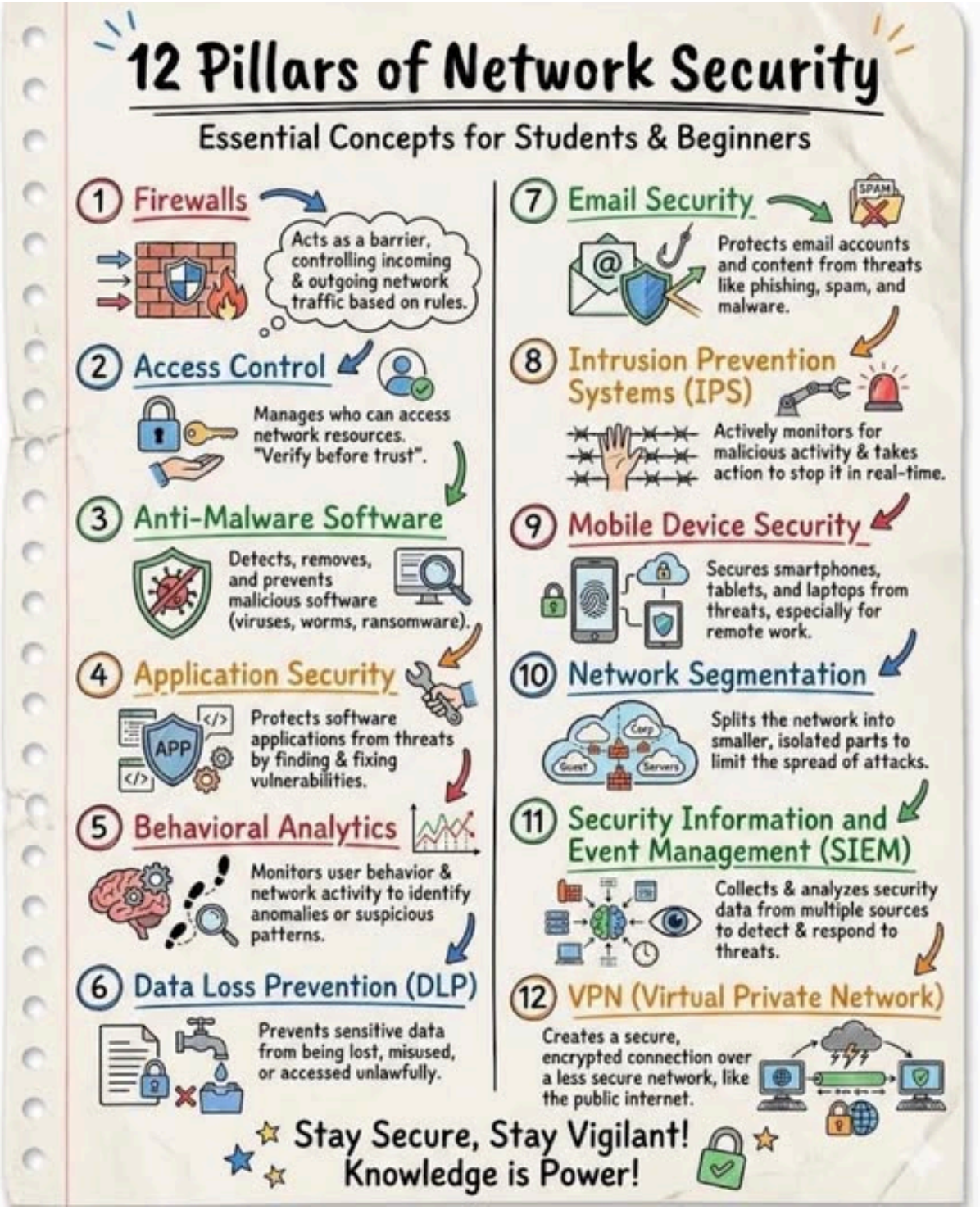
Universidad de Buenos Aires
Facultad de Ciencias Económicas

Los 12 Pilares de la Seguridad en Redes

Material de Estudio



Traducción y Comentarios

12 PILARES DE LA SEGURIDAD DE RED

Conceptos esenciales para estudiantes y principiantes

---

1. Firewalls (Cortafuegos)

Actúan como una **barrera de control** entre redes internas y externas.

Filtran el tráfico entrante y saliente según **reglas de seguridad predefinidas**.

En sistemas de información:

Definen qué comunicaciones están permitidas entre sistemas, usuarios y servicios.

---

2. Control de Acceso (Access Control)

Gestiona **quién puede acceder** a los recursos de red.

Se basa en el principio *"verify before trust"* (verificar antes de confiar).

Incluye:

- autenticación,
- autorización,
- perfiles y roles de usuario.

---

3. Software Anti-Malware

Detecta, elimina y previene software malicioso:

- virus,
- worms (gusanos),
- ransomware.

Malware – Malicious Software / Software malicioso

Impacta directamente en la **continuidad operativa** del negocio.

---

4. Seguridad de Aplicaciones (Application Security)

Protege el software contra amenazas explotando vulnerabilidades.

Incluye:

- análisis de código,
- parches,
- pruebas de seguridad.

Clave para administración:

Las aplicaciones soportan procesos críticos (ventas, finanzas, RRHH).

---

5. Analítica de Comportamiento (Behavioral Analytics)

Monitorea el comportamiento de usuarios y la actividad de red.

Permite detectar:

- anomalías,
- patrones sospechosos,
- accesos inusuales.

Es clave para identificar **amenazas internas**.

---

6. Prevención de Pérdida de Datos

DLP – Data Loss Prevention / Prevención de Pérdida de Datos

Evita que información sensible:

- se filtre,
- se copie,
- se use indebidamente.

Muy relevante para:

- datos financieros,
- datos personales,
- información estratégica.

7. Seguridad del Correo Electrónico (Email Security)

Protege cuentas y contenidos contra:

- phishing,
- spam,
- malware.

El correo es uno de los **principales vectores de ataque** en organizaciones.

---

8. Sistemas de Prevención de Intrusiones

IPS – Intrusion Prevention System / Sistema de Prevención de Intrusiones

Monitorea la red en tiempo real y:

- detecta actividades maliciosas,
- bloquea ataques automáticamente.

A diferencia del IDS, **actúa**, no solo alerta.

---

9. Seguridad de Dispositivos Móviles (Mobile Device Security)

Protege:

- smartphones,
- tablets,
- laptops.

Especialmente crítico en:

- trabajo remoto,
- esquemas BYOD (*Bring Your Own Device / Trae tu propio dispositivo*).

---

10. Segmentación de Red (Network Segmentation)

Divide la red en partes más pequeñas y controladas.

Limita la propagación de ataques.

Beneficio clave:

Un incidente no compromete toda la organización.

---

11. Gestión de Eventos e Información de Seguridad

SIEM – Security Information and Event Management / Gestión de Información y Eventos de Seguridad

Recolecta y analiza datos de múltiples fuentes:

- logs,
- firewalls,
- servidores,
- aplicaciones.

Permite **detectar, correlacionar y responder** a amenazas.

---

12. VPN

VPN – Virtual Private Network / Red Privada Virtual

Crea una conexión:

- segura,
- cifrada,
- sobre redes públicas como Internet.

Fundamental para:

- acceso remoto,
- protección de datos en tránsito.

Mensaje central del esquema

Mantenerse seguro exige vigilancia constante.

En los sistemas de información, la seguridad no es solo técnica: es un **factor estratégico para la gestión, la continuidad del negocio y la confianza**

organizacional.

Material de Clases

Compilado por **Aníbal M. Mazza Fraquelli** Doctor de la Universidad de Buenos Aires para el uso de sus clases en la Facultad de Ciencias Económicas de la Universidad de Buenos Aires.

Contenidos de esta página

Los contenidos **aquí incluidos integran desarrollos y escritos propios del autor, así como materiales de terceros (documentos, textos, fragmentos, conceptos, imágenes, esquemas, definiciones u otros recursos),** los cuales son utilizados a título ilustrativo, explicativo o formativo, respetando la normativa vigente en materia de derechos de autor y citando las fuentes cuando corresponde.
La selección, organización, adaptación pedagógica y contextualización de los contenidos constituye un trabajo original del autor, orientado a facilitar los procesos de enseñanza y aprendizaje.
Este material no persigue fines comerciales y su reproducción, total o parcial, queda limitada al ámbito educativo, debiendo preservarse siempre la mención de la autoría y las fuentes originales.

Autorización de uso

Se permite la reproducción, comunicación pública, distribución y utilización total o parcial de los contenidos de su material, en formato físico o digital, con fines exclusivamente educativos, académicos o de divulgación, siempre que se respete la integridad del contenido y se incluya la correspondiente referencia a la fuente y a la autoría.
Las ideas, opiniones e interpretaciones contenidas en este material corresponden exclusivamente al autor.
Queda expresamente excluido cualquier uso con fines comerciales.