

TRABAJO FIN DE GRADO INGENIERÍA EN INGENIERÍA INFORMÁTICA

Título del proyecto

Subtítulo del proyecto

Autor

Pedro Luis Fuertes Moreno

Directores

Alberto Guillén Perales Gabriel Maciá Fernández



ESCUELA TÉCNICA SUPERIOR DE INGENIERÍAS INFORMÁTICA Y DE TELECOMUNICACIÓN

Granada, mes de 201

Título del proyecto: Subtítulo del proyecto

Pedro Luis Fuertes Moreno

Palabras clave: palabra_clave1, palabra_clave2, palabra_clave3,

Resumen

Poner aquí el resumen.

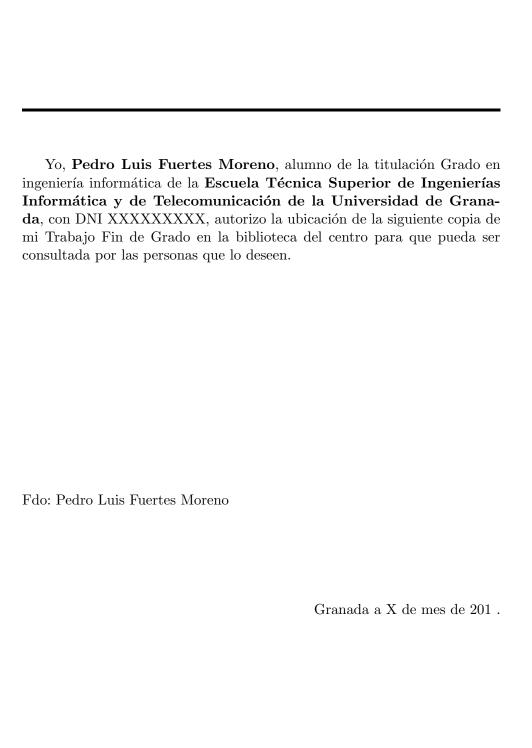
Título del proyecto: Subtítulo del proyecto

Pedro Luis Fuertes Moreno

Keywords: Keyword1, Keyword2, Keyword3,

Abstract

Write here the abstract in English.



- D. Alberto Guillén Perales, Profesor del Área de XXXX del Departamento Departamento de ... de la Universidad de Granada.
- D. Gabriel Maciá Fernández, Profesor del Área de XXXX del Departamento Departamento de ... de la Universidad de Granada.

Informan:

Que el presente trabajo, titulado *Título del proyecto*, *Subtítulo del proyecto*, ha sido realizado bajo su supervisión por **Pedro Luis Fuertes Moreno**, y autorizamos la defensa de dicho trabajo ante el tribunal que corresponda.

Y para que conste, expiden y firman el presente informe en Granada a X de mes de 201 .

Los directores:

Alberto Guillén Perales Gabriel Maciá Fernández

Agradecimientos

Poner aquí agradecimientos...

Índice general

Ín	dice general	15
1.	Introducción 1.1. Tipos de amenazas mediante correo electrónico	17 17 17
2.	Motivación	19
3.	Objetivos	21
	Elección del lenguaje de programación para la extracción de datos 4.1. Perl 4.2. C++ 4.3. Java 4.4. Pyhton Elección de la base de datos en la que almacenar los datos 5.1. NO-SQL 5.2. SQL 5.2.1. MariaBD 5.2.2. PostgreSQL	23 23 23 23 23 25 25 25 25
6.	Visualización de los datos	27
7.	Adecuación a la ley de protección de datos	29
8.	Conclusiones y vías futuras	31
Ri	hliografía	33

Introducción

El correo electrónico, desde que se creó, ha sido una fuente incesante de amenazas a los usuarios y, sin embargo, es el estándar de facto de la comunicación entre usuarios y empresas. Esto es debido a que cuando se crearon las primeras versiones de los protocolos SMPT y POP, en 1982 [1] y 1984 [2] respectivamente, que se usan ampliamente en el envío y recepción de correos electrónicos, en internet apenas había una decena de miles de nodos conectados y la mayoría eran universidades y centros de investigación, por lo que la seguridad en aquel entonces no era un problema como lo es actualmente. Esa falta de seguridad en los primeros protocolos deriva en que en la actualidad el correo electrónico sea uno de los mayores agujeros de seguridad de las empresas y usuarios. Sumada a esta debilidad de la seguridad está la complejidad de los ataques, que son cada vez más complicados de detectar tanto por herramientas automatizadas como por los propios usuarios.

1.1. Tipos de amenazas mediante correo electrónico

1.1.1. SPAM

Motivación

Objetivos

Elección del lenguaje de programación para la extracción de datos

- 4.1. Perl
- 4.2. C++
- 4.3. Java
- 4.4. Pyhton

Elección de la base de datos en la que almacenar los datos

- 5.1. **NO-SQL**
- 5.2. SQL
- 5.2.1. MariaBD
- 5.2.2. PostgreSQL

Visualización de los datos

Adecuación a la ley de protección de datos

Conclusiones y vías futuras

Bibliografía

- [1] J. B. Postel. Simple Mail Transfer Protocol. RFC 821, University of Southern California, agosto 1982. URL https://tools.ietf.org/html/rfc821.
- [2] J. K. Reynolds. Post Office Protocol. RFC 918, Network Working Group, octubre 1984. URL https://tools.ietf.org/html/rfc918.