Objetivo de la Seguridad Informática

El objetivo de la seguridad informática es mantener la **Integridad**, **Disponibilidad**, **Privacidad**, Control y Autenticidad de la información manejada por computadora.

Elementos de la Seguridad Informática

- Integridad

  Los componentes del sistema permanecen inalterados a menos que sean modificados por los usuarios autorizados.

- Disponibilidad

  Los usuarios deben tener disponibles todos los componentes del sistema cuando así lo deseen.

- Privacidad

  Los componentes del sistema son accesibles sólo por los usuarios autorizados.

Elementos de la Seguridad Informática

- **Control**

  Solo los usuarios autorizados deciden cuando y como permitir el acceso a la información.

- **Autenticidad**

  Definir que la información requerida es válida y utilizable en tiempo, forma y distribución.

- **No Repudio**

  Evita que cualquier entidad que envió o recibió información alegue, que no lo hizo.

- **Auditoria**

  Determinar qué, cuándo, cómo y quién realiza acciones sobre el sistema.

Operatividad vs Seguridad

$$\text{OPERATIVIDAD} = \frac{1}{\text{SEGURIDAD}}$$

Seguridad Física

Aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información.

Seguridad Física

Amenazas

- Incendios
- Inundaciones
- Terremotos
- Trabajos no ergométricos
- Instalaciones eléctricas
  - Estática
  - Suministro ininterrumpido de corriente
  - Cableados defectuosos
- Seguridad del equipamiento

Seguridad Física

Controles

- Sistemas de alarma
- Control de personas
- Control de vehículos
- Barreras infrarrojas-ultrasónicas
- Control de hardware
- Controles biométricos
  - Huellas digitales
  - Control de voz
  - Patrones oculares
  - Verificación de firmas

Seguridad Lógica

Aplicación de barreras y procedimientos que resguarden el acceso a los datos y sólo se permita acceder a ellos a las personas autorizadas para hacerlo.

Seguridad Lógica

Identificación: El usuario se da a conocer al sistema.

Autentificación: Verificación del sistema ante la Identificación.

Formas de Autentificación-Verificación

”. Algo que la persona **conoce** - Password

. Algo que la persona **es** - Huella digital

⓪. Algo que la persona **hace** - Firmar

①. Algo que la persona **posee** - Token Card

Delito Informático

Cualquier comportamiento antijurídico, no ético o no autorizado, relacionado con el procesado automático de datos y/o transmisiones de datos.

Se realizan por medios informáticos y tienen como objeto a la **información** en sí misma.

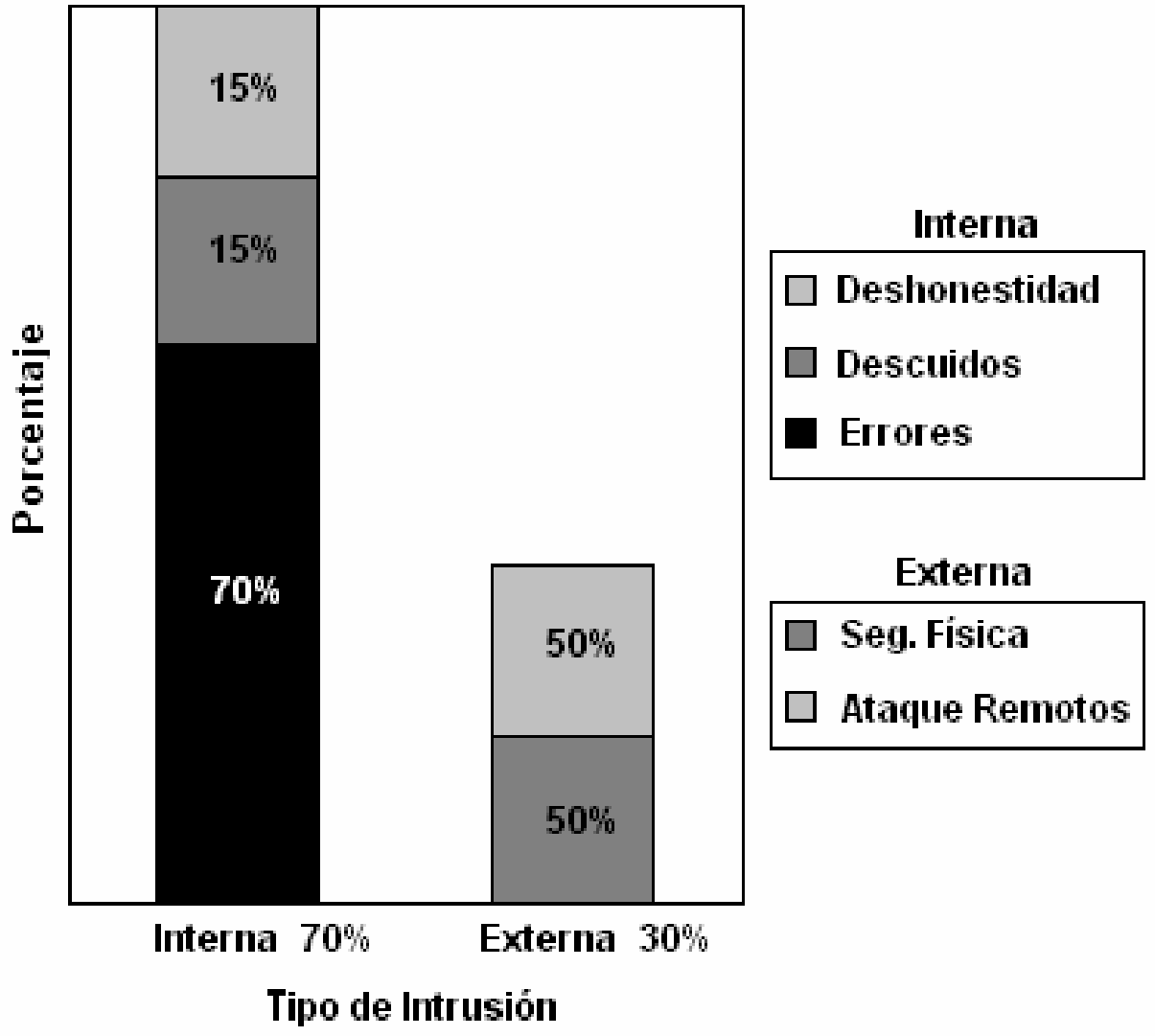
Delitos Informáticos

- Fraudes cometidos mediante manipulación de computadoras
- Daños a programas o datos almacenados
- Manipulación de datos de E/S
- Distribución de virus
- Espionaje
- Acceso no autorizado
- Reproducción y distribución de programas protegido por la ley

Amenazas Humanas

- **Hacker:** persona curiosa, inconformista y paciente que busca su superacion continua aprovechando las posibilidades que le brindan los sistemas.
- **Cracker:** hacker dañino.
- **Phreaker:** persona que engaña a las compañias telefónicas para su beneficio propio.
- **Pirata Informático:** persona que vende software protegido por las leyes de Copyright.
- **Creador de virus → Diseminadores de virus**
- **Insider:** personal interno de una organización que amenaza de cualquier forma al sistema de la misma.

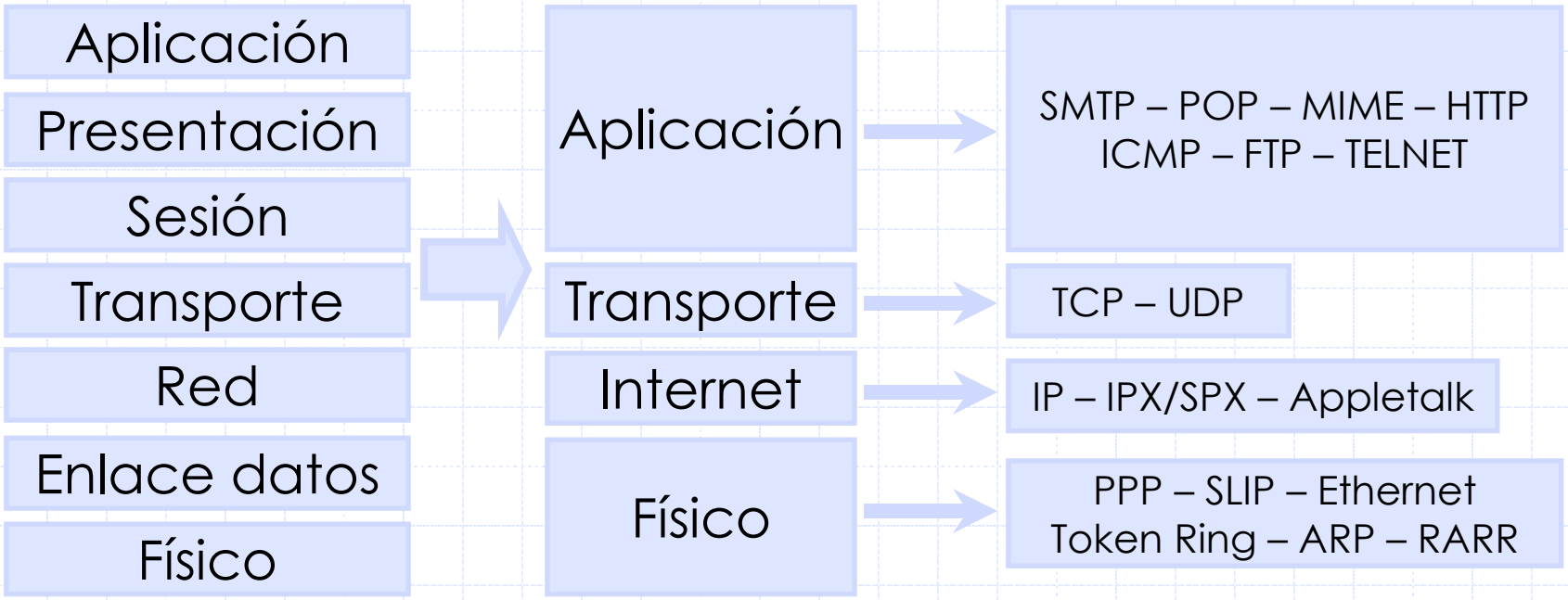
Intrusión – Amenazas



Comunicaciones

Protocolo: conjunto de normas que rige el intercambio de información entre dos computadoras.

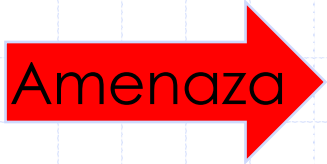
Modelo OSI → TCP/IP



Amenazas

Marco Legal acorde con los avances tecnólogicos

- Crackers
- Hackers
- Insiders
- Errores
- Virus
- Ingeniería Social



Bien Protegido

Marco Tecnológico – Comunicaciones – Internet

Amenaza: elemento que compromete al sistema

Tipos de Ataques

- Ingeniería Social – Social Inversa
- Trashing
- Vulnerabilidades propias de los sistemas

Monitorización

Observación

- Shoulder Surfing
- Decoy
- Scanning

Autentificación

Verificación Falsa

- Spoofing
- Looping
- Hijacking
- Backdoors
- Exploits
- Obtención de claves

Tipos de Ataques

Denial of Service

Saturación de Servicios

- Jamming Flooding
- SynFlood
- Connection Flood
- Land Attack
- Smurf Attack
- Nuke
- Tear Drop
- Bombing

Modificación

Daños

- Tampering
- Borrado de huellas
- Ataques con Scripts
- Ataques con ActiveX
- Ataque con JAVA
- Virus

Ataques

Implementación

”. Recopilación de información
. Exploración del sistema
⓪. Enumeración e identificación
①. Intrusión

Defensa

⊙ Mantener hardware actualizado
⊙ No permitir tráfico broadcast
⊙ Filtrar tráfico de red
⊙ Auditorías
⊙ Actualización de los sistemas
⊙ **Capacitación permanente**

Virus

Programa de actuar **subrepticio** para el usuario; cuyo código incluye información suficiente y necesaria para que, utilizando los mecanismos de ejecución que le ofrecen otros programas, puedan **reproducirse** y ser susceptibles de mutar; resultando de dicho proceso la modificación, alteración y/o **daño** de los programas, información y/o hardware afectados.

Modelo:

Dañino

Autoreproductor

Subrepticio

Daño Implícito

Daño Explícito

Tipos de Virus

Carácter Vandálico
↓
Amateur

- Sector de arranque
- Archivos ejecutables
- Residentes
- Macrovirus
- De email
- De sabotaje

Programas que no cumplen con la definición de virus

- Hoax
- Gusanos
- Caballos de troya
- Bombas lógicas

Carácter Dirigido
↓
Profesional y de espionaje

- Armas digitales

Antivirus

Gran base de datos con la "huella digital" de todos los virus conocidos para identificarlos y también con las pautas más comunes de los virus.

Detección
Confirmar la presencia de un virus
↓
Identificación
Determinar que virus fue detectado

Detección – Identificación

- Scanning
- Búsqueda heurística
- Monitor de actividad
- Chequeador de integridad

Modelo de Protección

- Política de seguridad de la organización
- Auditorías permanentes
- Plan de respuestas a incidentes
- Sistema de seguridad a nivel físico
- Seguridad a nivel Router–Firewall
- Sistemas de detección de intrusos (IDS)
- Penetration Testing

Modelo Descendente

Penetration Testing

Conjuntos de técnicas tendientes a realizar una evaluación integral de las debilidades de los sistema.

Externo

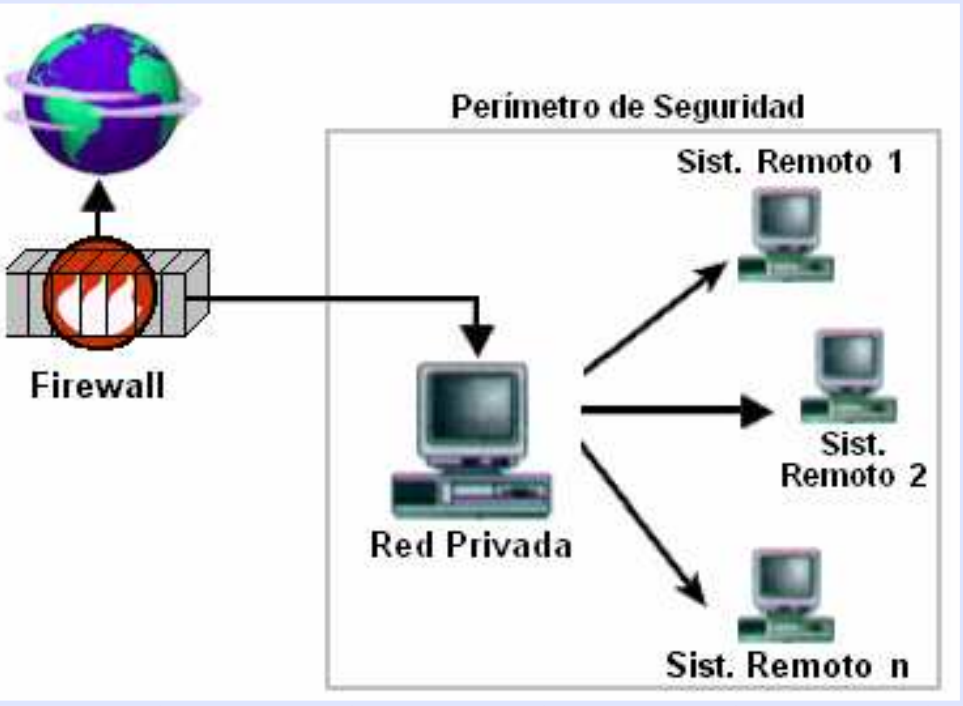
- Fuerzas de las passwords
- Captura de tráfico de red
- Detección de protocolos
- Scanning de puertos
- Vulnerabilidades existentes
- Ataques de DoS
- Test de servidores

Interno

- Protocolos internos
- Autentificación de usuarios
- Aplicaciones propietarias
- Verificación de permisos
- Ataques de DoS
- Seguridad física en las estaciones de trabajo

Firewalls

Sistema ubicado entre dos redes y que ejerce una política de seguridad establecida. Mecanismo encargado de proteger una red confiable de otra que no lo es.



Características

- Defensa perimetral.
- Defensa nula en el interior.
- Protección nula contra un intruso que lo traspasa.
- Sus reglas son definidas por humanos.

Tipos de Firewalls

”. Filtrado de paquetes

- Filtran Protocolos, IPs y puertos utilizados

. Gateway de Aplicaciones

- Se analizan cada uno de los paquetes que ingresa al sistema

⓪. Firewalls personales

- Aplicaciones disponibles para usuarios finales.

Tipos de Firewalls

”. Filtrado de paquetes

- ⊙ Filtra Protocolos, IPs y puertos utilizados
- ✓ Economicos y con alto desempeño
- ✘ No esconden la topología de la red

. Gateway de Aplicaciones

- ⊙ Nodo Bastion intermediario entre Cliente y Servidor
- ✓ Transparente al usuario
- ✘ Bajan rendimiento de la red

⓪. Dual Homed Host

- ⊙ Conectados al perímetro interior y exterior
- ✓ Paquetes IPs desactivado

Tipos de Firewalls

① . Screened Host

- ⊙ Router + Host Bastion.
- ✓ El Bastion es el único accesible desde el exterior.

② . Screened Subnet

- ⊙ Se aisla el Nodo Bastion (el más atacado).
- ⊙ Se utilizan dos o más routers para establecer la seguridad interna y externa.

③ . Inspección de paquetes

- ⊙ Cada paquete es inspeccionado.

④ . Firewalls personales

- ⊙ Aplicaciones disponibles para usuarios finales.

IDS

Sistema encargado de detectar intentos de intrusión en tiempo real.

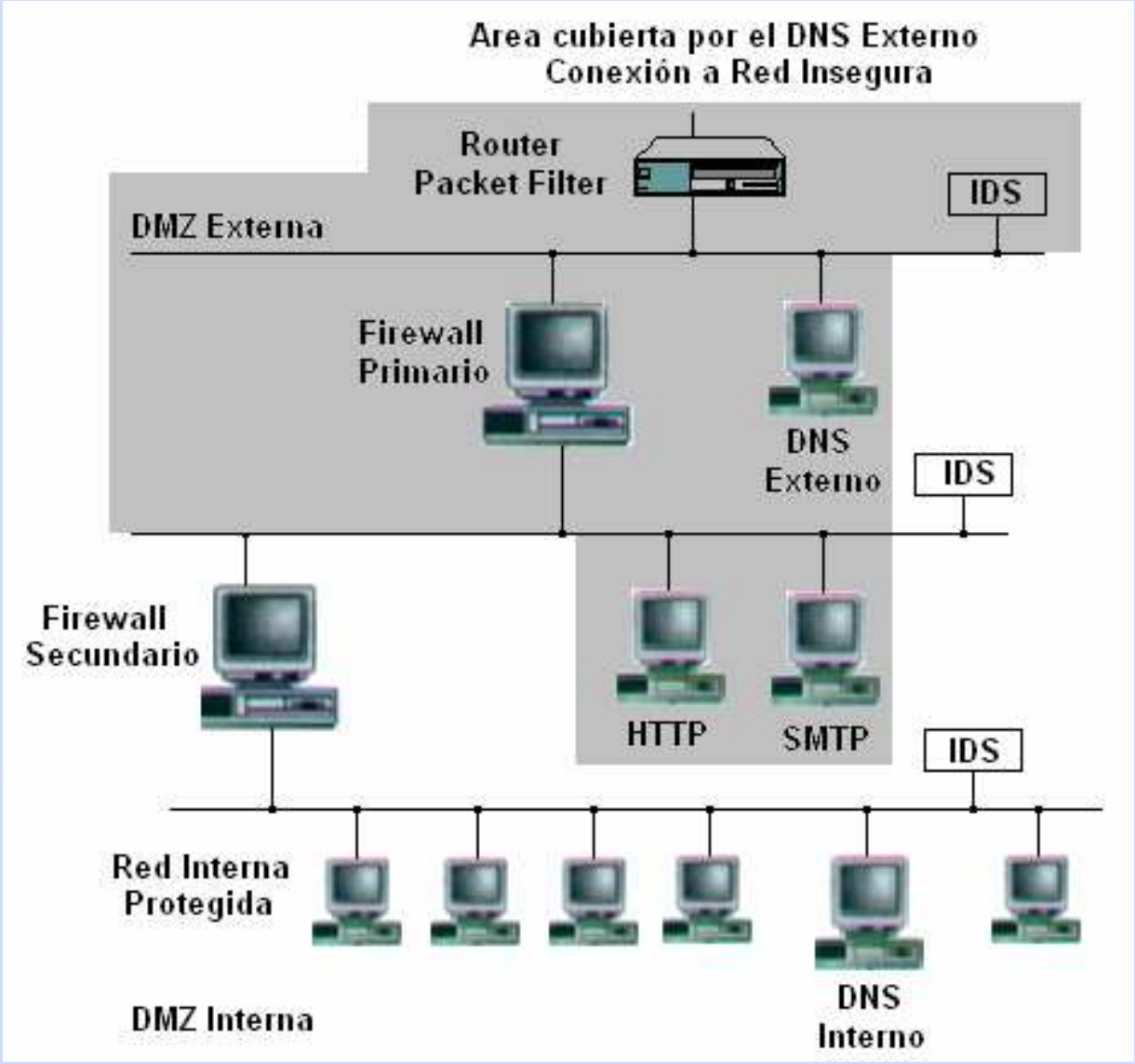
Ventajas

- Mantener un registro completo de actividades.
- Recoger evidencia.
- Descubre intrusiones automáticamente.
- Es disuador de "curiosos".
- Es Independiente del SO.
- Dificulta la eliminación de huellas.

Debilidades

- Tiene una alta tasa de falsas alarmas.
- Necesita reentrenamiento período.
- Puede sufir ataques durante la fase de aprendizaje y son considerados normales.
- No contempla la solución a nuevos agujeros de seguridad.

Firewall–IDS



Passwords

Cant. Caracteres	26 Min.	36 Min. + Dig.	52 May. + Min.	96 Todos
6	51 min.	6 horas	2,3 días	3 meses
7	22,3 horas	9 días	4 meses	24 años
8	24 días	10,5 meses	17 años	2.280 años
9	21 meses	32,6 años	890 años	219.601 años
10	45 años	1.160 años	45.840 años	21.081.705 años

Ataque a 13.794 cuentas con un diccionario de 62.727 palabras

- 1 Año → 3.340 claves (24,22%)
- 1° Semana → 3.000 claves (21,74%)
- 1° 15 Minutos → 368 claves (2,66%)

Ataque a 2.134 cuentas a 227.000 palabras/segundo

- Dicc. 2.030 → 36 cuentas en 19 segundos.
- Dicc. 250.000→ 64 cuentas en 36:18 minutos

Passwords

Normas de elección de passwords

- No utilizar contraseñas que sean palabras.
- No usar contraseñas con algún significado.
- Mezclar caracteres alfanuméricos.
- Longitud mínima de 7 caracteres.
- Contraseñas diferentes en sistemas diferentes.
- Ser fáciles de recordar → Uso de nmotécnicos.

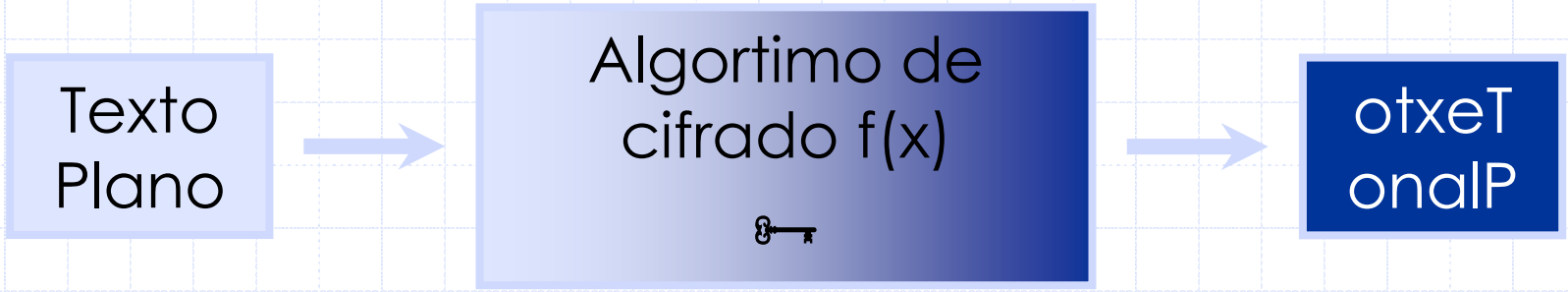
Normas de gestión de passwords

- NO permitir cuentas sin contraseña.
- NO mantener las contraseñas por defecto.
- NO compartirlas.
- NO escribir, enviar o decir la contraseña.
- Cambiarlas periódicamente.

Criptografía

Criptografía: del griego Κρυιπτοζ (Kripto– Oculto). **Arte** de escribir con **clave** secreta o de un modo enigmático.

Ciencia que consiste en transformar un mensaje inteligible en otro que no lo es, mediante la utilización de **claves**, que solo el emisor y receptor conocen.



Métodos Criptográficos

Simétricos o de Clave Privada: se emplea la misma clave para cifrar y descifrar. El emisor y receptor deben conocerlas.

Clásicos

- Método del Cesar
- Transposición
- Sustitución general
- La escítala

Modernos

- Redes de Feistel
- DES–3DES
- IDEA
- Blowfish
- RC5
- CAST
- Rijndael→AES

Métodos Criptográficos

Asimétricos o de Clave Pública: se emplea una doble clave k_p (privada) y K_P (Pública). Una de ellas es utilizada para cifrar y la otra para descifrar. El emisor conoce una y el receptor la otra. Cada clave no puede obtenerse a partir de la otra.

Métodos

⊙ **Diffie–Hellman (DH):** basado en el tiempo necesario para calcular el logaritmo de un número muy alto⊙.

⊙ **RSA:** basado en la dificultad de factorizar números primos muy altos⊙.

⊙ **Curvas Elípticas:** basado en los Logaritmos Discretos de DH y las raíces cuadradas módulo un número compuesto.

⊙ **Muy Alto = 200 dígitos +**

Autenticación

Firma Digital: función Hash de resumen y de longitud constante, que es una muestra única del mensaje original.

Condiciones

”. Si A firma dos documentos produce criptogramas distintos.

. Si A y B firman dos documentos m producen criptogramas diferentes.

⓪. Cualquiera que posea la clave pública de A puede verificar que el mensaje es autenticamente de A.

Métodos

- MD5
- SHA–1
- RIPEMD
- N–Hash
- Snefru
- Tiger
- Haval

Utilidad de la Criptografía

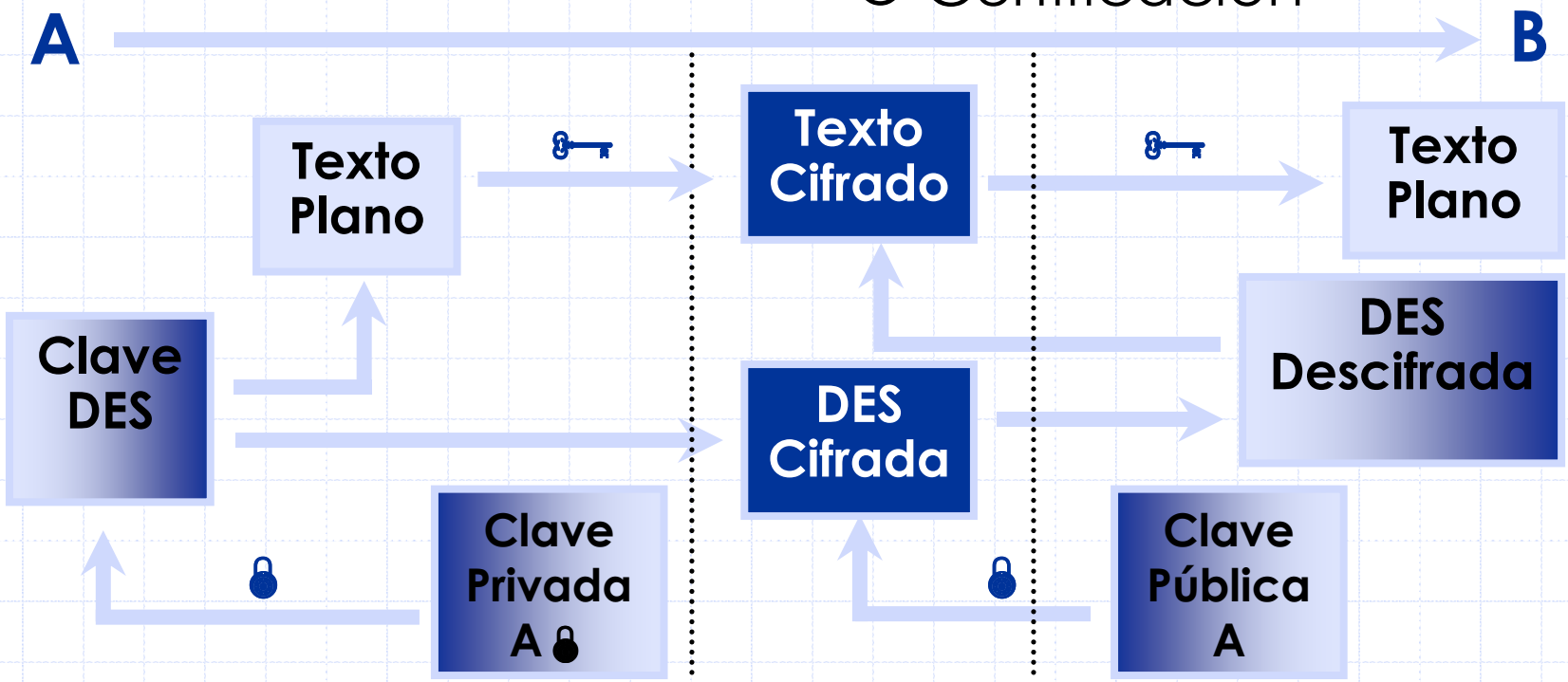
Cifrado

- Confidencialidad

Firma Digital

- Integridad
- No Repudio
- Autentificación
- Actualidad del mensaje
- Certificación

Modelo Cifrado–Firmado



Evaluación de Costos

Siendo:

CP: Costo de los bienes **P**rotegidos.

CR: Costo de los medios para **R**omper la seguridad.

CS: Costo de las medidas de **S**eguridad.

CR > CP: Debe ser más costoso un ataque que el valor de los mismos.

CP > CS: Debe ser más costoso el bien protegido que las medidas de seguridad dispuestas para el mismo.

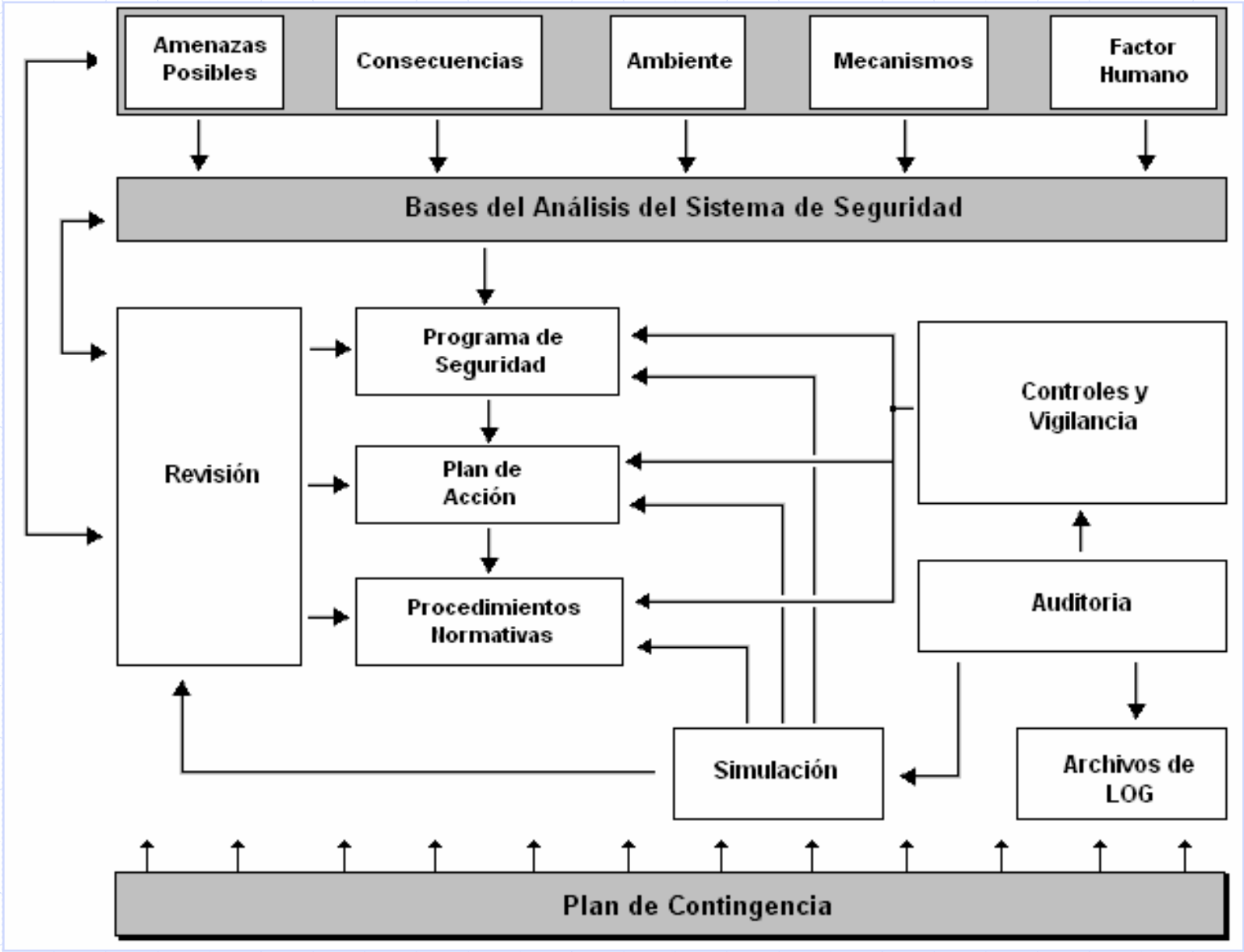
Luego:

CR > CP > CS

Minimiza el costo de la protección.

Maximiza el costo de los atques.

Políticas de Seguridad



Conclusiones

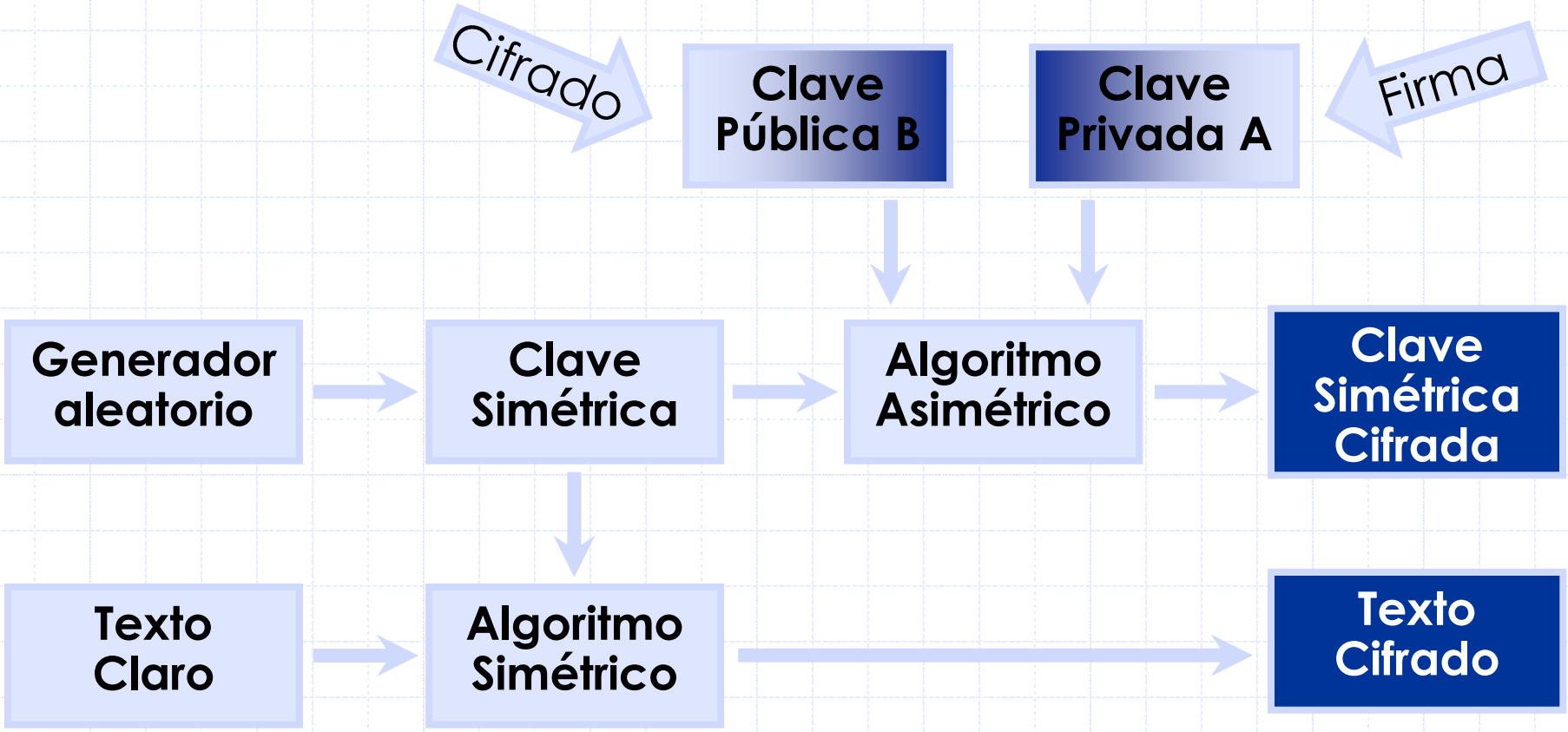
- Se requiere un diseño seguro.
- Adaptación de la legislación vigente.
- Tecnología como elemento protector.
- Los daños son minimizables.
- Los riesgos son manejables.
- Inversión baja comparada con los daños.
- La seguridad es un viaje permanente.

Muchas Gracias !

Diapositivas Extras

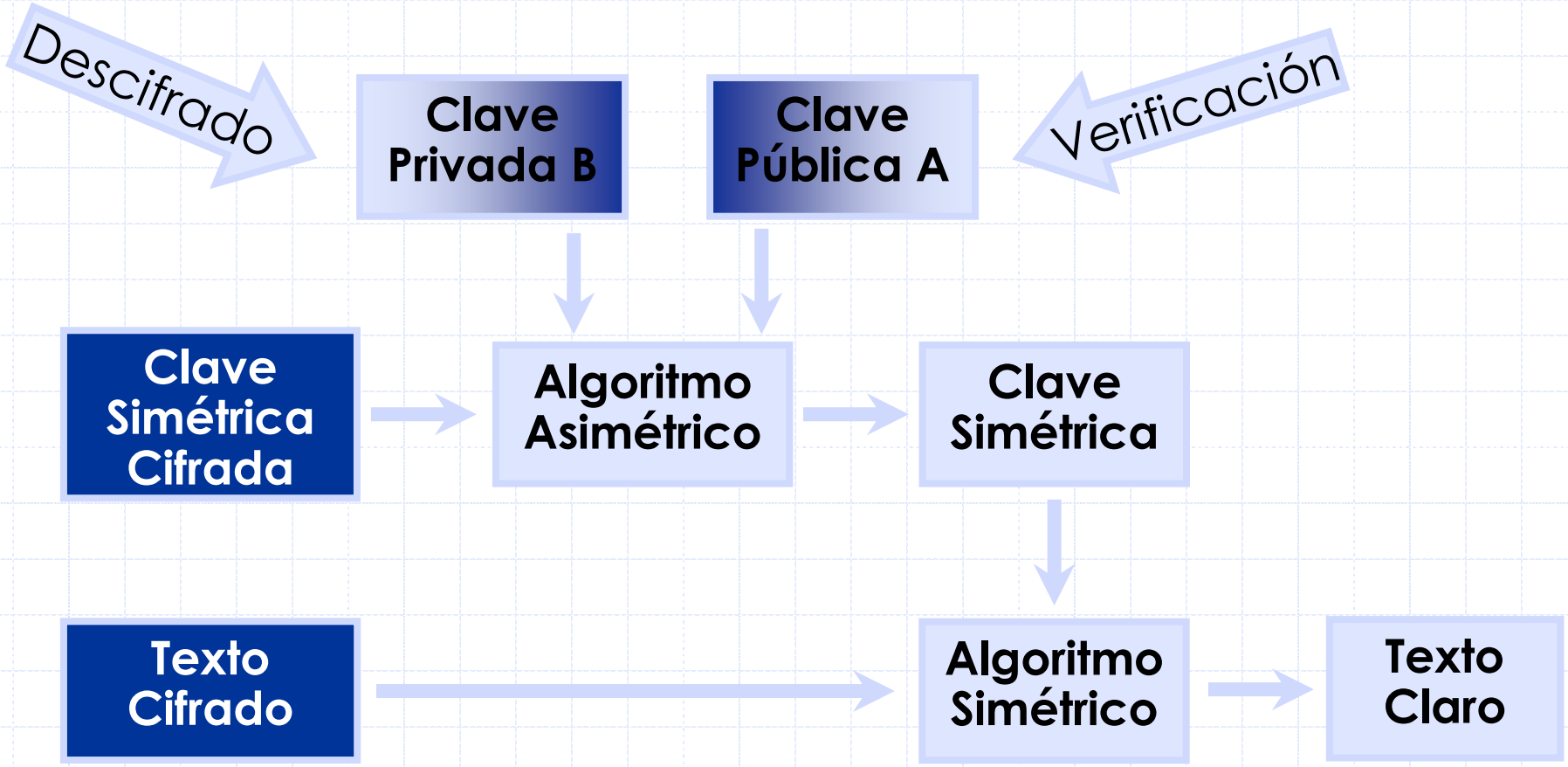
Funcionamiento de PGP

Cifrado y Firmado por parte de A



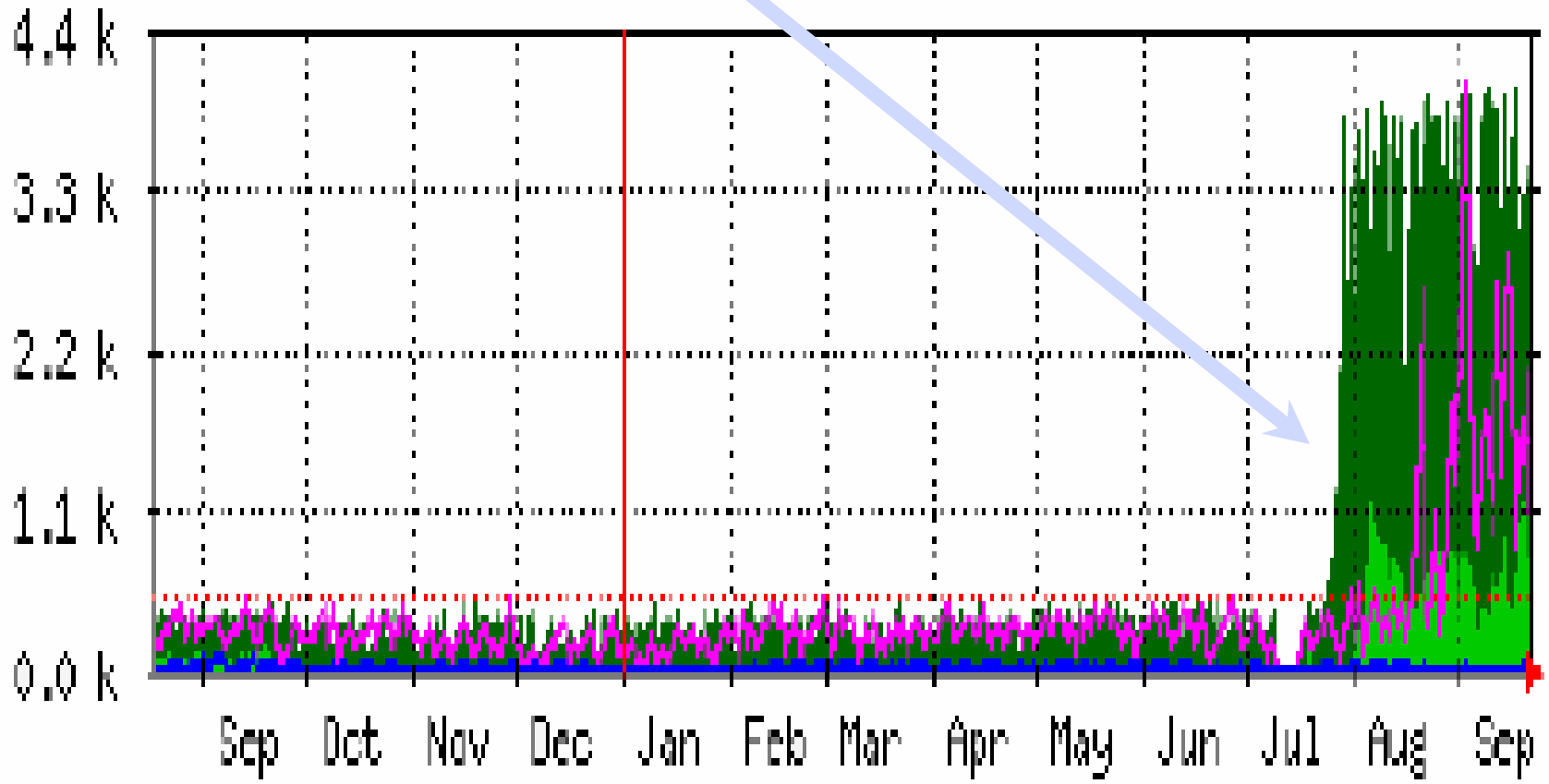
Funcionamiento de PGP

Descifrado y Verificación por parte de B

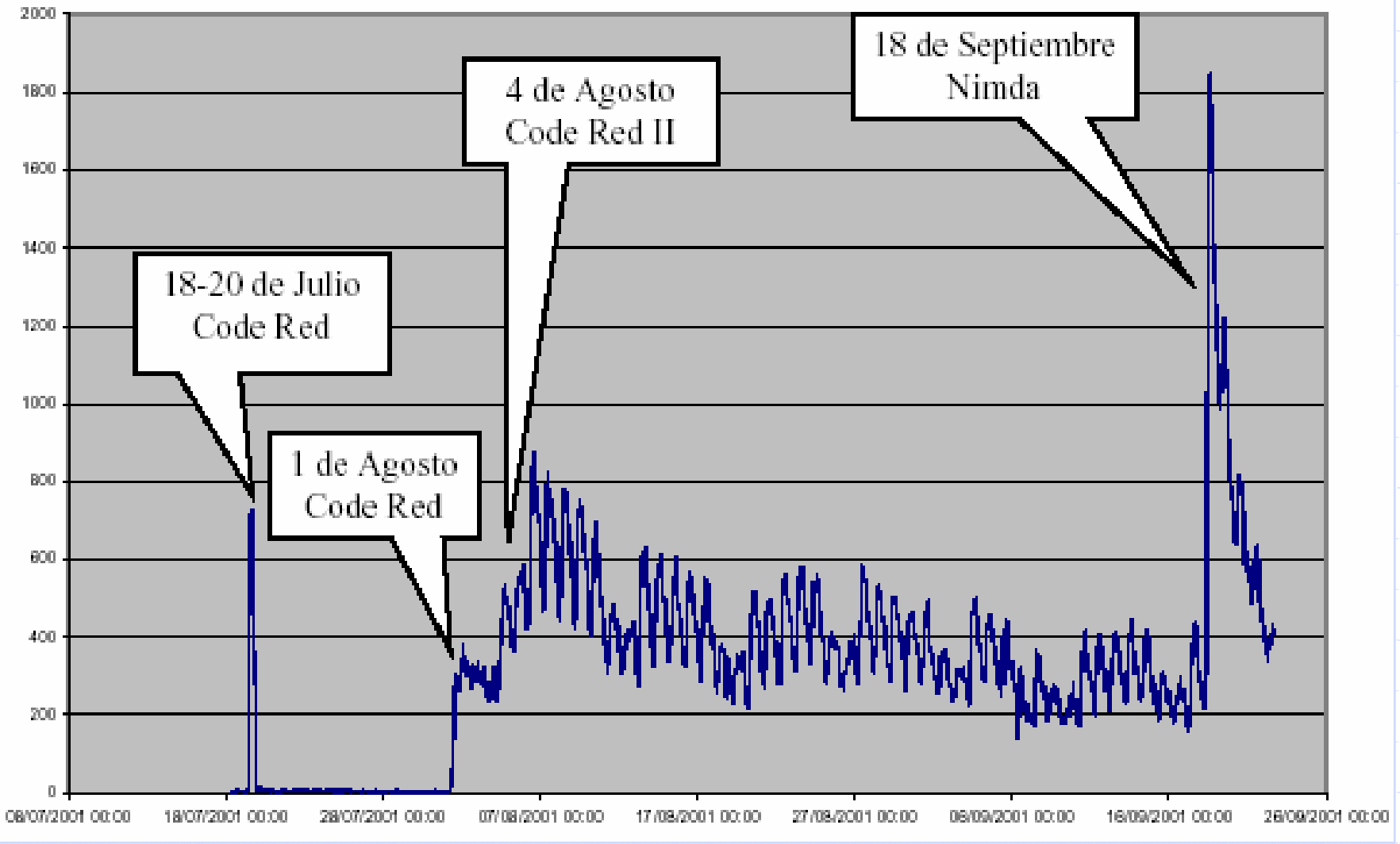


Estadísticas de Ataques

Aparición de los Bugs de IIS



Estadísticas de Ataques



Estadísticas de Ataques