As Falhas Criptográficas, que antes eram conhecidas como Exposição de Dados Sensíveis, subiram uma posição e ficaram em segundo lugar no último top 10 realizado pela OWASP (Open Worldwide Application Security Project). Isso mostra ser um sintoma amplo do que uma causa raiz e o foco está nas falhas relacionadas à criptografia (ou à falta dela). O que muitas vezes leva à exposição de dados confidenciais.

Desta forma, é preciso buscar boas práticas para evitar as falhas criptográficas, que estão elencadas a seguir:

1. Classificação de Dados: Identifique quais dados são confidenciais de acordo com as leis de privacidade, requisitos regulamentares ou necessidades de negócios.
2. Minimize o Armazenamento: Evite armazenar dados confidenciais desnecessariamente. Descarte-os o mais rápido possível ou utilize técnicas como tokenização ou truncamento.
3. Criptografia: Certifique-se de criptografar todos os dados confidenciais armazenados.
4. Algoritmos Fortes: Utilize algoritmos, protocolos e senhas criptográficas fortes e atualizados. Implemente um gerenciamento de senhas adequado.
5. Dados em Trânsito: Criptografe todos os dados em trânsito com protocolos seguros, como TLS. Aplique diretivas como HTTP Strict Transport Security (HSTS).
6. Cache Seguro: Desative o armazenamento em cache para respostas que contenham dados confidenciais.
7. Controles Adequados: Aplique os controles de segurança necessários de acordo com a classificação de dados.
8. Evite Protocolos Legados: Não use protocolos legados, como FTP e SMTP, para transportar dados confidenciais.
9. Hash Seguro: Armazene senhas usando funções de hash adaptáveis e saltadas com um fator de trabalho.
10. Aleatoriedade Criptográfica: Garanta que a aleatoriedade criptográfica seja usada quando apropriado e não seja previsível.

Referência:
https://blog.grancursosonline.com.br/owasp-top-10-de-2021-parte-02/

https://owasp.org/Top10/A02_2021-Cryptographic_Failures/