

# WATCHDOG

## **Integrantes:**

Demétrio Henrique Souza Cleto

Lucca Gomes Vieira

Luigi Augusto Bezerra Consentino

Mateus Macedo Batista de Souza

Mateus Sousa Piccinin

Matheus Andrade Mauro

Nathan Camargo de Oliveira Silva

Thiago Henrique Martinho da Silva

## **Uso de Inteligência Artificial no Projeto WatchDog**

### **1. Descrição Geral do WatchDog**

O Watchdog é uma solução inovadora de segurança digital projetada para proteger o que realmente importa: os dados e a privacidade dos usuários. Com foco em simplicidade e eficácia, o Watchdog oferece um serviço de configuração de segurança para celulares, que personaliza as configurações do dispositivo, tornando-o mais resistente a acessos indevidos em caso de roubo ou perda. Inclui também um eBook com dicas práticas para que o usuário mantenha seus dados seguros no dia a dia. Para proteção de arquivos no computador, o Watchdog conta com um app de criptografia que guia o usuário no processo de codificação dos arquivos, permitindo que eles sejam acessados apenas com um pen drive exclusivo. Essa abordagem completa torna o Watchdog uma solução única, acessível e prática, garantindo a tranquilidade e segurança digital dos usuários.

### **2. Detalhamento das Funcionalidades de Segurança Móvel**

O WatchDog foca em oferecer orientações e serviços de segurança digital especialmente para usuários com menos conhecimento sobre práticas de segurança básicas, promovendo

uma configuração robusta de seus dispositivos móveis. Entre as principais funcionalidades oferecidas, destacam-se:

- **Ativação de Autenticação de Dois Fatores (2FA):** A autenticação de dois fatores (2FA) é um recurso essencial para proteger contas, pois adiciona uma camada extra de segurança além da senha. Para tornar esse recurso acessível ao usuário, o WatchDog identifica e orienta a ativação do 2FA em aplicativos e serviços compatíveis instalados no dispositivo, como e-mail, redes sociais e bancos. A ativação do 2FA permite que o usuário seja alertado e precise aprovar tentativas de login, protegendo suas contas contra acessos indevidos.
- **Verificação e Fortalecimento de Senhas:** O WatchDog verifica se as senhas usadas pelo usuário são consideradas seguras e oferece sugestões de aprimoramento. Ele incentiva o uso de gerenciadores de senhas, que permitem a criação de senhas fortes e únicas para cada conta, e ajuda o usuário a evitar práticas comuns de senhas inseguras, como repetir a mesma senha em várias contas ou usar sequências fáceis de adivinhar. A interface intuitiva orienta o usuário em cada etapa, assegurando que até mesmo aqueles que desconhecem essas práticas possam configurá-las facilmente.

### 3. Arquitetura do Sistema

O uso de Machine Learning (ML) para decidir a intensidade da criptografia com base na frequência de acesso ao arquivo é uma abordagem inteligente e inovadora.

- **Análise de Frequência e Tipo de Arquivo:** O sistema utiliza ML para avaliar se o arquivo é acessado com frequência, o que pode justificar uma criptografia mais leve e rápida, ou se é um arquivo sensível que exige maior proteção, aplicando então uma criptografia mais robusta.
- **Customização da Criptografia:** O modelo de ML poderia considerar variáveis como o tamanho do arquivo, tipo de dado, frequência de acesso e o nível de sensibilidade, para recomendar o tipo de criptografia mais adequada. Isso personaliza a segurança sem sacrificar a usabilidade do sistema.

### 4. Explicação dos Algoritmos de Criptografia Utilizados

O WatchDog utiliza algoritmos de criptografia com diferentes níveis de segurança e desempenho, de acordo com as necessidades específicas de cada arquivo. Isso permite que o sistema ofereça um equilíbrio entre segurança e velocidade de acesso, conforme descrito a seguir:

- **Algoritmo Rápido e Leve (AES-128):** Para arquivos que precisam ser acessados frequentemente e em alta velocidade, o WatchDog utiliza o algoritmo **AES-128 (Advanced Encryption Standard)**. Esse algoritmo oferece um bom nível de segurança com tempos de processamento mais rápidos, sendo ideal para arquivos de uso diário. O AES-128 garante uma criptografia ágil e eficiente, com uma chave de

128 bits que dificulta o acesso não autorizado, sem comprometer o desempenho do sistema.

- **Algoritmo Robusto e Mais Lento (RSA-2048):** Para arquivos mais sensíveis que são acessados com menos frequência, o WatchDog recomenda o uso do **RSA-2048**, um algoritmo mais seguro, porém com maior demanda de processamento. Com uma chave de 2048 bits, o RSA oferece um alto nível de segurança e é ideal para documentos que exigem máxima proteção contra violações. Embora o tempo de criptografia e descriptografia seja mais longo, o RSA é altamente resistente a tentativas de quebra de criptografia, proporcionando segurança para dados confidenciais que não precisam ser acessados constantemente.

## 5. Infraestrutura e Tratamento de Dados

Para garantir a segurança e a privacidade dos usuários:

- **Processamento Local e Efêmero de Dados:** As configurações do dispositivo e as informações de análise de segurança devem ser processadas localmente, evitando o armazenamento excessivo de dados sensíveis. Isso mantém a privacidade do usuário e reduz os riscos associados ao armazenamento de dados pessoais.
- **Chave Pública no Pen Drive:** Esse componente físico para armazenar a chave pública torna o projeto mais seguro e agrega uma camada de proteção física para o sistema de criptografia.

## 6. Segurança Física da Chave no Pen Drive e Backup na Nuvem

O modelo de criptografia do WatchDog utiliza um pen drive como chave física para descriptografar arquivos, proporcionando uma camada de segurança extra. No entanto, para evitar a perda de dados caso o pen drive seja extraviado ou danificado, o WatchDog oferece uma opção de backup seguro na nuvem, mediante o consentimento do usuário.

- **Backup Opcional na Nuvem:** Para usuários que preferem um nível extra de segurança contra perda de dados, o WatchDog disponibiliza um serviço de backup na nuvem. Este backup permite que o usuário recupere seus arquivos mesmo em caso de perda ou dano do pen drive. Contudo, informamos que, embora seguro, esse backup reduz a segurança física dos arquivos, pois passa a envolver um domínio externo. O WatchDog utiliza uma criptografia forte para esses backups e armazena os arquivos de forma segura, mas sempre comunicamos aos usuários que o armazenamento em nuvem envolve alguns riscos adicionais em comparação ao pen drive físico.

## 7. Considerações Éticas e Limitações

A inclusão de Machine Learning e criptografia física levanta algumas questões éticas e técnicas, como:

- **Proteção Contra Falsos Positivos e Negativos no Modelo de ML:** O modelo deve ser ajustado para minimizar erros na escolha do tipo de criptografia, uma vez que uma criptografia inadequada pode comprometer a segurança ou a usabilidade dos arquivos.
- **Impacto da Criptografia nos Recursos Computacionais:** Criptografias mais robustas podem exigir mais processamento. Considerar o desempenho dos dispositivos em que o software será executado ajuda a evitar problemas de usabilidade.

## 8. Conclusão e Perspectivas Futuras

O projeto apresenta uma solução diferenciada, capaz de unir segurança física e digital para proteger dados e privacidade. Algumas perspectivas de desenvolvimento futuro incluem:

- **Expansão para Outros Dispositivos:** Além dos smartphones, o projeto poderia eventualmente incluir segurança para dispositivos conectados, ampliando a proteção para o ecossistema completo do usuário.