Empresa	
Conexão com a audiência	
6. ANALISE E GERENCIE	16
Avaliação de Efetividade	
Processo de Melhoria	



[Site](#)



[Youtube](#)



[Twitter](#)



[Linkedin](#)



[Facebook](#)

COMO FAZER UM PROGRAMA DE CONSCIENTIZAÇÃO ORIENTADO A DADOS EM 6 PASSOS

1 IDENTIFIQUE SEU PÚBLICO

O primeiro passo é entender qual o **público alvo** do seu programa de conscientização. Para isso, levante o número de pessoas, a localização e a linguagem a ser utilizada. Também é importante analisar como está dividida sua audiência, seguindo por criticidade do público.

2 ENTENDA SEU AMBIENTE

Após identificar seu público, é preciso verificar qual o **nível de maturidade** que a empresa está, quais são os **principais riscos**, quais **temas** de segurança da informação serão abordados no programa e quais **canais de comunicação** estarão disponíveis.

3 DEFINA A ESTRATÉGIA E OBJETIVOS

Com todo o levantamento feito, é hora de definir qual será a estratégia da campanha. Nela, deverá ser definido o **objetivo do programa** considerando a **maturidade** que se quer alcançar, **pessoas envolvidas** e **stakeholders**, recursos disponíveis e quais **ações** deverão ser executadas num determinado **período de tempo**.

4 ESTABELEÇA MÉTRICAS

Com base nas definições anteriores, defina as **métricas** de risco e de engajamento que possibilitem avaliar se o programa atingiu suas metas. Elas ajudarão na apresentação dos resultados de seus esforços para a alta administração, a garantir a continuidade do programa e, além disso, obter meios para a tomada de ações corretivas que garantam o melhor resultado possível para o programa.

5 ENGAJE E TREINE

Está na hora de usar a criatividade para engajar e **mudar a cultura do seu público**. Utilize diferentes **ações de treinamentos** atrativas e cativantes e mostre aos usuários a importância de ser um profissional consciente.

6 ANALISE E GERENCIE

A eficácia de um programa de conscientização e sua capacidade de trazer resultados depende de um programa de gestão das métricas que vai permitir entender os possíveis pontos de atenção, necessidade de aumento de escopo, comunicação com gestores responsáveis e replanejamento da sua estratégia da campanha.

1. IDENTIFIQUE SEU PÚBLICO

Sabemos que dentro de uma empresa as pessoas possuem diferentes conhecimentos de como se comportar diante das ameaças digitais e de como proteger informações. Isso por conta das experiências anteriores de cada um e da forma que as empresas nas quais elas já passaram lidavam com segurança da informação. Além disso, **os colaboradores possuem diferentes níveis de acesso às informações** dependendo do cargo ou função que ocupam.

Por isso, o primeiro passo para desenvolver um Programa de Conscientização em Segurança da Informação é entender o seu público e definir o seu alvo.

Um programa de conscientização deve ser desenvolvido tendo em vista todos os usuários da empresa. Por isso, entender a demografia da sua empresa, levantando o **número de pessoas**, sua **localização** e seus diferentes **idiomas** é fundamental.

É desejável que o programa envolva todos os colaboradores da organização com o objetivo de **nivelar conhecimento** e assim trazer uma base comum de comportamento seguro.

Com esta base estabelecida, é preciso endereçar necessidades relacionadas a grupos específicos. Dependendo do tamanho e complexidade da empresa e do nível de maturidade que o programa alcançar, recomenda-se agrupar os colaboradores em **segmentos**. Levando em consideração o nível de maturidade, área de atuação, filial, região em que trabalha e idioma, promovendo atividades especializadas como análise de risco, treinamentos e ações de impacto como palestras.

Uma forma de testar se a estratégia, o conteúdo, a conscientização e a educação foram definidas de maneira adequada é iniciar o programa com um público restrito.



Identifique líderes apoiadores para envolver no seu programa de conscientização, esta amostragem irá ajudar no direcionamento da mensagem e no teste dos canais de comunicação disponíveis.

2. ENTENDA SEU AMBIENTE

Um Programa de Conscientização de sucesso deve ser adaptado às necessidades específicas de cada organização, para que o investimento seja direcionado na mudança de comportamento que irá trazer valor e visibilidade ao negócio. Para isso, deve-se levar em conta os seguintes critérios de avaliação:

Principais riscos associados ao fator humano

No ambiente das organizações existem alguns comportamentos inadequados que ressaltam aos olhos. Em algumas, existe uma cultura de compartilhamento de senhas e em outras é muito comum ouvir pessoas conversando assuntos sigilosos em espaços públicos. Endereçar os principais comportamentos de riscos dos usuários vai ajudar nas ações de mudança de cultura que mais trazem ameaças para a organização. **Históricos de incidentes de segurança** e **análises de risco** são ferramentas usadas como input no processo de identificação destes riscos.

Entender os objetivos legais, regulatórios ou de auditoria

Dependendo do segmento da organização e a sua forma de atuação, existem obrigações legais e regulatórias das quais ela precisa cumprir. No desenvolvimento do Programa de Conscientização este cenário deverá ser considerado para que a mensagem esteja alinhada e em conformidade com as estratégias definidas pela empresa.

Nível de maturidade de conscientização

Para desenvolver um Programa é importante saber aonde você está. Entender qual o nível de maturidade é crucial para determinar a evolução do seu programa e aonde você quer chegar.

Para isso, identifique as ações de conscientização que já foram executadas previamente e classifique em:



Quando uma empresa nunca fez ações de conscientização deverá entender que o básico de segurança deve ser o foco desta campanha, divisão de conteúdo para corporação, neste momento, não é o caminho ideal. Deve-se criar uma base para o assunto Segurança da Informação, e quando o nivelamento de conhecimento for alcançado e os usuários tiverem a noção de que existe o tema segurança, a empresa está pronta para o próximo nível.

Afinal, como ensinaremos melhores práticas se o usuário ainda não está convencido da importância do assunto pra vida pessoal e profissional.

Canais de comunicação disponíveis

Para que você se comunique com seu público será necessário utilizar os canais de comunicação da empresa. Os meios de comunicação internos são ferramentas utilizadas pelas empresas para estabelecer um relacionamento e se comunicar com os funcionários.

Porém, para atingir todo o seu público alvo, possivelmente, você precisará utilizar diversos desses canais.

Por esse motivo, é importante saber identificar qual a melhor maneira de transmitir a sua mensagem para público, em cada localização e em cada canal. Neste passo, é importante ter a Área de Comunicação como aliada, pois além de ser gestora destes canais, ela conhece a efetividade de cada um deles e poderá te ajudar na definição da estratégia do uso desses recursos.

3. DEFINA A ESTRATÉGIA E OBJETIVOS

Nesta fase do programa é hora de determinar os recursos, pessoas e processos com base nos objetivos do programa.

OBTENHA PATROCÍNIO

Obter o apoio e patrocínio da alta administração é talvez o aspecto mais crucial para o programa de conscientização. É vital construir um consenso entre os tomadores de decisão de que o programa de conscientização não é só importante para o negócio como também o tornará mais competitivo. Se os principais interessados não compreenderem o imperativo de um programa de conscientização de segurança da informação e não apoiarem os objetivos e metas, a iniciativa não seguirá em frente. Como administradores da empresa, eles precisam saber que seu negócio está seguro e protegido tendo visibilidade por meio de informações fornecidas por feedback e métricas, melhorias na conscientização de segurança em toda a organização também ficarão aparentes.

FAÇA ALIANÇAS

É aqui que o conceito de gerenciamento de partes interessadas entra em jogo. Procurar dentro da organização áreas que vão apoiar e contribuir para a implementação do programa tornará o processo muito mais fácil.

A equipe de TI, RH, Comunicações, Treinamento e Desenvolvimento tem experiência e formações mais adequadas para determinadas ações dentro do programa de conscientização.

Buscar apoio com áreas pares e principalmente consultá-las serve a um propósito de gerenciamento de partes interessadas, pois pode ajudar a obter seu apoio para a execução do programa. O não envolvimento destas áreas pode inadvertidamente colocá-los contra isso.

DEFINA PAPÉIS E RESPONSABILIDADES

Antes de iniciar o programa deixe claro os papéis e responsabilidades da equipe responsável pelo desenvolvimento, entrega e manutenção em todas as fases. Recomenda-se que a equipe seja composta por pessoal de diferentes áreas da organização, com responsabilidade que representem uma seção transversal da organização.

RECURSOS DISPONÍVEIS

Para executar o programa de conscientização você precisará de recursos para apoiar a iniciativa. Esses recursos envolvem tanto pessoas com experiência para gerir a iniciativa quanto os custos associados ao desenvolvimento, produção e entrega de materiais de conscientização. Se já existir pessoal com experiência adequada na organização, esses indivíduos precisarão ser destacados para o projeto. Caso contrário, seu orçamento deverá incluir os custos associados à terceirização. Essa definição traz consigo o desafio de identificar o que pode ser terceirizado, garantindo que ações estratégicas sejam assumidas por recursos internos.

ESTABELEÇA UM PLANO DE TRABALHO

Com todas essas informações levantadas e definidas é hora de elaborar um plano de trabalho determinando seus objetivos, o que você deseja alcançar e seus marcos. Tenha em mente que estes objetivos devem ser claros e viáveis de acordo com os recursos disponíveis. Este plano deverá ser dinâmico e estará em constante revisão conforme o desenvolvimento do seu programa de conscientização.

Quando temos um plano de ação sabemos o caminho que queremos percorrer, além de processos, liberações e apoio que teremos que alcançar ao longo do caminho. Transformar ações pontuais em ações periódicas é fundamental para alcançar uma mudança de cultura. Afinal, tudo precisa ter constância para se tornar um hábito. E quando falamos do cenário de proteção onde ataques novos aparecem diariamente, senhas são vazadas e rotatividade de funcionários é uma realidade, optar pelo pontual é contar com a sorte que nada aconteça até a próxima campanha.

4. ESTABELEÇA MÉTRICAS

A chave do sucesso de um programa de conscientização depende intrinsecamente da sua capacidade de gerar métricas. A avaliação de um programa por meio de indicadores é essencial para entender sua eficácia, ajustar seu caminho e torná-la ainda mais bem-sucedida direcionando os investimento corretamente.

Em geral, existem duas categorias principais para medir a efetividade do programa de conscientização:

MÉTRICAS DE RISCO:

Esta categoria fornece indicadores de nível de conhecimento e comportamentos dos usuários diante de ameaças potenciais representadas em porcentagem.

Métrica de maturidade dos usuários

Índice de conhecimento dos usuários acerca dos temas de segurança. Pode ser medida por meio de pesquisa quantitativa que endereçam questões com cenários de risco, o que possibilita identificar o quanto as pessoas estão conscientes das suas atitudes no dia a dia.

Métrica de Comportamento Inadequado

Índice que indica o comportamento do usuário quando ele se encontra diante ao risco. É medida utilizando técnicas qualitativas para capturar a sensação dos funcionários em relação à conscientização e se eles realmente exercem a consciência de segurança por meio de simulações de situações de risco. É aqui que você entende como o usuário irá se comportar quando ele receber um e-mail phishing, por exemplo.

Essas métricas são essenciais para:

Direcionar a estratégia do programa

Identificar temas com menor índice de conhecimento

Departamentos ou pessoas com menor índice de conhecimento por tema

Departamentos que necessitam diferentes abordagens



5. ENGAJE E TREINE

A segurança cibernética dificilmente é conhecida por ser o tópico mais sexy do mundo. Aos olhos de muitos é limitador e enfadonho. Porém, é um assunto útil para todo mundo, tanto profissionalmente como pessoalmente.

Mudar uma cultura requer mudar as pessoas, mudando a forma como elas pensam e percebem os problemas. Para promover essa mudança cultural, o programa de conscientização deve conquistar todos para a causa de segurança da informação. E para fazer isso, alguns pontos devem ser levados em consideração, por exemplo:

CULTURA DA EMPRESA

Os aspectos culturais da empresa devem estar alinhados na estratégia de comunicação do programa de conscientização. E não são as senhas, o software antivírus ou as políticas que constituem a cultura de segurança da informação de uma organização. É sim, na maneira que as pessoas percebem como a organização enxerga e trata os problemas de segurança. No processo de mudança cultural é importante mudar a cultura de maneira imperceptível, aproveitando todas as oportunidades para cultivar as ideias da organização sobre como proteger as informações.

CONEXÃO COM A AUDIÊNCIA

Provavelmente você já assistiu a um vídeo no YouTube com um conteúdo que normalmente nunca assistiria, mas, pelo fato de o vídeo te ajudar a resolver um problema ele se tornou interessante e você gostou de assisti-lo.

Por isso, a mensagem de qualquer processo de conscientização deve gerar interesse no receptor para que ela impacte no seu processo de mudança. As pessoas têm formas e tempos distintos de aprendizado, por isso, não há como definir um modelo padrão e ideal para um grupo. Porém, existem algumas técnicas e mecanismos que, efetivamente, colaboram para o conhecimento de todos:

Faça um paralelo com a vida pessoal

O processo de conscientizar as pessoas a proteger as informações da empresa não pode ser entendido separadamente do processo de tomada de consciência da importância da proteção para suas próprias informações e sua privacidade. Só a partir do momento que este valor for incorporado será possível ser propagado para o contexto corporativo.

Mostre benefício

Alinhe sua mensagem se atentando às necessidades do seu interlocutor, mostrando soluções que contribuam para suas atividades, mesmo que isso traga maior esforço.

Use a criatividade

Criar conteúdo é uma coisa, impactar é outra. Campanhas criativas promovem a curiosidade, motivam e despertam o interesse, proporcionando assim, maior retenção do conteúdo e, conseqüentemente, o seu aprendizado. Você precisa falar a língua do seu público e se isso significa ser mais ousado e informal, seja. Por isso, a utilização de materiais lúdicos e divertidos, abrindo mão do tom corporativo ou de jargões, vão contribuir com o desafio de conscientizar acerca da proteção, sem tirar a seriedade do assunto.

#DICA DE OURO

Tenha um canal de geração de conteúdo jornalístico especializado em segurança da informação e mantenha sempre um excelente relacionamento com a Área de Comunicação. Estas parcerias vão te trazer o melhor dos mundos: **conteúdo especializado e acesso aos usuários.**



6. ANALISE E GERENCIE

A gestão do programa de conscientização tem como objetivo avaliar a eficácia e revelar deficiências na estratégia utilizada, além de considerar a efetividade das abordagens utilizados na entrega dos materiais ou no próprio conteúdo. Também ajuda a justificar o investimento em iniciativas de conscientização de segurança e a incentivar o aumento da atividade do programa.

1) Avaliação de Efetividade:

Medir a efetividade da campanha de conscientização requer levar em consideração as seguintes questões:

- Se a informação atingiu o alvo de maneira efetiva - Esse é o aspecto mais importante na avaliação do programa de conscientização, pois avalia quantas pessoas realmente absorveram a informação entregue e, portanto, se o objetivo principal do programa, que é formar pessoas conscientes, foi alcançado.



- A medição da eficácia é realizada por meio de análise das métricas de risco e de engajamento. Com essa metrificação é possível identificar se a abordagem de canais e conteúdos requer pequenas melhorias ou modificações de percurso. A correlação dessas métricas fornece indicadores do comportamento real dos usuários. O usuário pode participar de todos os treinamentos, ter pontuação máxima nas avaliações, mas falhar nas simulações no momento em que se é apresentado uma situação de risco. **No quadrante ao lado é possível observar um exemplo da relação entre as métricas de risco e engajamento por departamento, e com isso, identificar as recomendações e os pontos que necessitam de atenção.**

QUADRANTE 2: GRUPO DE ATENÇÃO

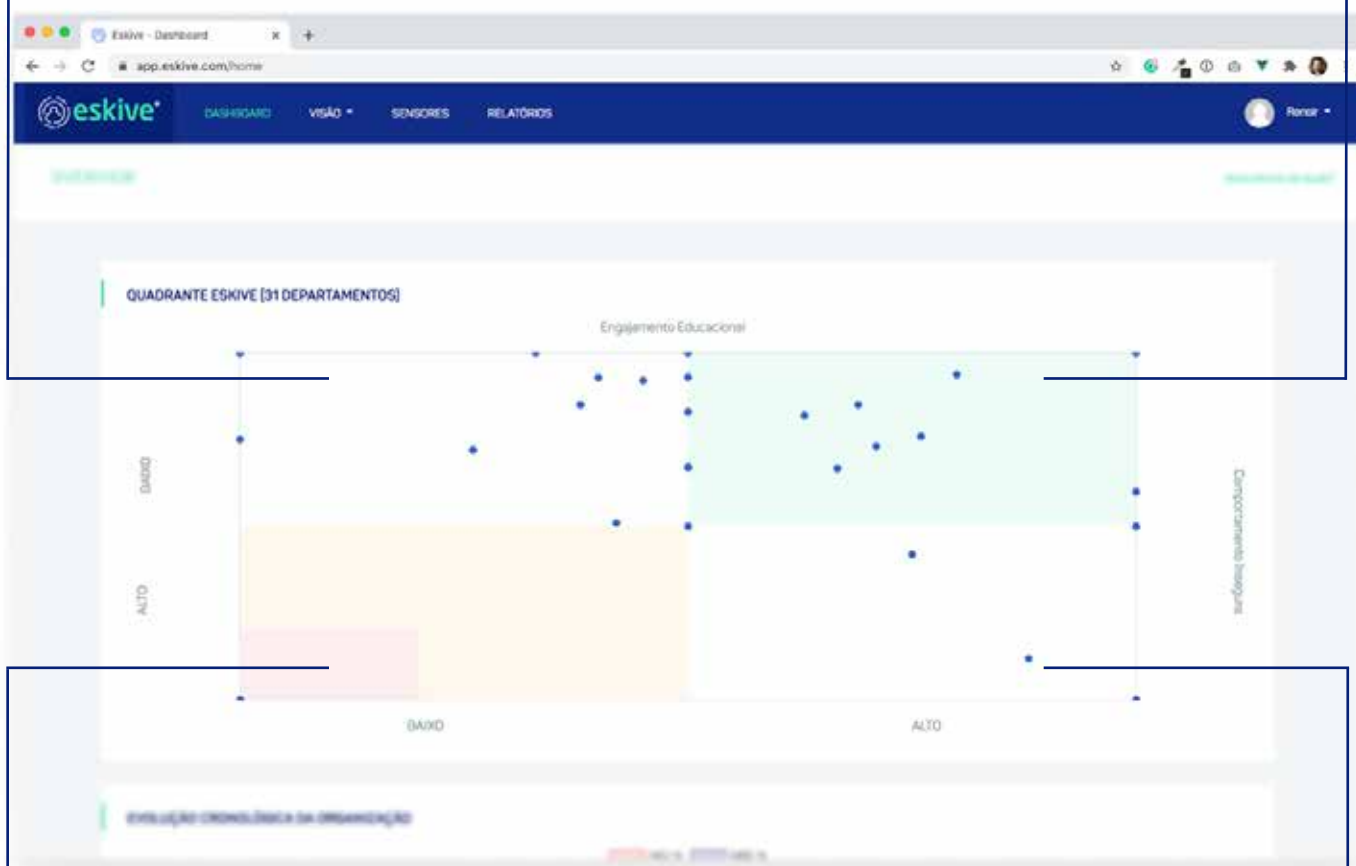
Departamentos com baixo engajamento educacional e baixo comportamento inadequado.

RECOMENDAÇÕES: Priorizar grupo em ações presenciais e impacto.

QUADRANTE 1: GRUPO IDEAL

Departamentos mais engajados em conteúdos educacionais e baixo índice de comportamento inadequado.

RECOMENDAÇÕES: Aumentar o nível das análises de comportamento.



QUADRANTE 3: GRUPO DE RISCO

Departamentos com baixo engajamento educacional e alto índice de comportamento inadequado.

RECOMENDAÇÕES: Priorizar grupo em ações presenciais e impacto. Buscar apoio das lideranças para reverter esse cenário.

QUADRANTE 4: GRUPO MALICIOSO

Departamentos mais engajados em conteúdos educacionais e alto índice de comportamento inadequado.

RECOMENDAÇÕES: Segmentar ações de conscientização para esse grupo. Revisar abordagem e buscar apoio das lideranças.

Assumindo todos estes pontos de avaliação será possível determinar se é significativo continuar investindo ou focar em outras abordagens mais eficazes. **A equipe não deve hesitar em investigar abordagens comprovadamente ineficaz.**

Se a estratégia definida é a mais adequada - Avaliar a eficácia da estratégia constitui identificar se os objetivos definidos foram alcançados, observando os pontos fracos do programa. Alguns questionamentos são importantes para constatar o que pode ter comprometido o alcance deste objetivo, por exemplo: O apoio necessário para realização do programa foi adequado? O orçamento destinado foi suficiente? A estratégia de divulgação precisa ser redefinida? (analisar fatores como se o volume do conteúdo foi adequado para não sobrecarregar o usuário).

Além disso, determinar se os incidentes relacionados à conscientização de segurança estão diminuindo, pode trazer à tona questões que o grupo deveria ter abordado, mas foram deixadas de fora do programa.

2) Processo de Melhoria



Os resultados da avaliação do programa devem apontar para um processo de melhoria contínua. Conforme o programa vai passando por diversos ciclos, uma base comparativa vai se formando e se torna um indicador de sucesso.

A equipe de conscientização deve avaliar suas práticas em relação às necessidades identificadas e a capacidade de entrega com base no plano de trabalho detalhado na etapa de definição da estratégia. Recomenda-se que os períodos de campanha sejam cíclicos para que ao final de cada campanha seja feita uma avaliação quanto a eficácia do programa lançado.