**Universidade Positivo – UP**

**Curso de Ciências da Computação**

**Relatório de Segurança em Camadas**

**Relatório:** Segurança em Camadas para a fábrica Fashion!.

Curitiba – PR

2023

**FELIPE FRANCO PINHEIRO**

**GABRIEL CONSULO**

**GABRIEL MARTINS DELFES**

**GAEL HUK KUKLA**

**THIAGO BITTENCOURT SANTANA**

**YANN LUCAS SAITO DA LUZ**

**Relatório:** Segurança em Camadas para a fábrica Fashion!.

Relatório escrito como requisito para conclusão da atividade para composição de nota Bimestral da disciplina Criptografia e Segurança de Sistemas Computacionais da Universitário Positivo – UP. Professor (a): Leandro Fabian Almeida Escobar.

Curitiba – PR

2023

**SUMÁRIO**

[**1. INTRODUÇÃO 4**](#_nlqx8qnfem43)

[**2. FÍSICA 5**](#_885umgj65c7w)

[**3. ACESSO AO SISTEMA 6**](#_wgsv1m781bfe)

[**4. SISTEMA E REDE 7**](#_pvufitagp7yh)

[**5. MANUTENÇÃO 8**](#_xydkl02y4qfi)

[**6. EXTRA 9**](#_hwa39t5e8ah0)

[**7. CONCLUSÃO 10**](#_smzeooq96pez)

[**8. REFERÊNCIAS 11**](#_a7vbd74ps7pn)

### **1. INTRODUÇÃO**

A segurança da informação é um aspecto fundamental em qualquer sistema de computação, especialmente em ambientes que lidam com dados sensíveis ou críticos. Este relatório aborda as diversas camadas de segurança implementadas em um projeto de servidor, visando proteger a integridade, confidencialidade e disponibilidade dos dados.

## **2. FÍSICA**

Para uma boa segurança física dos servidores, estes estarão hospedados em nuvem.

A camada física constitui a base da segurança de um sistema, garantindo a proteção contra falhas de hardware e a disponibilidade dos dados. Nesse contexto, os backups desempenham um papel crucial, permitindo a recuperação de dados em caso de falhas físicas. São realizadas cópias de segurança regularmente atualizadas, conforme preconizado pelas boas práticas de segurança.

## **3. ACESSO AO SISTEMA**

A autenticação multifator é uma estratégia eficaz para reforçar o controle de acesso ao sistema, exigindo a verificação de múltiplos elementos de identidade. Além disso, é implementada uma política de senha sofisticada, com requisitos de complexidade e rotação regular, a cada duas semanas, para todos os usuários do sistema e administradores.

## **4. SISTEMA E REDE**

Nesta camada, várias medidas são adotadas para proteger a integridade e confidencialidade dos dados. Isso inclui a implementação de firewalls para controlar o tráfego de rede, a utilização de software antivírus e antimalware para identificar e remover ameaças, a criptografia de dados durante o armazenamento e a transmissão, bem como a filtragem de e-mails para evitar ameaças de phishing e malware. Além disso, são empregadas ferramentas de detecção de tentativas de invasão para monitorar e responder a possíveis ataques. O cuidado com a segurança do banco de dados é de extrema importância para um projeto seguro, onde passos como: Limitar o acesso à base de dados, Identificar os dados sensíveis e os dados críticos, Criptografar a informação, Não utilizar a mesma base de dados para testes em aplicações e Registrar a atividade da base de dados; são passos fundamentais para a segurança dos dados.

## **5. MANUTENÇÃO**

A manutenção adequada do sistema é essencial para garantir sua segurança contínua. Nesse sentido, são realizadas atualizações e patches constantes para corrigir vulnerabilidades de segurança e manter o software atualizado com as últimas tecnologias. Essas medidas são implementadas em resposta à verificação de erros e atualizações de tecnologia.

## **6. EXTRA**

Além das camadas tradicionais de segurança, medidas adicionais são adotadas para mitigar ameaças específicas. Isso inclui a verificação na Dark Web, a fim de monitorar atividades suspeitas e identificar possíveis vazamentos de informações sensíveis. Além disso, é fornecido treinamento contínuo à equipe, visando promover a conscientização sobre práticas de segurança e prevenir incidentes de segurança causados por falhas humanas.

## **7. CONCLUSÃO**

A implementação de múltiplas camadas de segurança em um projeto de servidor é essencial para proteger os dados contra uma variedade de ameaças. Ao adotar uma abordagem holística que abrange aspectos físicos, de acesso, sistema/rede, manutenção e medidas extras, é possível criar um ambiente seguro e resiliente que atenda aos requisitos de segurança da informação.

## **8. REFERÊNCIAS**

WHITMAN, M.E., & MATTORD, H. J. (2011). PRINCIPLES OF INFORMATION SECURITY.

PFLEEGER, C. P., & PFLEEGER, S. L. (2015). SECURITY IN COMPUTING.

STALLINGS, W., & BROWN, L. (2017). COMPUTER SECURITY: PRINCIPLES AND PRACTICE.

STALLINGS, W. (2019). NETWORK SECURITY ESSENTIALS: APPLICATIONS AND STANDARDS.

CHAPPLE, M., STEWART, J. M., & GIBSON, D. (2018). CISSP (ISC)2 CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL OFFICIAL STUDY GUIDE.