NIST Cybersecurity Framework - Projeto Fidelize

1. Introdução

O NIST Cybersecurity Framework (CSF) é uma referência internacional para gerenciamento de riscos de segurança cibernética, estruturado em cinco funções principais: Identificar (ID), Proteger (PR), Detectar (DE), Responder (RS) e Recuperar (RC).

Este documento aplica o NIST CSF ao projeto Fidelize, cujo objetivo é desenvolver um dashboard interativo para análise de campanhas de marketing, perfil de clientes e pedidos em uma rede de estabelecimentos. O foco está em proteger os usuários, clientes, o dashboard e o site, garantindo confidencialidade, integridade e disponibilidade.

2. Funções do NIST aplicadas ao Projeto

2.1 Identificar (ID)

1. ID.AM (Gestão de ativos): Mapeamento de ativos como o dashboard, site, servidores, APIs integradas, banco de dados PostgreSQL e Firebase, além dos dados de clientes (nome, sexo, status, etc).

2. ID.BE (Ambiente de negócios): O projeto tem como missão apoiar decisões estratégicas por meio de um dashboard seguro e confiável, onde a cibersegurança serve à credibilidade dos indicadores gerados.

3. ID.GV (Governança): Definição clara de papéis de segurança cibernética levando em consideração a proteção de dados, infraestrutura, plataforma e decisão estratégica.

4. ID.RA (Avaliação de risco): Avaliação de riscos com base em ameaças (ataques externos, falhas humanas), vulnerabilidades (código inseguro, credenciais fracas) e controles já existentes (anonimização dos dados).

5. ID.RM (Estratégia de gestão de risco): Estratégias em reduzir riscos de privacidade, reputação e disponibilidade, alinhando-se às metas do projeto.

2.2 Proteger (PR)

1. PR.AC (Controle de acesso): Implementação de autenticação para o dashboard, segregação de funções entre perfis de usuários e registro de auditoria (createdBy/updatedBy).

2. PR.AT (Conscientização e treinamento): Treinamento da equipe de desenvolvimento, design e suporte em práticas de segurança, incluindo codificação

segura e privacidade de dados.

3. PR.DS (Segurança de dados): Proteção de dados com anonimização, criptografia em repouso e em trânsito, backups regulares e verificações de integridade.

4. PR.IP (Processos e procedimentos de proteção de informações): Aplicação de políticas de segurança no ciclo de vida do software, incluindo testes de vulnerabilidade e revisões de código.

5. PR.MA (Manutenção): Atualizações recorrentes do dashboard e dos dados utilizados, aplicação de patches e correções contínuas.

6. PR.PT (Tecnologia de proteção): Configuração de firewalls, monitoramento de rede e uso de ferramentas para garantir segurança técnica.

2.3 Detectar (DE)

1. DE.CM (Monitoramento contínuo de segurança): Monitoramento contínuo do dashboard e site por meio de alertas de comportamento e análise de acessos.

2. DE.DP (Processos de detecção): Procedimentos para tratar de eventos suspeitos, escalonando para a equipe de segurança.

3. DE.AE (Anomalias e eventos): Definição de critérios para identificar incidentes, como tentativas de login indevido, acessos não autorizados ou falhas de integridade nos dados.

2.4 Responder (RS)

1. RS.RP (Planejamento de resposta): Elaboração de plano de resposta a incidentes, incluindo etapas de contenção, erradicação e recuperação.

2. RS.CO (Comunicação): Protocolos para comunicação com stakeholders (gerência, suporte, clientes) em caso de incidente.

3. RS.AN (Análise): Investigações pós-incidente para identificar causa, impactos e medidas preventivas.

4. RS.MI (Mitigação): Ações de mitigação, como isolamento de sistemas comprometidos, aplicação de backups ou remoção de códigos.

5. RS.IM (Melhorias): Atualização contínua dos planos e controles de segurança com base em lições aprendidas.

2.5 Recuperar (RC)

1. RC.RP (Planejamento de recuperação): Desenvolvimento e testes de planos de recuperação (backup e testes de backup) de desastres e continuidade de negócios

para o dashboard e site, com definição de RTO (Recovery Time Objective) e RPO (Recovery Point Objective).

2. RC.IM (Melhorias): Revisão periódica das estratégias de recuperação e testes de resiliência.

3. RC.CO (Comunicação): Comunicação clara com usuários e stakeholders sobre progresso de recuperação e status dos serviços.

3. Considerações Específicas do Projeto

1. ID.RA: A anonimização dos dados é uma contramedida eficaz, reduzindo riscos legais e de privacidade.

2. PR.DS: A proteção dos dados sensíveis (clientes e campanhas) deve usar criptografia ponta a ponta.

3. DE.CM: O monitoramento deve incluir tanto métricas de uso do dashboard quanto de segurança.

4. RS.CO: A comunicação em caso de incidentes deve ser rápida, clara e direcionada às partes corretas.

5. RC.RP: O plano de recuperação deve priorizar disponibilidade contínua, já que o dashboard apoia decisões estratégicas.

4. Conclusão

A aplicação do NIST CSF ao projeto Fidelize fornece uma estrutura robusta para reduzir riscos cibernéticos e garantir uma maior resiliência ao dashboard e ao site.

Cada função - Identificar (ID), Proteger (PR), Detectar (DE), Responder (RS) e Recuperar (RC) - foi mapeada de acordo com práticas e medidas específicas:

1. ID.AM, ID.RA: reconhecimento de ativos e avaliação de riscos.

2. PR.AC, PR.DS: proteção de acessos e dados sensíveis.

3. DE.CM, DE.AE: monitoramento contínuo e detecção de eventos.

4. RS.RP, RS.IM: resposta estruturada a incidentes.

5. RC.RP, RC.CO: recuperação rápida e comunicação transparente.