# Integração de experiência prática: a comunicação de crise e a cibersegurança

**StrategicLab & DigitaLab 21.12.2023**

**José Gabriel Andrade**
Investigador do Centro de Estudos de Comunicação e Sociedade

Andrade, J.G. (2023, 21 de dezembro). Integração de experiência prática: a comunicação de crise e a cibersegurança [Post em blogue]. Retirado de https://createlab.pt/integracao-de-experiencia-pratica-a-comunicacao-de-crise-e-a-ciberseguranca/

CreateLab

CECS centro de estudos de comunicação e sociedade

Num mundo cada vez mais interligado pela tecnologia, a cibersegurança assume um papel vital na proteção de dados e informações sensíveis. No entanto, apesar dos avanços tecnológicos, as ameaças cibernéticas continuam a representar um desafio constante para empresas e organizações. Diante desse cenário, a comunicação de crise desempenha um papel fundamental na gestão e mitigação de possíveis danos. Antes de qualquer crise ocorrer, é essencial antecipar cenários e estabelecer estratégias de comunicação preventiva. A previsão de crises no espaço da cibersegurança requer uma abordagem proativa, que englobe não apenas a proteção dos sistemas, mas também a prontidão para lidar com potenciais violações ou ameaças. Esta preparação implica a criação de planos de contingência claros e testados, que delineiem os procedimentos a serem seguidos em caso de incidente.

Nesse sentido, com o intuito de destacar a relevância da comunicação de crise no espaço da cibersegurança, importa mencionar iniciativas recentes que têm tentado reforçar essa importância. No final do mês de novembro, foi realizado o Encontro C-Days Açores, um evento promovido pelo Centro Nacional de Cibersegurança (CNCS). Nessa reunião, participaram diversos especialistas que debateram questões cruciais relacionadas com a temática, transformando-se numa oportunidade valiosa para discutir e disponibilizar os estudos e os caminhos que têm sido desenhados a respeito da gestão de crises no âmbito da cibersegurança.

Partilhámos da opinião que antes de qualquer crise ocorrer, é essencial antecipar cenários e estabelecer estratégias de comunicação preventiva. A previsão de crises no espaço da cibersegurança requer uma abordagem proativa, que englobe não apenas a proteção dos sistemas, mas também a prontidão para lidar com potenciais violações ou ameaças. Esta preparação implica a criação de planos de contingência

claros e testados, que delineiem os procedimentos a serem seguidos em caso de incidente. A eficácia da comunicação de crise está intrinsecamente ligada à rapidez e precisão das respostas oferecidas. No contexto da cibersegurança, a agilidade é crucial, pois uma resposta tardia pode agravar consideravelmente os danos. É importante comunicar de forma transparente e honesta, fornecendo informações relevantes, sem comprometer a segurança. Esta abordagem é essencial para preservar a confiança dos clientes, parceiros e do público em geral. Além disso, a comunicação de crise no âmbito da cibersegurança deve ser uma responsabilidade compartilhada por diferentes departamentos dentro de uma organização. A colaboração entre equipas de TI, relações públicas, de âmbito jurídico e de gestão de crises é essencial para garantir uma resposta coordenada e coesa diante de uma ameaça cibernética.

A tecnologia continua a evoluir, trazendo consigo desafios e oportunidades. Nesse sentido, é necessário investir na formação contínua das equipas, bem como na implementação de soluções de segurança robustas e atualizadas - esta abordagem é crucial para mitigar os riscos cibernéticos. A constante adaptação a novas ameaças e a revisão periódica dos planos de comunicação de crise são passos essenciais para manter a resiliência das organizações, permitindo a sua preparação para potenciais ataques.  Finalmente, a comunicação de crise no espaço da cibersegurança não trata apenas da reação a incidentes, mas antes da forma de antecipar, preparar e responder de modo eficaz a potenciais ameaças. A previsão e a prontidão são os pilares fundamentais para mitigar danos, preservar a confiança e manter a integridade das organizações num ambiente tão dinâmico e desafiador como o ciberespaço.

## A Importância da comunicação durante uma crise de cibersegurança

Quando uma crise de cibersegurança surge, a comunicação torna-se a peça-chave na gestão da situação. O impacto de uma violação de segurança pode ser significativo, afetando não apenas a infraestrutura tecnológica, mas também a confiança dos clientes, parceiros e a reputação da organização. Nesse cenário, uma comunicação eficaz desempenha um papel crucial na minimização de danos e na recuperação da confiança perdida. Logo, a transparência imediata é essencial, sendo imprescindível comunicar de forma clara e direta o incidente, bem como os potenciais impactos e as medidas tomadas ou em andamento para resolver a situação - esta reação é fundamental para manter a confiança dos stakeholders.

Terminada uma crise de cibersegurança, a fase de recuperação é crucial para restaurar a confiança dos clientes e reconstruir a reputação da organização. O marketing de crise desempenha um papel fundamental nesse processo, ajudando a mitigar os danos e a reposicionar a empresa de forma positiva no mercado. Assim, é importante valorizar a:

1. **Análise e avaliação pós-crise:** após a resolução da crise, é fundamental realizar uma análise completa do incidente. Isso inclui entender as causas, identificar pontos fracos nos sistemas de segurança e avaliar a eficácia da resposta da empresa. Essa observação serve de base para ações futuras e para aprimorar os protocolos de segurança.
2. **Reconstrução da confiança:** o marketing de crise visa reconstruir a confiança dos clientes e stakeholders. Isso pode ser alcançado por meio de campanhas de comunicação que enfatizem a transparência, o

compromisso renovado com a segurança cibernética e medidas concretas tomadas para evitar incidentes semelhantes no futuro.

3. **Partilha de histórias de sucesso:** destacar histórias de sucesso e recuperação após a crise pode-se transformar numa ferramenta poderosa. Casos de clientes satisfeitos, testemunhos de melhoria na segurança e ações positivas tomadas pela organização podem ser usados para reforçar uma imagem positiva.
4. **Educação e envolvimento:** investir em programas de educação para clientes e funcionários sobre segurança cibernética pode ser uma estratégia eficaz. Isso demonstra compromisso com a proteção dos dados e ajuda a fortalecer a confiança, mostrando que a empresa/instituição está ativamente envolvida na prevenção de futuros incidentes.
5. **Comunicação contínua:** manter uma linha de comunicação aberta e contínua é crucial mesmo após a resolução da crise. Isso pode incluir atualizações regulares sobre novas medidas de segurança, relatórios de conformidade e práticas recomendadas para os clientes.
6. **Revisão e melhoria contínua:** a crise é uma oportunidade para aprender e melhorar. É importante rever constantemente os protocolos de segurança, investir em tecnologias mais avançadas e permanecer vigilante contra ameaças futuras.

Em suma, o marketing de crise é essencial após uma violação de segurança, sendo considerado uma etapa crítica para restaurar a confiança e a reputação da empresa/instituição. A transparência, a comunicação eficaz e a demonstração de ações concretas para evitar futuros incidentes são fundamentais para reconstruir a confiança dos clientes e manter a integridade da marca.