Modelos Matematicos de Propagacion de Virus Informaticos:

Marco Teorico

El modelo SIR es un modelo dinámico clásico, propuesto por Kermack y McKendrick. Describe la evolución temporal de una población dividida en tres compartimentos:

- S(t) (susceptibles)
- I(t) (infectados)
- R(t) (recuperados).

Parámetros:

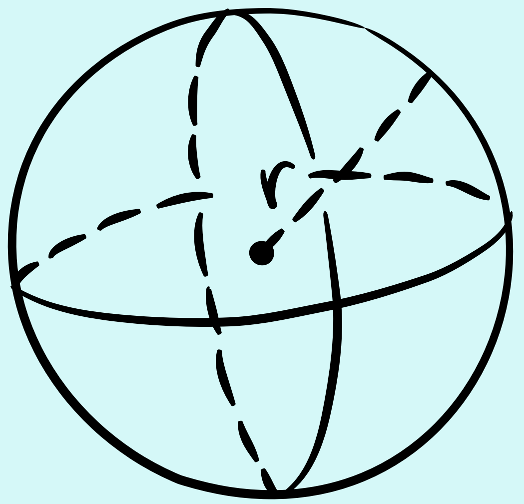
- β :eficacia del vector de infección.
- γ :eficacia de la respuesta.
- R_0 :mide cuán rápido se expande un brote digital en su fase inicial.

Analogía:

- S (Susceptibles): dispositivos vulnerables pero aún no comprometidos.
- I (Infectados): equipos comprometidos que pueden seguir propagando el malware.
- R (Recuperados): dispositivos limpiados, parcheados o aislados que ya no difunden el ataque.

$$\frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

$$y = mx + b$$



$$V = \frac{4}{3}\pi r^3$$

Modelo lineal

Se selecciona un troyano de acceso remoto (RAT), porque:

- Su propagación depende de la interacción humana
- Es una amenaza persistente en entornos corporativos y domésticos
- Permite estudiar el efecto de medidas de contención

Variables

- $I(t)$:computadores infectados en el tiempo
- $r(t)$:tasa de nuevas infecciones
- N :tamaño de la red al inicio

Tasa de propagación propuesta

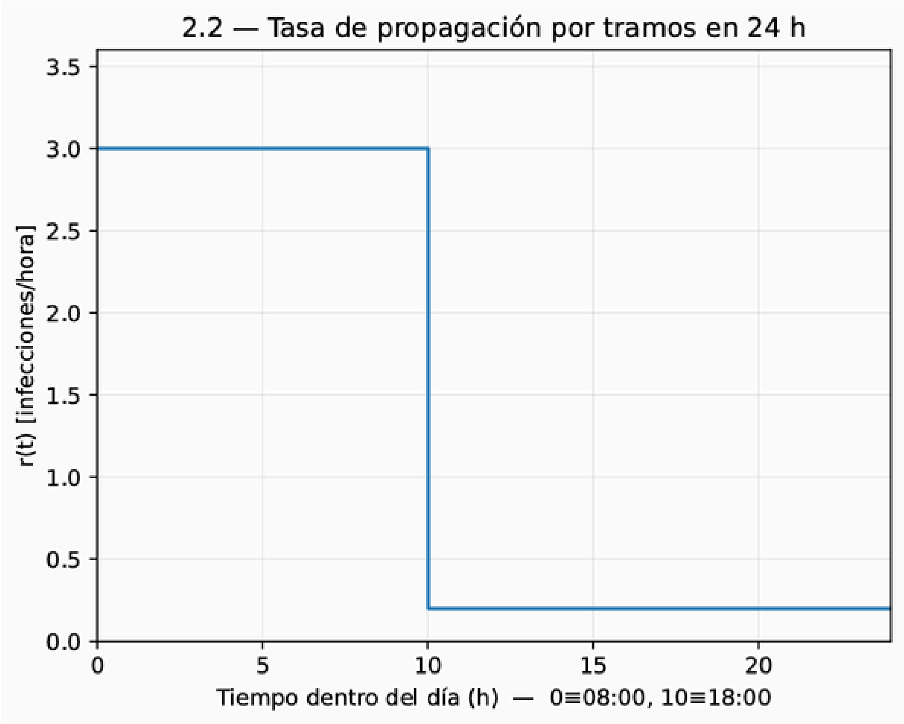
$$r(t) = \begin{cases} 3 \text{ infecciones/hora}, & \text{si } t \text{ esta en } [08{:}00, 18{:}00], \\ \rho \text{ infecciones/hora}, & \text{fuera de ese horario, con } 0 < \rho \ll 3 \end{cases}$$

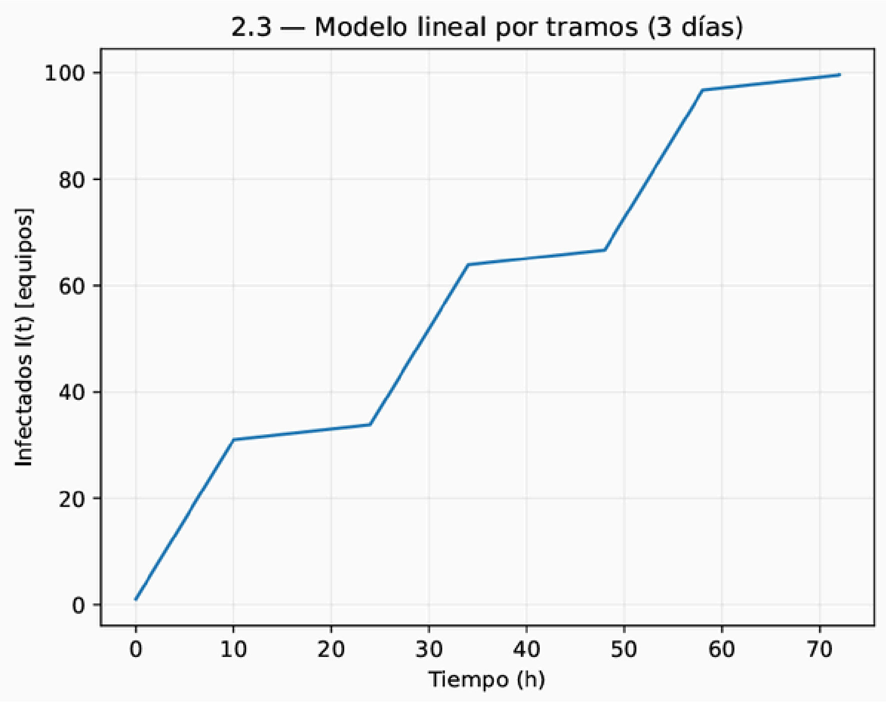
Ecuación diferencial

$$I(t) = \begin{cases} I_0 + 3\,t, & 0 \le t \le 10, \\ I_0 + 30 + \rho\,(t - 10), & 10 < t \le 24. \end{cases}$$

Supuestos

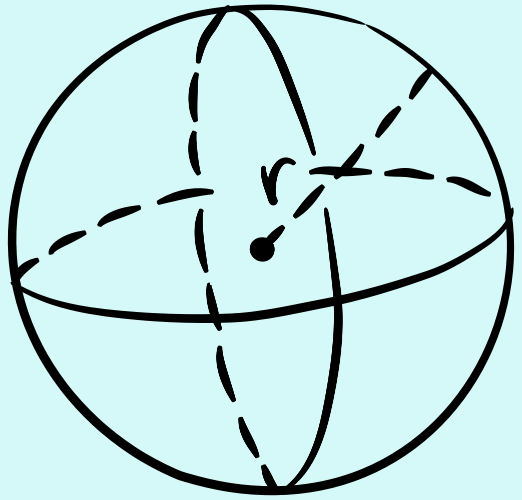
- $N = 1000$,equipos susceptibles inicialmente; condición inicial
- Actividad principal en la jornada laboral (08:00–18:00); fuera de ese rango la actividad disminuye, pero no es nula.
- Etapa temprana: el modelo lineal se usa mientras $I \leqslant N$





$-b \pm \sqrt{b^2 - 4a}$ / $2a$

$y = mx + b$



$V = \frac{4}{3}\pi r^3$

Modelo no lineal

Dependencia temporal:

- Más infecciones en horario laboral (08:00–18:00).
- Oleadas de phishing al inicio, luego decrecen.
- Medidas de seguridad (parches, filtros) reducen r(t).

Dependencia en el estado:

- Saturación: menos equipos vulnerables → propagación se frena.
- Concientización: más infectados → usuarios y defensas se vuelven más cuidadosos.

Ecuacion diferencial

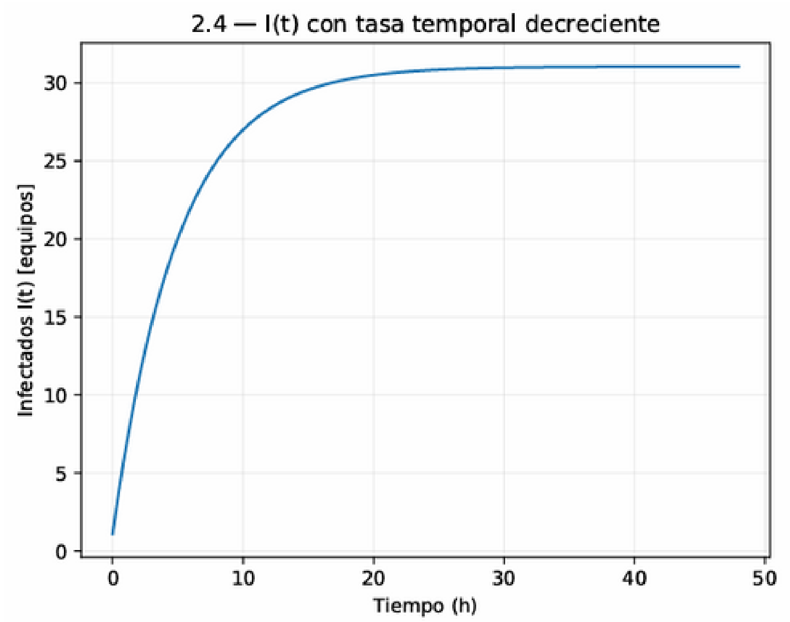
$$I'(t) = r\,I(t)\left(1 - \frac{I(t)}{K}\right), r, K > 0, I(0) = I_0 \in (0, K).$$

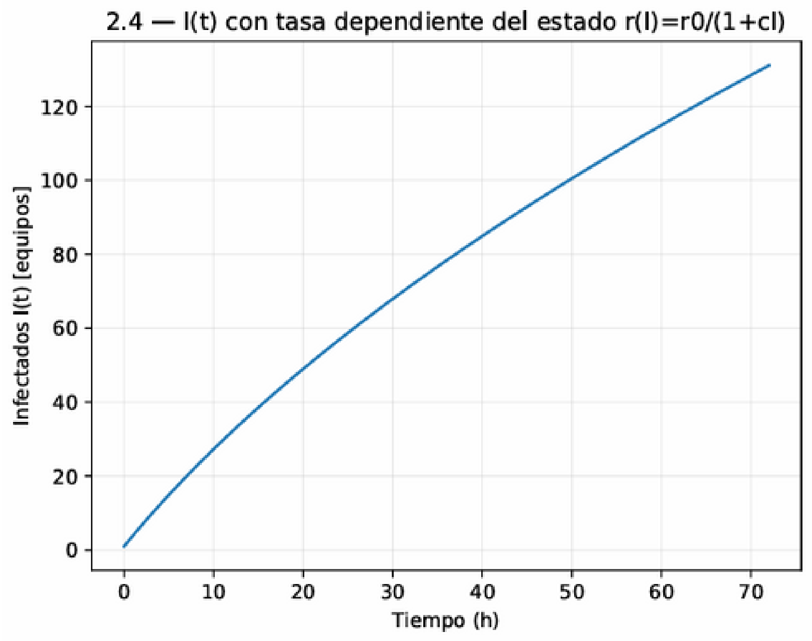
Solución analítica

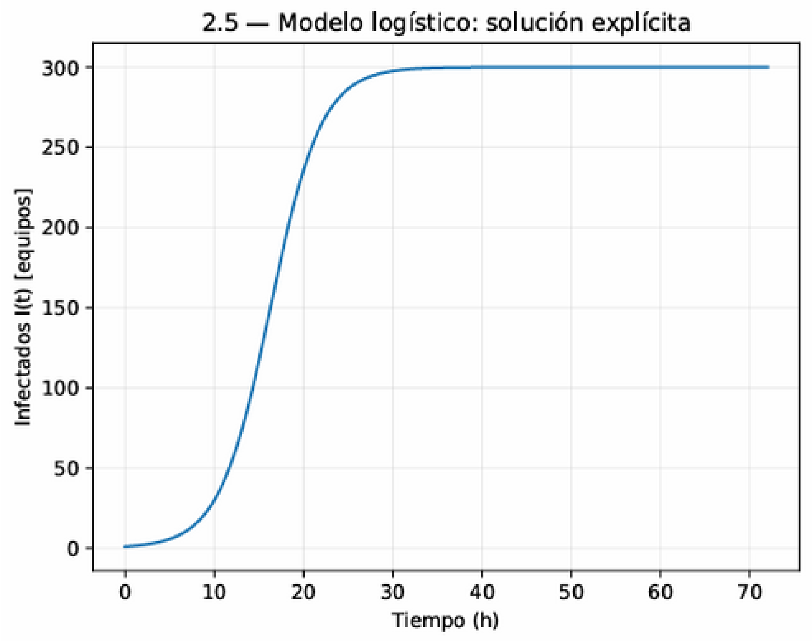
$$I(t) = \frac{K}{1 + A\,\mathrm{e}^{-rt}}, \qquad A = \frac{K - I_0}{I_0}.$$

Interpretación de parámetros:

- r :controla la rapidez de la propagación inicial (pendiente en torno a
- K :es la capacidad efectiva o nivel maximo esperable dadas las barreras
- I_0 :fija el punto de partida

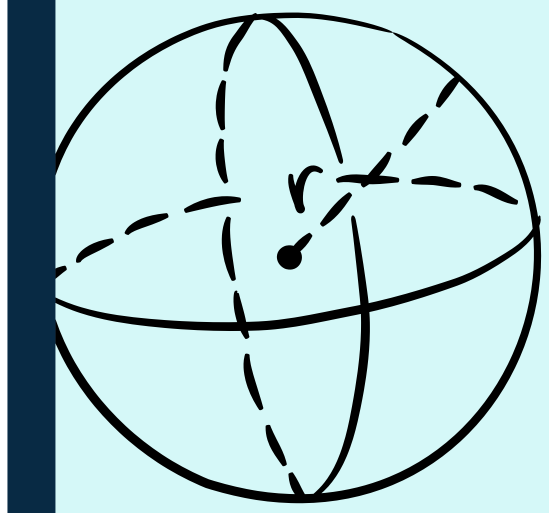






$\frac{-b \pm \sqrt{b^2 - 4a}}{2a}$

$y = mx + b$



$V = \frac{4}{3}\pi r^3$

Conclusiones

- Lineal: útil en el corto plazo.
- Logístico: mejor en mediano plazo, incluye límites reales.
- Parámetros clave:
  - r: velocidad de propagación.
  - K: capacidad máxima.
- En ciberseguridad:
  - Reducir r → concientización, filtros, antivirus.
  - Reducir K → aislamiento, parches, segmentación.

Lineal

Ecuación:

- Ventajas: simple, describe bien etapas tempranas y horarios laborales.
- Limitación: predice crecimiento indefinido si no baja.

Logístico

Ecuación:

- Ventajas: incluye saturación y concientización → curva con meseta.
- Limitación: no refleja horarios ni shocks de campañas directamente.