VANTICO

Plano prático para **Conscientização** em **Cibersegurança**

Nesse material você vai encontrar...

Orientações para criar um plano de 30 ou 90 dias de conscientização em segurança cibernética, incluindo formato, objetivo e sugestão para as ações, além de métricas para medir sua eficiência.

Recomendamos que, com base nesse material, você faça as alterações necessárias para implementar no contexto da sua empresa e time.

E LEMBRE-SE:

Outubro é o mês da conscientização em Segurança Cibernética, mas, para manter-se realmente à frente das ameaças, é preciso ter continuidade!

Plano de 30 dias

Métricas e KPIs sugeridos

Mensure desde o 1º dia.

01. Taxa de clique em simulações de phishing (target inicial < 20% e redução contínua).

02. Taxa de reporte de phishing (percentual de usuários que reportam suspeitas).

03. Taxa de completude do micro-treino (meta ≥ 90% em cada semana).

04. Tempo médio para reportar incidente suspeito (minutes/hours).

05. Pontuação de cultura (pesquisa rápida de percepção pré e pós 30 dias).

06. SANS e CISA destacam que medir comportamento e reportes é tão importante quanto treinar.

Semana 1

Higiene Digital

Dias 1 a 7 | **Objetivo:** garantir controles básicos.

Dia 1: Abertura e compromisso
Comunicado do CEO / Diretor: “30 dias para melhorar nossa defesa humana”. Explique objetivos e KPIs.

Dia 2: Senhas e MFA
Mini-treinamento: por que senhas fracas falham e como ativar MFA em serviços críticos (passkeys / FIDO2 quando possível). A NIST recomenda autenticação forte.

Dia 3: Atualizações e patching pessoal
Checklist rápido: habilite atualizações automáticas em notebook e celular.

Dia 4: Bloqueio de tela e dispositivos
Ative bloqueio automático; política sobre telas desbloqueadas.

Semana 1

Higiene Digital

Dias 1 a 7 | **Objetivo:** garantir controles básicos.

Dia 5: Segurança de e-mail
Sinais de e-mail suspeito: remetente estranho, pedido urgente, links encurtados, anexos inesperados. O CISA recomenda treinar para reconhecer esses sinais.

Dia 6: Mídias removíveis e políticas USB
Evite uso de pendrives desconhecidos; use controles DLP/whitelist.

Dia 7: Check-in
Resumo semanal por e-mail.

Semana 2

Resistência ao phishing

Dias 8 a 14 | **Objetivo:** reduzir cliques e aumentar reporte.

Dia 8: Anatomia do phishing
Carrossel explicando técnicas: spear-phishing, business e-mail compromise (BEC), vishing.

Dia 9: Verificação rápida
Treino prático: 3 perguntas antes de clicar (é esperado? vem de canal conhecido? pede ação financeira?).

Dia 10: Links e anexos seguros
Como checar links sem clicar (hover, copiar e colar, sandbox). Recomende ferramentas corporativas.

Dia 11: Telefone e vishing
Simulação de cenários com reposta correta (role-play para líderes).

Semana 2

Resistência ao phishing

Dias 8 a 14 | **Objetivo:** reduzir cliques e aumentar reporte.

Dia 12: Social engineering awareness
Post com exemplos reais (anonimizados) e como reportar.

Dia 13: Simulação leve de phishing
Envio de phishing simulado com objetivo de aprender. SANS recomenda combinar simulações com briefings educacionais.

Dia 14: Retorno e lições
Relatório simples aos times: taxa de clique, quem reportou, mensagens de reforço.

Semana 3

Trabalho remoto, cloud e dispositivos

Dias 15 a 21 | **Objetivo:** fortalecer postura em home office e cloud sharing.

Dia 15: VPN e Wi-Fi seguro
Políticas: não usar redes públicas sem VPN corporativa.

Dia 16: Proteção de endpoints móveis
Atualize políticas MDM/MDM checks; configurar criptografia.

Dia 17: Compartilhamento seguro em nuvem
Configurações de link compartilhado, expiração, permissões “view only”.

Dia 18: Backup e recuperação pessoal
Sensibilizar sobre importância de backups críticos e versions (não só ransomware).

Semana 3

Trabalho remoto, cloud e dispositivos

Dias 15 a 21 | **Objetivo:** fortalecer postura em home office e cloud sharing.

Dia 19: Gerenciamento de permissões
Princípio do least-privilege: quem realmente precisa daquele acesso?

Dia 20: Revisão de apps e integrações
Verifique apps conectados às contas corporativas (OAuth) e revogue as obsoletas.

Dia 21: Mini-exercício: cenário remoto
Simule um pedido urgente de troca de conta via chat, verificar processo de validação.

Semana 4

Cultura, resposta e continuidade

Dias 22 a 30 | **Objetivo:** consolidar hábitos, planejar próximos passos e integrar com governança.

Dia 22: Privacidade e LGPD / proteção de dados
Boas práticas ao manusear dados pessoais e sensíveis.

Dia 23: IoT e dispositivos compartilhados
Políticas rápidas para impressoras, TVs e dispositivos de salas de reunião.

Dia 24: Supply chain awareness
Verificar proveniência de software e dependências, conscientizar sobre riscos em terceiras partes (SBOM awareness).

Dia 25: Incidente: o que fazer se você clicou
Passo a passo prático: desconectar, reportar, não tentar “consertar” sozinho.

Semana 4

Cultura, resposta e continuidade

Dias 22 a 30 | **Objetivo:** consolidar hábitos, planejar próximos passos e integrar com governança.

Dia 26: Tabletop (mini) para liderança
Exercício de 30 minutos com 2–3 executivos sobre um incidente simulado e comunicações.

Dia 27: Revisão de políticas e autorizações
Checar listas de aprovadores financeiros e processos de confirmação multicanal.

Dia 28: Survey de clima e cultura
Curta pesquisa (5 perguntas) para medir percepção e confiança.

Dia 29: Plano de 90 dias (próximos passos)
Entregue roadmap: treinamentos, controles, PTaaS / pentest, BAS, threat hunting.

Dia 30: Reconhecimento e encerramento
Agradeça a participação e mostre KPIs alcançados. Publique resumo executivo interno.

Plano de 90 dias

Semanas 1 a 3

Fundamentos e postura individual

Objetivo: nivelar conhecimento básico, reduzir erros simples e criar compromisso organizacional.

01. Abertura executiva e alinhamento
Formato: reunião plenária com liderança (apresentação + Q&A).
Objetivo: explicar propósito, regras, expectativas e próximos passos.

02. Treinamento rápido: Senhas e autenticação
Formato: explainer + checklist impresso/ PDF.
Objetivo: melhores práticas para senhas e ativação de MFA.

03. Workshop curto: Proteção de dispositivo
Formato: sessão interativa sobre bloqueio de tela, atualizações, MDM.
Objetivo: confirmar configuração mínima nos dispositivos corporativos.

Semanas 1 a 3

Fundamentos e postura individual

Objetivo: nivelar conhecimento básico, reduzir erros simples e criar compromisso organizacional.

04. Treinamento rápido: E-mail seguro
Formato: 3 heurísticas práticas para avaliar e-mails suspeitos.
Objetivo: reduzir cliques impulsivos.

05. Sessão prática: Uso seguro de pendrives e impressoras
Formato: demonstração com dispositivos de teste (ao vivo).
Objetivo: reforçar políticas de mídias removíveis e impressão segura.

06. Atividade de leitura comentada
Formato: breve resumo de 1 artigo (ex.: “phishing moderno”) + discussão em pequenos grupos.
Objetivo: entendimento contextual das ameaças.

Semanas 1 a 3

Fundamentos e postura individual

Objetivo: nivelar conhecimento básico, reduzir erros simples e criar compromisso organizacional.

07. Retrospectiva curta com líderes
Formato: reunião de líderes para ajustar comunicações da próxima semana.
Objetivo: alinhar tom e logística.

Semanas 4 a 6

Resistência a Phishing e engenharia social

Objetivo: treinar reconhecimento e resposta a tentativas de engenharia social (inclui vishing e smishing).

08. Treinamento rápido: Sinais de phishing avançado
Formato: exemplos anonimizados e checklist de verificação.

09. Role-play em pares: Vishing
Formato: exercícios ao vivo, dois a dois, com scripts controlados (sem gravação).
Objetivo: praticar respostas a chamadas suspeitas (como confirmar identidade por outro canal).

10. Workshop: Protegendo processos financeiros
Formato: sessão com Finance/Legal/IT sobre regras de autorização e verificação multicanal.
Objetivo: definir gatilhos e procedimentos de confirmação.

11. Práticas: Comunicações instantâneas
Formato: regras práticas para Slack/Teams/WhatsApp corporativo.

Semanas 4 a 6

Resistência a Phishing e engenharia social

Objetivo: treinar reconhecimento e resposta a tentativas de engenharia social (inclui vishing e smishing).

12. Exercício controlado de reporte
Formato: equipe reporta 1 ou 2 mensagens “suspeitas” internas; feedback coletivo.
Objetivo: praticar o fluxo de reporte e escalonamento.

13. Workshop: Como conduzir uma verificação multicanal
Formato: simulação de caso (financeiro/recursos humanos) com decisão conjunta.

14. Mesa redonda com SOC
Formato: SOC explica o que acontece após um reporte; Q&A.
Objetivo: fechar ciclo de aprendizado sobre reporte e resposta.

Semanas 7 a 9

Segurança para funções críticas

Objetivo: treinar grupos por função com conteúdos práticos e alinhados ao seu risco.

15. Sessão Dev: Segurança em APIs e autenticação
Formato: workshop prático com exemplos de design seguro e checklists para code review.

16. Sessão Finance: prevenção a fraudes
Formato: role-plays de cenário de fraude + definição de processo de confirmação.

17. Sessão RH: proteção de dados de colaboradores
Formato: práticas de manuseio de dados sensíveis e comunicação segura.

18. Sessão Comercial / Parcerias: contratos e riscos de terceiras partes
Formato: checklist de due diligence e perguntas obrigatórias sobre segurança em contratos.

Semanas 7 a 9

Segurança para funções críticas

Objetivo: treinar grupos por função com conteúdos práticos e alinhados ao seu risco.

19. Workshop prático: hardening de endpoints para área técnica
Formato: hands-on guiado (ex.: configurações básicas, EDR checks).

20. Sessão Execs: riscos emergentes
Formato: foco em decisões (p.ex., investimento em mitigação), sem detalhes operacionais.

21. Feedback de funções
Formato: líderes de cada área sintetizam mudanças práticas a adotar.

Semanas 10 a 12

Resposta a incidentes, tabletop e integração

Objetivo: treinar coordenação entre áreas, validar playbooks e planejar continuidade.

22. Treinamento rápido: primeiros passos após um incidente
Formato: passo a passo simples: isolar, reportar, preservar evidências (sem expor logs).

23. Tabletop executivo
Formato: cenário simulado (anonimizado) para executivos praticarem comunicação e decisões.
Objetivo: melhorar escalonamento e comunicação ao board.

24. Tabletop operacional (90 min)
Formato: SOC + TI + Business - executar steps do playbook em tempo real.

25. Workshop de forense inicial para TI
Formato: como preservar evidências, coletar pcaps e acionar especialistas; prática sem registro.

Semanas 10 a 12

Resposta a incidentes, tabletop e integração

Objetivo: treinar coordenação entre áreas, validar playbooks e planejar continuidade.

26. Exercício de comunicação com clientes e parceiros
Formato: criar template de comunicado e rotinas de divulgações controladas.

27. Simulação de cenário "phishing + fraude" em pequena escala
Formato: envio de um caso preparado que testa o fluxo de detecção, reporte e decisão.

28. Revisão coletiva de playbooks e ajustes
Formato: consolidar melhorias e responsáveis por ações.

29. Planejamento de continuidade
Formato: roadmap de treinamentos contínuos e integração com PTaaS / pentest.

Semanas 10 a 12

Resposta a incidentes, tabletop e integração

Objetivo: treinar coordenação entre áreas, validar playbooks e planejar continuidade.

30. Encerramento e compromisso formal
Formato: comunicado final dos líderes com compromissos concretos e próximos passos.

VANTICO

Gostou desse conteúdo?

Continue nos acompanhando para mais.

Kaique Bonato

Vantico

Site

Blog