

Sistema de Protección Parental: Angelus Custos

Alumno: Nicolás A. Ortega Froya

Tutor: Indalecio García Mateos

Centro: CEU San Pablo Andalucía

Ciclo: Administración de Sistemas Informáticos en Red

17 de abril de 2023



CEU

*Centro de Estudios
Profesionales*

Fundación San Pablo Andalucía

Índice

1. Introducción	2
2. Contexto	2
2.1. Situación Actual	2
2.2. Justificación	3
3. Planificación y Costes	4
3.1. Metodología	4
3.2. Fases del Proyecto	4
3.3. Planificación Temporal	4
3.4. Estimación de Costes	4
4. Desarrollo	4
4.1. Análisis de Requisitos	4
4.1.1. Requisitos Hardware	4
4.1.2. Requisitos Software	5
4.2. Diseño de Solución	6
5. Pruebas y Despliegue	6
5.1. Plan de Pruebas	6
5.2. Manuales Técnicos y de Usuario	6
5.3. Plan de Despliegue	6
6. Conclusiones y Propuestas de Mejora	6
7. Bibliografía	6
8. Derechos de Autor y Licencia	7

1. Introducción

Angelus Custos (i.e. Ángel de la Guarda) es un proyecto para facilitar a los padres la protección de la inocencia de sus hijos ante la degeneración de la pornografía. Se trata de una solución que cualquier persona con un mínimo de conocimiento técnico lo puede montar en su casa para proteger a sus hijos, y también compartir la misma tecnología con otros padres, en espíritu solidario cristiano, para que ellos también puedan proteger a los suyos.

También optaremos, en este mismo espíritu colaborativo, por soluciones software que sean libres y gratuitos, ya que el objetivo es proveer una solución para personas particulares, y no un plan de negocio.

2. Contexto

2.1. Situación Actual

Vivimos en un mundo muy digitalizado donde los niños están expuestos a pornografía desde una edad muy temprana. Aunque hay muchos factores que contribuyen a esto, uno de ellos es la facilidad de acceso: que un niño puede encontrarse con contenido pornográfico en la web sin querer, haciendo una búsqueda completamente inocente o incluso por culpa de anuncios inapropiados. Aunque diferentes organismos han intentado mitigar esta posibilidad con soluciones como las *búsquedas seguras* en los buscadores, no ha sido suficiente.

A causa de esto se han creado muchas alternativas para bloquear pornografía en entornos familiares, educativos, religiosos, etc. Estas alternativas han llegado incluso a ser muy avanzadas, pudiendo reconocer contenido pornográfico con reconocimiento de imágenes, y enviando reportes a los responsables, que pueden ser los padres o, en casos de adultos que quieren ayuda para librarse de su adicción a la pornografía, un amigo o familiar que se responsabiliza. Muchos de éstos han conseguido convertirlo en un negocio para poder así hacer este tipo de mejoras y desarrollos a sus productos.

Aunque existen todas estas soluciones, parece que hay pocos que se interesan por el daño que provoca la pornografía en nuestra salud mental, particularmente en la salud de los menores de edad. Una parte puede ser la falta de información: es un asunto que se habla poco debido a su naturaleza clandestina y pervertida.

Otra barrera que puede aparecer es también que estos productos/servicios suelen funcionar en base a una suscripción mensual. Si fuera un producto que se compra una sola vez entonces quizá habría más padres dispuestos a instalarlo en sus casas para proteger a sus hijos. Pero al ser una suscripción, pone una barrera innecesaria a la hora de facilitar a los padres este servicio tan necesario en el mundo de hoy.

2.2. Justificación

Como explicamos anteriormente, es necesario una solución para protegernos – a nuestros hijos, pero también a nosotros mismos – de la presencia y facilidad de acceso a la pornografía en *internet*. Pero la mayoría de las soluciones son comerciales y en base a una suscripción, que constituye una barrera para muchos padres aunque sea tan sólo una inconveniencia. Por este motivo el objetivo de este documento es explicar cómo montar y configurar un ordenador cualquiera para servir de monitor y bloquear las páginas pornográficas, además de añadir otras funcionalidades para mejor administrarlo. De este modo, siguiendo la filosofía de compartir del *movimiento software libre*, se puede conseguir facilitar a muchos el acceso a esta clase de soluciones o directamente en el caso de las personas que tengan algún conocimiento técnico, o de manera indirecta con el caso de alguien que se lo monta para sus familiares, amigos, y vecinos, o incluso si una empresa lo quiere comercializar de una forma que no ponga sobre los clientes un peso innecesario de suscripciones para poder protegerse a ellos mismos y a sus familias.

3. Planificación y Costes

3.1. Metodología

3.2. Fases del Proyecto

3.3. Planificación Temporal

3.4. Estimación de Costes

4. Desarrollo

4.1. Análisis de Requisitos

Podemos dividir los requisitos de nuestro proyecto en dos categorías principales: *hardware* y *software*.

4.1.1. Requisitos Hardware

En cuestión de requisitos *hardware*, será necesario un ordenador tan sólo lo suficientemente potente como para responder a peticiones DNS en una red local, responder a una petición a una página pornográfica con una página personalizada del usuario, y enviar correos electrónicos para avisar al responsable del dispositivo y de la red. Luego entonces, para una red normal, un requisito mínimo para el dispositivo podría ser como a continuación:

- Ancho de banda de red:
- Rendimiento de la CPU:
- Memoria:
- Almacenamiento:

Los requisitos son muy básicos, y casi cualquier ordenador (incluso uno antiguo que ya no se usa) serviría para la implementación de esta solución. En

caso de que no haya un ordenador libre a su disposición, convendría más comprar un ordenador *monoplaca*, como sería un *Raspberry Pi*, *Rock64*, o *Pine64*. Lo importante para nuestros propósitos es que sea posible instalar en él un sistema operativo basado en UNIX tal como sería una de las distribuciones de BSD o Linux.

4.1.2. Requisitos Software

Luego, en cuestión de requisitos *software* haría falta, en primer lugar, un sistema operativo tipo UNIX que soporte a todo el *software* que mencionaremos después. Aunque hay muchas opciones que podrían servir, para este caso se utilizará Debian GNU/Linux, versión Bullseye (11), el actual estable en la fecha de publicación de este documento. Esta distribución de Linux se escoge por ser una distribución muy utilizada en el ámbito de servidores, con mucho soporte y comunidad, que utiliza pocos recursos – se puede instalar fácilmente sin entorno gráfico –, y es conocida por su estabilidad. Se puede seguir utilizando este guía para montar la solución con cualquier otra distribución de Linux (o incluso de BSD), pero habría que modificar ciertas instrucciones para ajustarse a los estándares y herramientas disponibles en cada distribución (e.g. si quisiera instalarlo en un servidor de Fedora, utilizaría el comando `dnf` en vez de `apt`).

En cuanto a los programas que se precisan, haría falta un programa para gestionar las peticiones DNS y redirigirlas, otro para recibir las peticiones y responder con una página de aviso, además de disparar un mecanismo para avisar al administrador de la red acerca del intento de acceso.

Para la gestión de peticiones DNS existen muchos programas alternativos a nuestra disposición, como podrían ser PowerDNS, MaraDNS, NSD, KnotDNS, y Bind9.

Entre los programas de servidores HTTP existen dos candidatos principales: Nginx y Apache.

4.2. Diseño de Solución

5. Pruebas y Despliegue

5.1. Plan de Pruebas

5.2. Manuales Técnicos y de Usuario

5.3. Plan de Despliegue

6. Conclusiones y Propuestas de Mejora

7. Bibliografía

8. Derechos de Autor y Licencia

Copyright © 2023 Nicolás A. Ortega Froya <nicolas@ortegas.org>

Este documento se distribuye bajo los términos y condiciones de la licencia Creative Commons Attribution No Derivatives 4.0 International.