Proposta de Treinamento e Conscientização para a Empresa de Cartões de Crédito **Copacki**

01 de Novembro 2024

1 Escopo

Este documento apresenta uma proposta de treinamento e conscientização para as diversas equipes da empresa de cartões de crédito Copacki, focando em práticas de segurança da informação, com base nos controles do NIST, CIS, ISO 27001 e PCI-DSS. Além disso, a empresa se compromete a se adequar à Lei Geral de Proteção de Dados (LGPD) e outras legislações pertinentes, garantindo que todas as atividades respeitem as normas de proteção de dados e privacidade, promovendo uma cultura de segurança que abrange tanto a proteção de informações sensíveis quanto a conformidade legal.

2 Introdução

Em um cenário onde o trabalho remoto se torna cada vez mais comum, a proteção de informações sensíveis é crucial. Este programa visa equipar os colaboradores com conhecimentos necessários para identificar e mitigar riscos de segurança, assim, mantendo a empresa mais segura e controlada.

3 Objetivos

- **Reduzir Vulnerabilidades**: Vamos diminuir as oportunidades para ataques à empresa. Isso incluirá revisar quem tem acesso a informações sensíveis e desativar serviços desnecessários. Realizaremos auditorias regulares para identificar e corrigir problemas de segurança.
- **Aumentar a Conscientização sobre Segurança da Informação:** Queremos que todos os colaboradores saibam como se proteger online. Implementaremos um programa de treinamentos regulares sobre como identificar ameaças como phishing e como proteger dados. Além disso, faremos campanhas contínuas para lembrar as melhores práticas de segurança.
- **Fazer os Funcionários se Sentirem Parte da Empresa:** Vamos incentivar a participação ativa de todos na segurança da empresa. Isso inclui criar um programa onde alguns funcionários se tornam "embaixadores de segurança" e promover eventos que envolvam todos. Reconheceremos publicamente os esforços dos colaboradores nessa área.

- **Realizar Avaliações Regulares de Segurança:** Faremos testes e auditorias periódicas para identificar e corrigir vulnerabilidades. Os resultados ajudarão a melhorar continuamente nossas políticas de segurança.

  Integrar Segurança em Todos os Níveis: A segurança deve ser uma responsabilidade de todos. Formaremos um comitê de segurança com representantes de diferentes áreas da empresa para garantir que todos estejam envolvidos na proteção da informação.

- **Aumentar a Transparência sobre Segurança:** Vamos manter todos informados sobre as práticas de segurança e qualquer incidente que ocorra. Relatórios regulares ajudarão a reforçar a importância da segurança e o papel de cada um.

- **Adaptar-se a Novas Ameaças:** A cibersegurança é um campo em constante mudança. Investiremos em treinamentos contínuos e em pesquisa para que a empresa esteja sempre pronta para enfrentar novas ameaças.

4 Público-Alvo

O público-alvo abrange todos os 1.000 funcionários da empresa, com uma atenção especial aos 500 colaboradores que trabalham remotamente. Essa ênfase nos trabalhadores remotos é crucial, pois eles enfrentam desafios únicos em termos de segurança da informação e precisam de orientações específicas para garantir a proteção de dados enquanto operam fora do ambiente corporativo.

5 Tempo de Duração

O programa de treinamento e conscientização em cibersegurança terá uma duração inicial de 3 meses. Durante esse período, a presença dos funcionários será obrigatória em todas as atividades mensais, que abordarão temas essenciais relacionados à segurança da informação. Avaliações periódicas serão realizadas para medir o progresso e a compreensão dos participantes. Além disso, sessões de reforço serão oferecidas para consolidar o aprendizado e garantir que todos os colaboradores se sintam preparados para enfrentar possíveis ameaças. Para assegurar um acompanhamento contínuo, testes serão aplicados ao longo de todo o ano. Caso algum funcionário não esteja totalmente preparado ao final dos 3 meses, o treinamento poderá ser estendido, proporcionando o suporte necessário até que todos atinjam um nível satisfatório de competência em cibersegurança.

6 Recompensas

Como parte do programa de treinamento e conscientização em cibersegurança, serão oferecidas diversas recompensas para incentivar a participação e o engajamento dos colaboradores. Além de brindes como garrafas, chocolates e copos personalizados, os funcionários poderão ganhar vouchers para experiências, como jantares ou ingressos para eventos. Também será considerada a possibilidade de reconhecimento público, com menções em newsletters da empresa e em reuniões, destacando os esforços e a dedicação dos participantes. Outro tipo de recompensa será a oferta de dias de folga ou horários flexíveis

para aqueles que completarem com sucesso todos os módulos do treinamento. Essas iniciativas visam promover um ambiente de aprendizado positivo e motivador, reforçando a importância da segurança da informação.

7 Métricas de Avaliação e Acompanhamento

Para avaliar a eficácia do programa de treinamento e conscientização em cibersegurança, serão utilizadas diversas estratégias. Serão aplicados questionários de avaliação pós-treinamento para medir a compreensão dos colaboradores, além da análise de relatórios de incidentes de segurança para identificar áreas de melhoria. O feedback qualitativo dos participantes ajudará a entender suas experiências e sugestões.

Adicionalmente, avaliações práticas permitirão que os funcionários demonstrem suas habilidades em situações simuladas. Testes regulares ao longo do ano e a observação do comportamento em relação às práticas de segurança também contribuirão para monitorar o progresso e promover uma cultura de segurança na empresa.

8 Medidas de Segurança Abordadas

- Gestão de senhas.
- Identificação de phishing e fraudes online.
- Proteção de dados pessoais e sensíveis.
- Uso seguro de redes públicas.
- Autenticação de Dois Fatores (2FA)
- Segurança em dispositivos móveis.
- Educação sobre engenharia social.
- Backup de dados.
- Políticas de uso aceitável.
- Segurança em e-mails.
- Gerenciamento de acessos.
- Monitoramento de atividades suspeitas.
- Treinamento contínuo.

9 Tipos de Treinamento

1. Vídeos de conscientização sobre segurança.
2. Palestras ao vivo com especialistas em segurança.
3. Campanhas de e-mail sobre boas práticas.

4. Materiais impressos (cartazes, folhetos).
5. Cursos online interativos.
6. Eventos presenciais de simulação de ataques.
7. Workshops sobre uso seguro de dispositivos móveis.
8. Simulações de phishing.
9. Webinars sobre novas ameaças cibernéticas.
10. Treinamentos sobre regulamentações (ex: PCI-DSS).
11. Testes de conhecimento em segurança.
12. Estudos de caso sobre incidentes reais.
13. Atualizações trimestrais de segurança.
14. Sessões de perguntas e respostas.
15. Formação de um grupo de segurança entre pares.
16. Desafios gamificados sobre segurança.
17. Podcasts sobre tópicos de segurança da informação.
18. Artigos e newsletters mensais.
19. Simulacros de resposta a incidentes.
20. Programa de embaixadores de segurança.
21. Materiais de referência (checklists, guias).

10 Ferramentas Auxiliares

- Plataformas de Edtech para cursos online (ex: Moodle, Canvas).
- Ferramentas de simulação de phishing (ex: KnowBe4, PhishMe).
- Softwares de gestão de aprendizado (LMS).
- Ferramentas de feedback e avaliação (ex: SurveyMonkey).
- Vídeos do Hacker Rangers.
- Vídeos recomendados e/ou feitos pela nossa equipe.

11 Resultados Esperados

Espera-se que a empresa esteja plenamente integrada à campanha de conscientização em cibersegurança. A colaboração entre as equipes será essencial para garantir que todos entendam a importância da segurança da informação e se sintam motivados a participar. Os resultados esperados incluem a redução de incidentes de segurança, maior capacidade de identificar ameaças e a promoção de uma cultura organizacional que prioriza a segurança. Além disso, o feedback contínuo será fundamental para aprimorar as práticas de conscientização e garantir a evolução do conhecimento sobre segurança da informação.

Por fim, espera-se que a equipe se sinta parte integrante da empresa, mais segura e confortável em seu ambiente de trabalho.

12 Conclusão

A implementação deste programa de treinamento e conscientização em cibersegurança trará benefícios significativos para a empresa. Primeiramente, a redução de incidentes de segurança contribuirá para um ambiente de trabalho mais seguro e protegido, mitigando riscos que possam impactar operações e dados sensíveis. Em segundo lugar, ao promover uma cultura sólida de segurança da informação, a empresa capacitará seus colaboradores a reconhecer e responder proativamente a ameaças, criando um compromisso coletivo com a proteção de dados. Por fim, a conscientização e a formação adequadas resultarão em um aumento da confiança dos clientes em nossos serviços, reforçando a reputação da empresa no mercado e estabelecendo relacionamentos mais sólidos com nossos clientes. Com esses resultados, a empresa estará melhor posicionada para enfrentar os desafios da segurança cibernética e a garantir a integridade de suas operações.