

# Internet segura para todos los usuarios

Dr. Gonzalo Álvarez Marañón

# Quién

- o Investigador en criptografía y criptoanálisis en el CSIC
- o Creador del **Criptonomicón**
- o Auditor de seguridad de aplicaciones web
- o Autor de los libros **Los mejores trucos para Internet** y **Seguridad informática para empresas y particulares**
- o [gonzaloalvarez.com](http://gonzaloalvarez.com)



---

# Qué

- I. Seguridad de la Información
- II. Amenazas en el entorno doméstico
- III. Medidas de seguridad
- IV. Conclusiones

---

# Definición

## SEGURO

- Libre y exento de todo peligro, daño o riesgo
- Cierto, indubitable y en cierta manera infalible
- No sospechoso

---

# Seguridad de la información

- o **Expectativas** de seguridad
- o **Contexto** de seguridad
- o Las **medidas** o **controles** de seguridad buscan satisfacer expectativas concretas en **contextos** determinados

---

# Enfoque tradicional

- ***“Queremos que no tenga éxito ningún ataque”***
- Seguridad = Invulnerabilidad
- **Imposible** de alcanzar

*La seguridad total no existe*

---

# Enfoque de gestión del riesgo

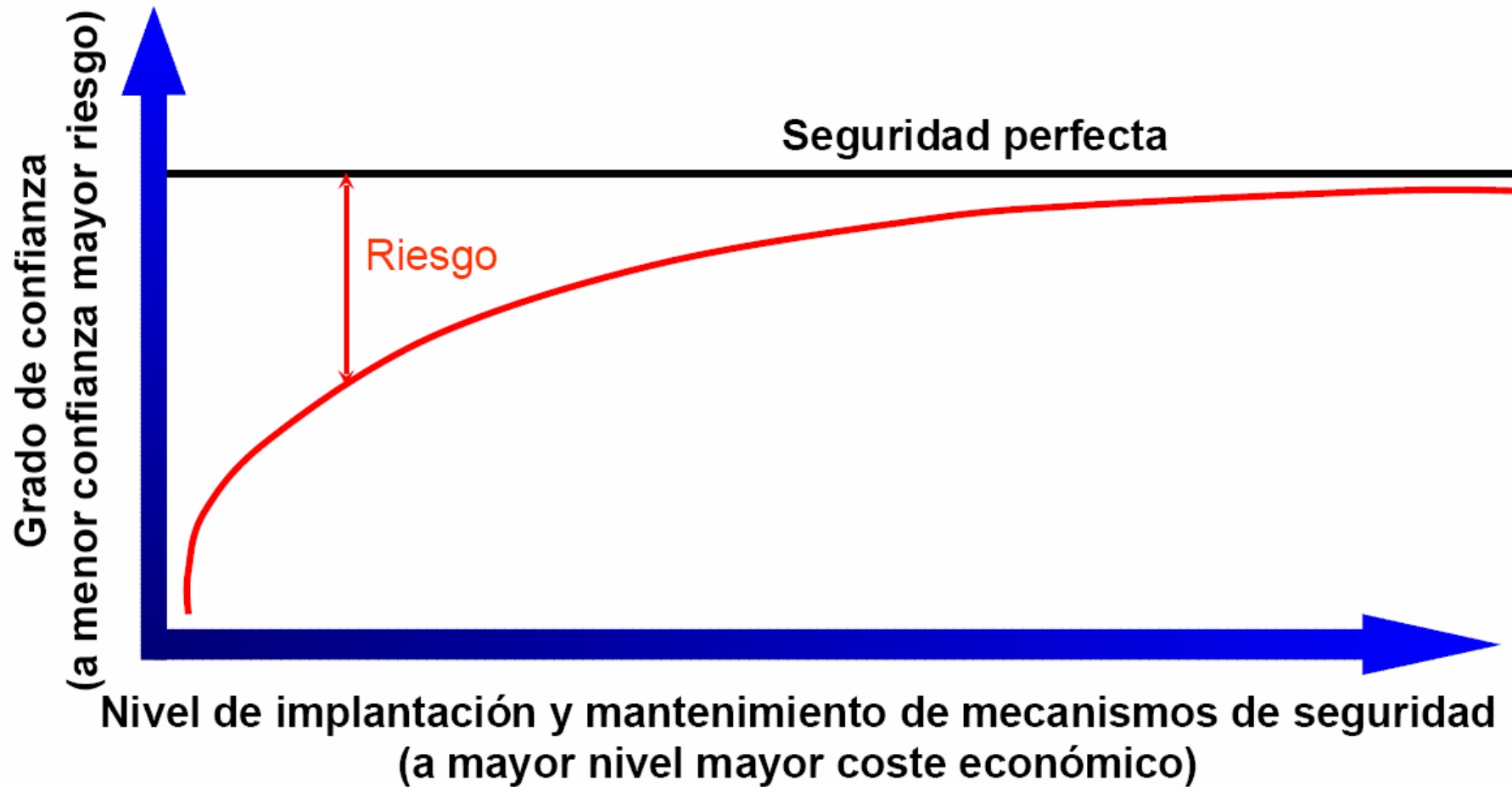
- ***“Queremos que nuestras expectativas se cumplan”***
- Seguridad = Confianza
- **Posible** de gestionar

*El riesgo no puede eliminarse completamente,  
pero puede reducirse*

# Análisis de riesgos

- Objetivo:
  - Identificar los riesgos
  - Cuantificar su impacto
  - Evaluar el coste para mitigarlos
  - Servir de guía para tomar decisiones
  
- **Riesgo = Activo x Amenaza x Vulnerabilidad**

# Riesgo y seguridad





“La seguridad no es un producto, es un proceso”

*Bruce Schneier*

---

# Seguridad en el hogar

## o Contexto

- ❑ Uno o dos ordenadores
- ❑ Adultos, jóvenes, niños
- ❑ Conocimiento de informática limitado
- ❑ Conexión a Internet por ADSL, Cable, módem
- ❑ Recursos limitados

## o Expectativas

---

# Amenazas

- Hackers
- Malware
- Fallos software y hardware: disponibilidad
- Timos, fraudes, robos
- Pérdida de privacidad
- Seguridad de menores

# Hackers

- ¿Qué tengo de valor para un hacker?
  - ▣ Espacio de disco
  - ▣ Ancho de banda
  
- ¿Cómo puede encontrarme?
  - ▣ Dirección IP

---

# Malware

- Virus
- Gusanos
- Troyanos
- Spyware
- Spam
- Dialers

# Virus

- Capacidad de replicación y destrucción
- Necesitan del usuario para propagarse
- Diversos métodos de infección: sector de arranque, archivos ejecutables, MBR, multipartitos, macro (Word, Excel, Access, Lotus)

---

# Gusanos

- Se autopropagan sin intervención humana
- Explotan vulnerabilidades en sistemas: Nimda, Blaster, etc.

---

# Troyanos

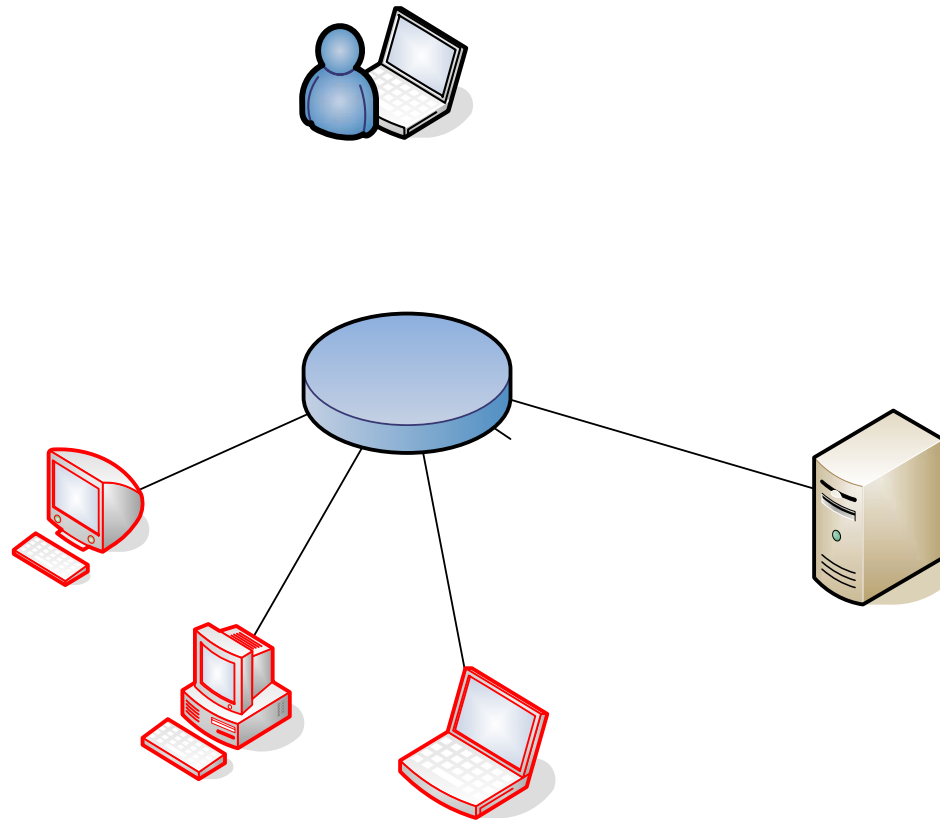
- Realizan tareas encubiertas
- Disfrazados de programas útiles
- Algunos permiten control remoto del equipo

# Zombies

- Equipos comprometidos al servicio de usuarios maliciosos, que utilizan las plataformas corruptas con el total desconocimiento de los propietarios y/o administradores
- Entre las tareas que realizan
  - Envío de **spam**
  - Servir **pornografía**
  - Servidores de fraude y **phishing**
  - Distribución de **malware**
- Las máquinas zombie se aglutinan en **botnets**

# Ataques al usuario: Funcionamiento de Botnets

- Spam
- DDoS
- Mass Scanning
- Phishing



---

# Spyware

- Software espía instalado sin el conocimiento del usuario
- Normalmente explotan vulnerabilidades en IE
- Presente en algún software gratuito (e incluso de pago)

# Spam

- Correo electrónico no deseado
- Vehículo de
  - Phishing
  - Virus
  - Timos
  - Bulos

---

# Dialers

- Conexión vía modem a números tarificación especial
- Sin consentimiento ni conocimiento de la víctima
- Generan gasto telefónico

# Picaresca (ingeniería social)

- Objetivo: entrar en redes u obtener secretos, engañando a la gente para que revelen contraseñas y otra información confidencial
- Apelan a las inclinaciones más profundas de la persona: el miedo, el deseo, la codicia o incluso la bondad
- Aplicaciones:
  - Timos
  - Phishing
  - Bulos

# Fallos software y hardware

- Tolerancia a fallos
  - ▣ Suministro eléctrico: SAI, regletas
  - ▣ Conectividad: líneas redundantes, Wifi con vecinos, 3G
  - ▣ Hardware: equipos de reserva
  
- Recuperación de sistemas
  - ▣ Copias de seguridad
  
- Plan de continuidad

# Privacidad

- Rastro del uso de Internet:
  - Dirección IP
  - Navegador
  - Sistema Operativo
  - Dirección de correo electrónico
  - Páginas visitadas, fotos vistas, documentos leídos, formularios rellenos, etc.
  - Cookies: hábitos de navegación, gustos, etc.

---

# Seguridad de menores

- Contenidos indebidos: sexo, violencia
- Revelación de información
- Juegos de azar
- Subastas
- Chat, mensajería, foros

# Medidas de seguridad

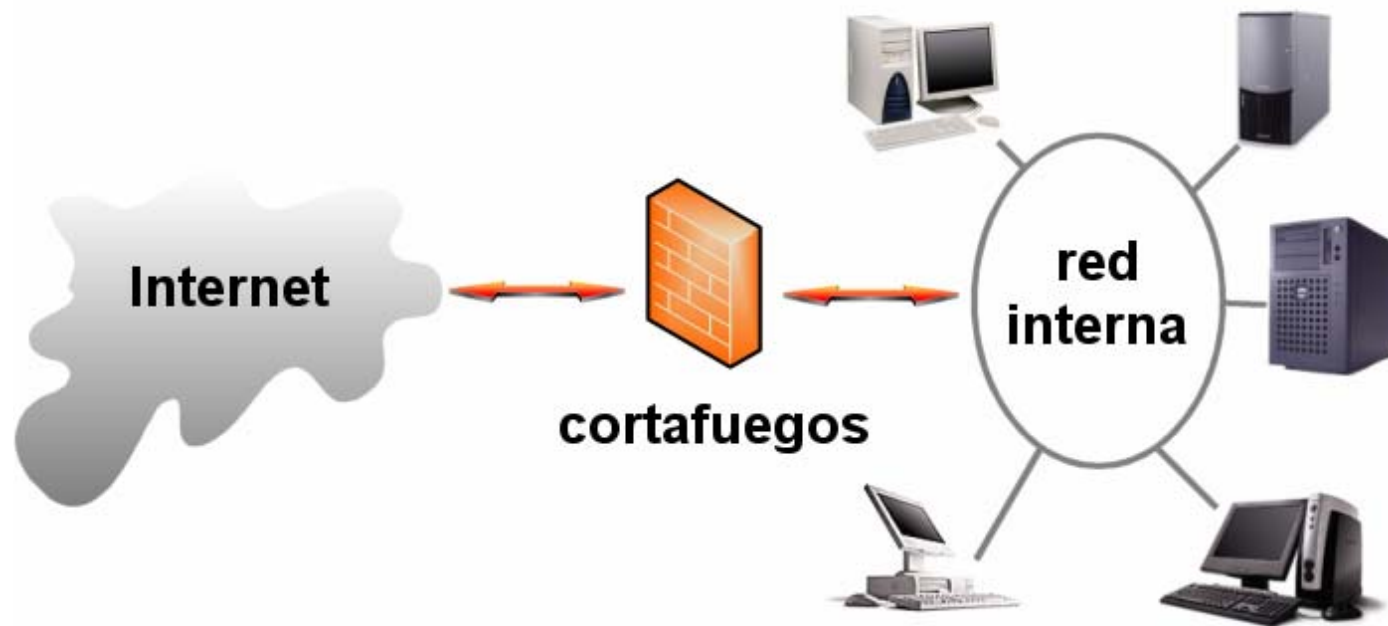
- Cortafuegos
- Antivirus
- Actualizaciones
- Listas de control de acceso
- Cifrado de los archivos del disco
- Copias de respaldo
- Anonimato
- Control de contenidos

---

# Cortafuegos

- o **Aislamiento** de Internet
  - Bloquea la entrada y salida
- o **Detección** de intrusos
  - Detecta aplicaciones que intentan acceder a Internet
- o **Auditoría** y registro de uso
  - Registra conexiones y ayuda a detectar intrusiones

# Cortafuegos



# Cortafuegos

- o ZoneAlarm:  
<http://download.zonelabs.com/bin/free/es/download/znalm.html>
- o Outpost: [www.outpost-es.com](http://www.outpost-es.com)
- o Comodo: [www.personalfirewall.comodo.com](http://www.personalfirewall.comodo.com)

# Antivirus

- Línea de defensa **fundamental**
- Si se produce un **positivo**:
  - Elimina el virus y restaura el archivo
  - Pone el archivo en cuarentena
  - Lo elimina por completo

# Antivirus

- AVG Free Edition: [www.grisoft.com/doc/products-avg-anti-virus-free-edition/Ing/la-es/tpl/tpl01](http://www.grisoft.com/doc/products-avg-anti-virus-free-edition/Ing/la-es/tpl/tpl01)
- BitDefender Free Edition v7: [www.bitdefender-es.com/PRODUCT-14-es--BitDefender-Free-Edition-v8.html](http://www.bitdefender-es.com/PRODUCT-14-es--BitDefender-Free-Edition-v8.html)
- AntiVir Personal Edition: [www.free-av.com](http://www.free-av.com)
- Free avast! 4 Home Edition: [www.asw.cz](http://www.asw.cz)

# Antispyware

- Windows Defender: [www.microsoft.com/spain/athome/security/spyware/software/default.mspix](http://www.microsoft.com/spain/athome/security/spyware/software/default.mspix)
- AdAware: [www.lavasoftusa.com/products/ad-aware\\_se\\_personal.php](http://www.lavasoftusa.com/products/ad-aware_se_personal.php)
- Spybot Search & Destroy (S&D): [www.safer-networking.org/es/home/index.html](http://www.safer-networking.org/es/home/index.html)

# Antispam

- o G-Lock SpamCombat: [www.glocksoft.com/sc](http://www.glocksoft.com/sc)
- o K9: [www.keir.net/k9.html](http://www.keir.net/k9.html)
- o Outlook Security Agent:  
[www.outlooksecurityagent.com](http://www.outlooksecurityagent.com)
- o SpamFighter: [www.spamfighter.com](http://www.spamfighter.com)
- o Spamihilator: [www.spamihilator.com](http://www.spamihilator.com)
- o SpamPal: [www.spampal.org](http://www.spampal.org)

---

# Actualizaciones

- o Mantener el sistema operativo siempre al día con las últimas actualizaciones
- o Descargas automáticas

---

# Listas de control de acceso

- Permiten especificar quién tiene acceso a qué archivos y con qué permisos
- Se basan en el uso de distintos usuarios
- **Principio del mínimo privilegio**

# Cifrado de los archivos del disco

- Permite cifrar el contenido de cualquier carpeta o archivo
- Solución altamente segura, integrada con el sistema de archivos, totalmente transparente para el usuario y con la capacidad de recuperar datos cifrados
- Se basa en el uso de criptografía de clave pública y de algoritmos de cifrado simétrico

# Copias de respaldo

- Formato de almacenamiento:
  - Disco duro externo
  - CD-RW/DVD-RW
  - Online:
    - [www.xdrive.com](http://www.xdrive.com)
    - [www.idrive.com](http://www.idrive.com)

# Anonimato

- CGI o anonimadores
  - @nonymouse: [anonymouse.ws](http://anonymouse.ws)
  - Megaproxy: [www.megaproxy.com](http://www.megaproxy.com)
  - The Cloak: [www.the-cloak.com](http://www.the-cloak.com)
- Proxies HTTP
  - HiProxy: [www.hiproxy.com](http://www.hiproxy.com)
  - Multiproxy: [www.multiproxy.org](http://www.multiproxy.org)
  - Privoxy: [www.privoxy.org](http://www.privoxy.org)
- SOCKS
  - SocksCap: [www.socks.permeo.com](http://www.socks.permeo.com)

# Control de contenidos

- Controlar por dónde navegan los suyos
  - Filtro de contenidos del navegador
  - Programas especializados:
    - Cyber Patrol: [www.cyberpatrol.com](http://www.cyberpatrol.com)
    - Cybersitter: [www.cybersitter.com](http://www.cybersitter.com)
    - Net Nanny: [www.netnanny.com](http://www.netnanny.com)
    - SurfControl: [www.surfcontrol.com](http://www.surfcontrol.com)

---

# Información

- o Seguridad en el hogar:  
[www.microsoft.com/spain/athome/security/default.mspx](http://www.microsoft.com/spain/athome/security/default.mspx)

---

# Conclusiones

- o **Amplio** abanico de herramientas de seguridad **gratuitas**
- o Un **pequeño** esfuerzo eleva drásticamente el nivel de seguridad
- o La **concienciación** es fundamental

---

# Kit de supervivencia

1. Cortafuegos
2. Antivirus
3. Actualizaciones
4. Concienciación