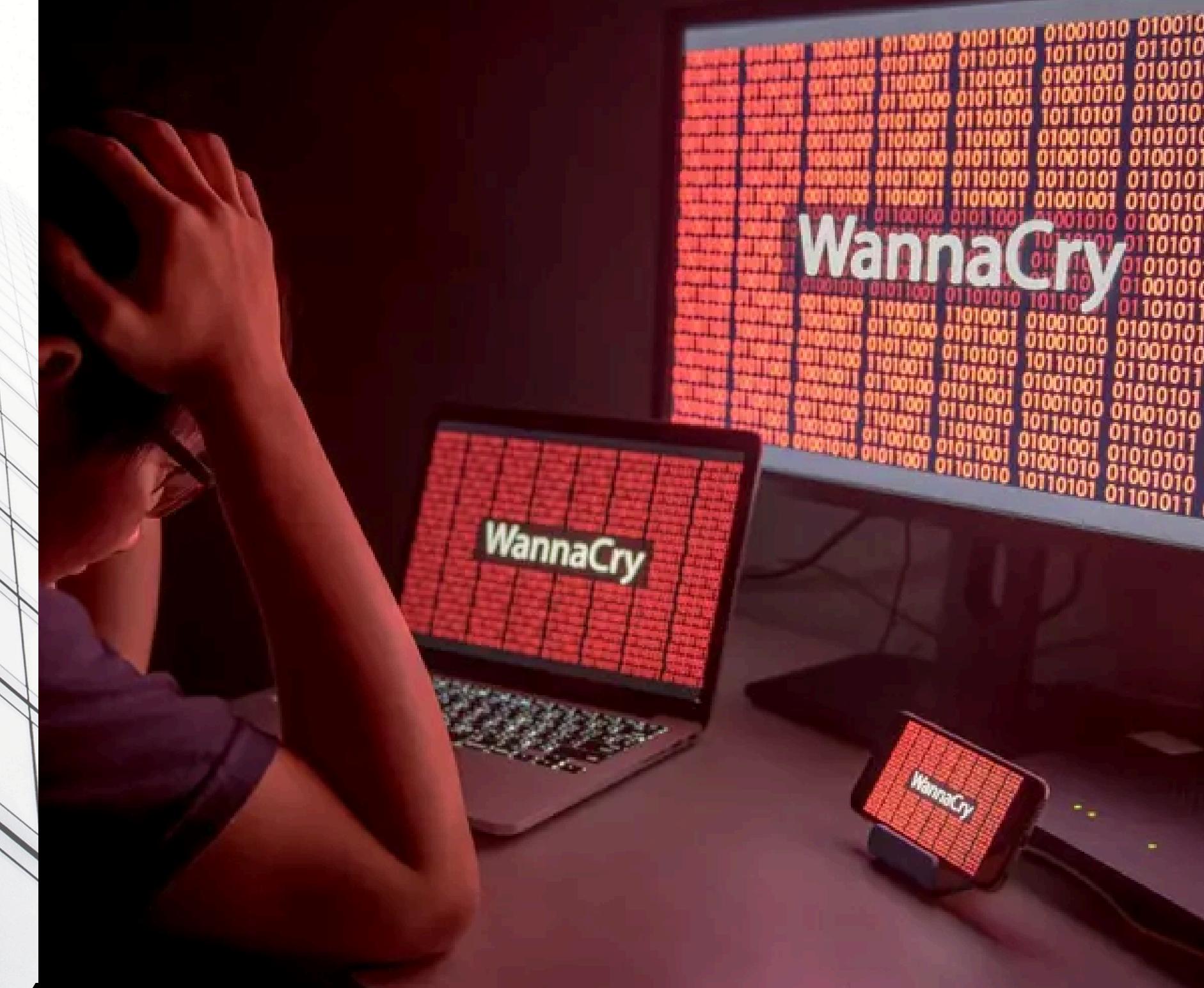


MODELAJE Y SIMULACIÓN DE UN POSIBLE BROTE DE WANNACRY



Miguel Ángel Rodríguez Feregrino

OBJETIVO

A PARTIR DE UNA APROXIMACIÓN MATEMÁTICA DESCRIBIR LA DINÁMICA DE INFECCIÓN DE UN
MALWARE TIPO RANSOMWARE (WANNA CRY) Y, A PARTIR DE ESTE MODELAJE SIMULAR
POR MEDIO DEL PAQUETE DESOLVE EL BROTE OCURRIDO EN 2017 JUNTO CON POSIBLES
ESCENARIOS ALTERNOS.

WANNA CRY

Ransomware tipo gusano. Transmisión local, con capacidad de sensar vulnerabilidad y copiarse en otros dispositivos.

En 2017 se liberó gracias al descubrimiento de la vulnerabilidad Eternal Blue presente en dispositivos Windows XP, Windows 7 y Windows 10 de ese entonces.

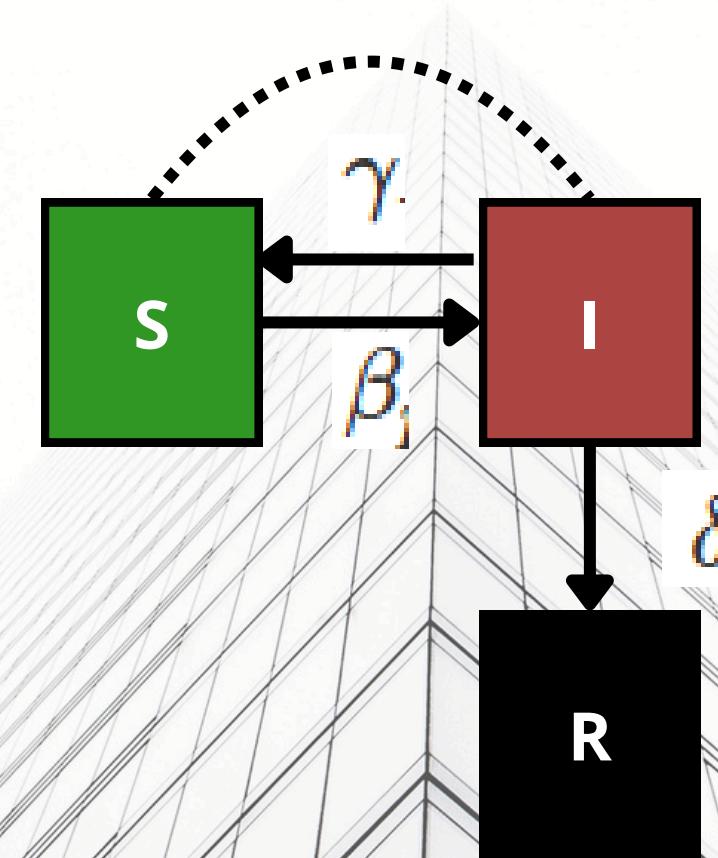
Grupo Lazarus, desde Corea del Norte publicaron el archivo, provocando cerca de 200,000 contagios en menos de 5 horas a nivel global, afectando instituciones de todo tipo.

Gracias a la liberación acelerada del prototipo este contaba con un kill switch, por lo que a menos de 24 h del ataque se pudo controlar la infección.

Este tipo de virus tienen una dinámica particular por la cual es útil estudiarlos. Diversos modos de transmisión dependen del estadio de infección y la conectividad local del infectado, junto con una amplia variedad de métodos de control.



MODELO BASE, SIS CON D



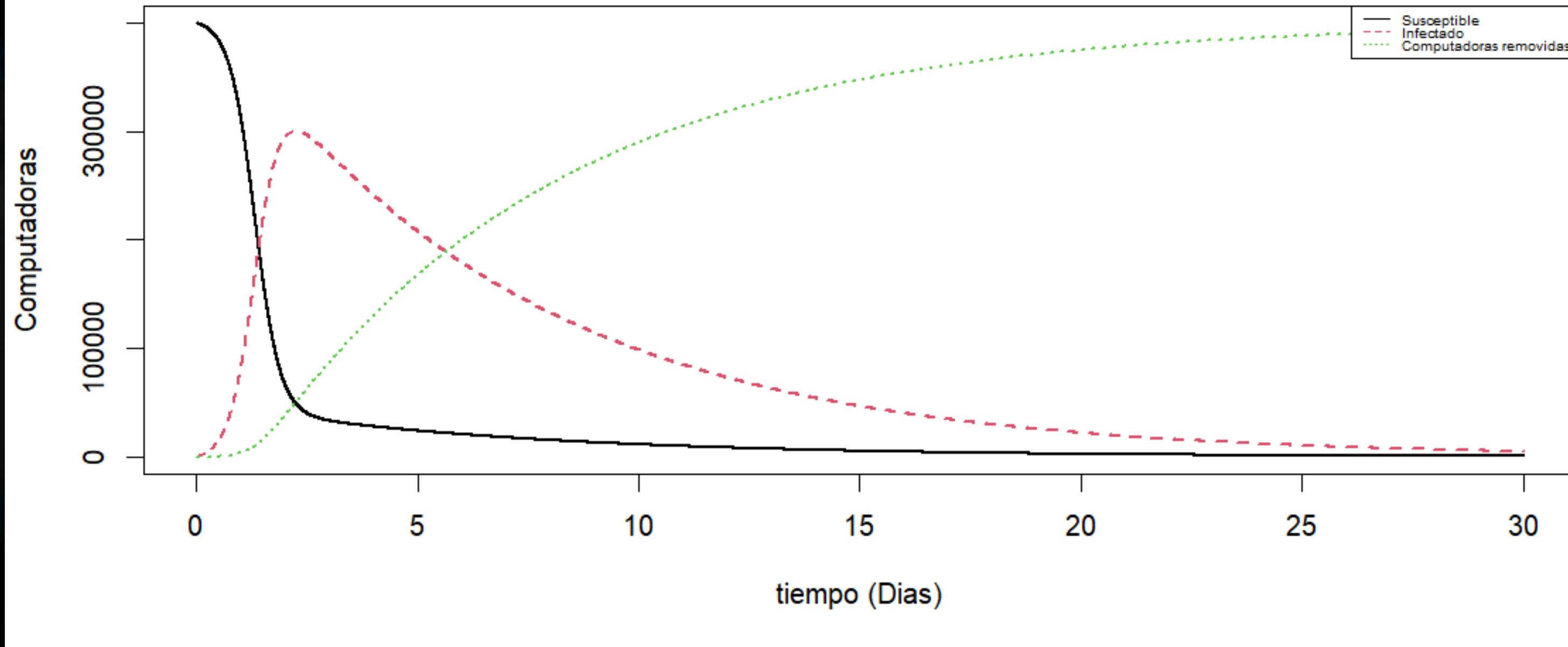
$$N_{\text{eff}} = S + I$$

$$\frac{dS}{dt} = \gamma I - \beta_p S - \beta_l \frac{SI}{N_{\text{eff}}}$$

$$\frac{dI}{dt} = \beta_p S + \beta_l \frac{SI}{N_{\text{eff}}} - \gamma I - \delta I$$

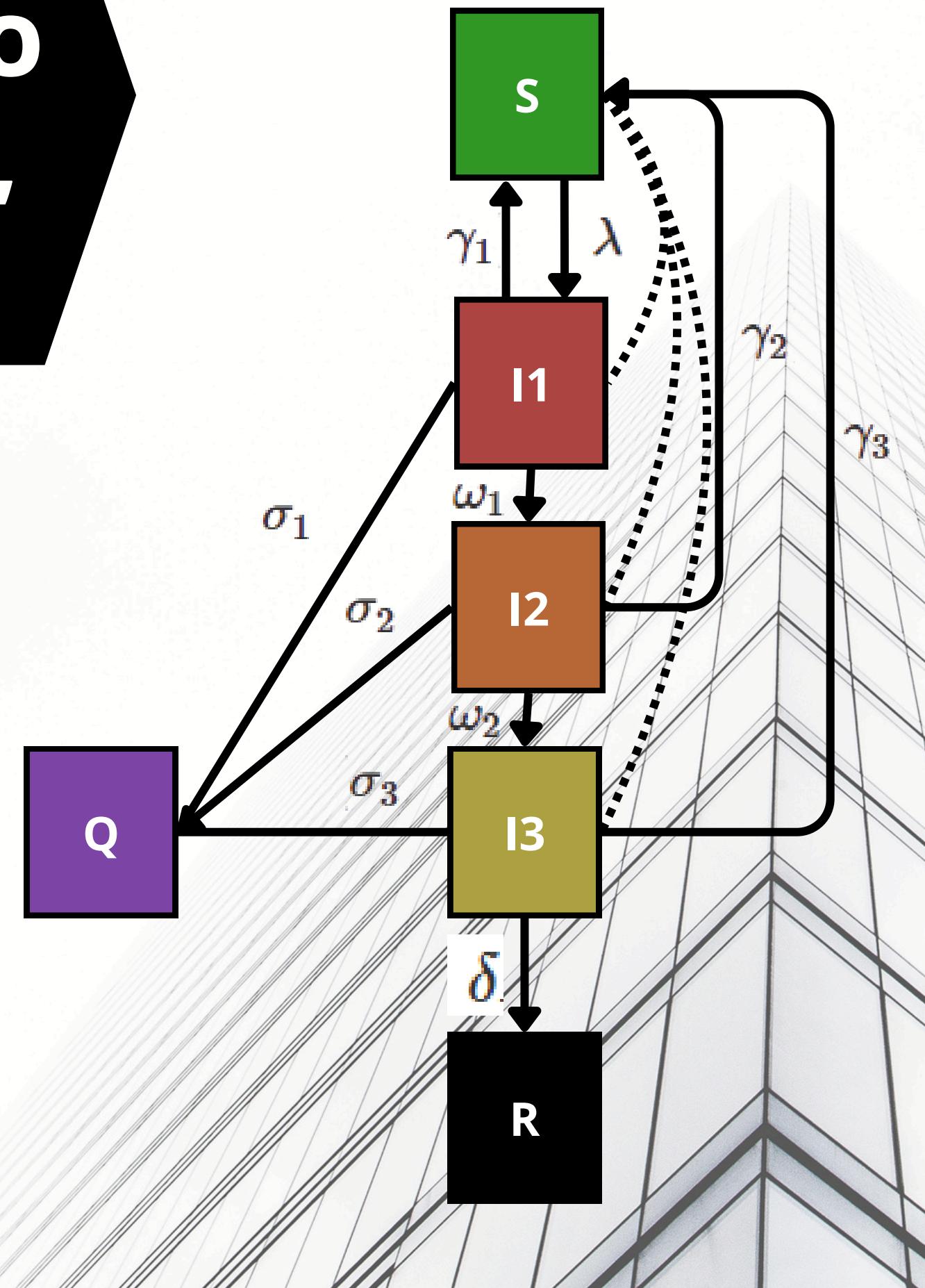
$$\frac{dR}{dt} = \delta I$$

Modelo inicial de WannaCry tipo SID



MODELO INICIAL, TIPO SIQS CON D, ERLANG

- Se incorporan estados de infección para cambiar distribución a tipo Erlang.
- Se incorpora recuperación, cuarentena y variabilidad de infección.



$$N_{\text{eff}} = S + I_1 + I_2 + I_3 + Q$$

$$\lambda = \mu\beta_p + \beta_{l1} \frac{I_1}{N_{\text{eff}}} + \beta_{l2} \frac{I_2}{N_{\text{eff}}} + \beta_{l3} \frac{I_3}{N_{\text{eff}}}$$

$$\frac{dS}{dt} = -\lambda S + \gamma_1 I_1 + \gamma_2 I_2 + \gamma_3 I_3$$

$$\frac{dI_1}{dt} = \lambda S - (\sigma_1 + \omega_1 + \gamma_1) I_1$$

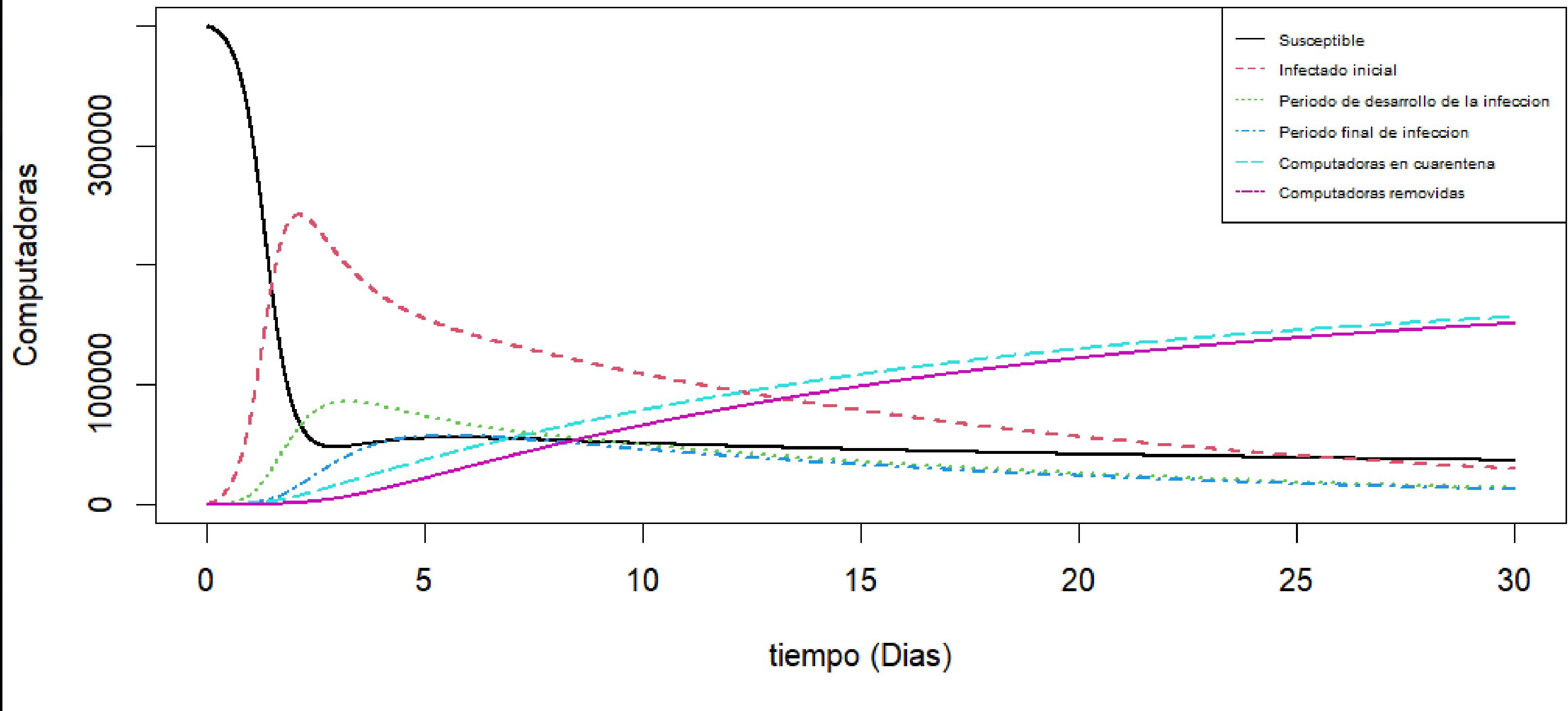
$$\frac{dI_2}{dt} = \omega_1 I_1 - (\sigma_2 + \omega_2 + \gamma_2) I_2$$

$$\frac{dI_3}{dt} = \omega_2 I_2 - (\sigma_3 + \gamma_3 + \delta) I_3$$

$$\frac{dQ}{dt} = \sigma_1 I_1 + \sigma_2 I_2 + \sigma_3 I_3$$

$$\frac{dR}{dt} = \delta I_3$$

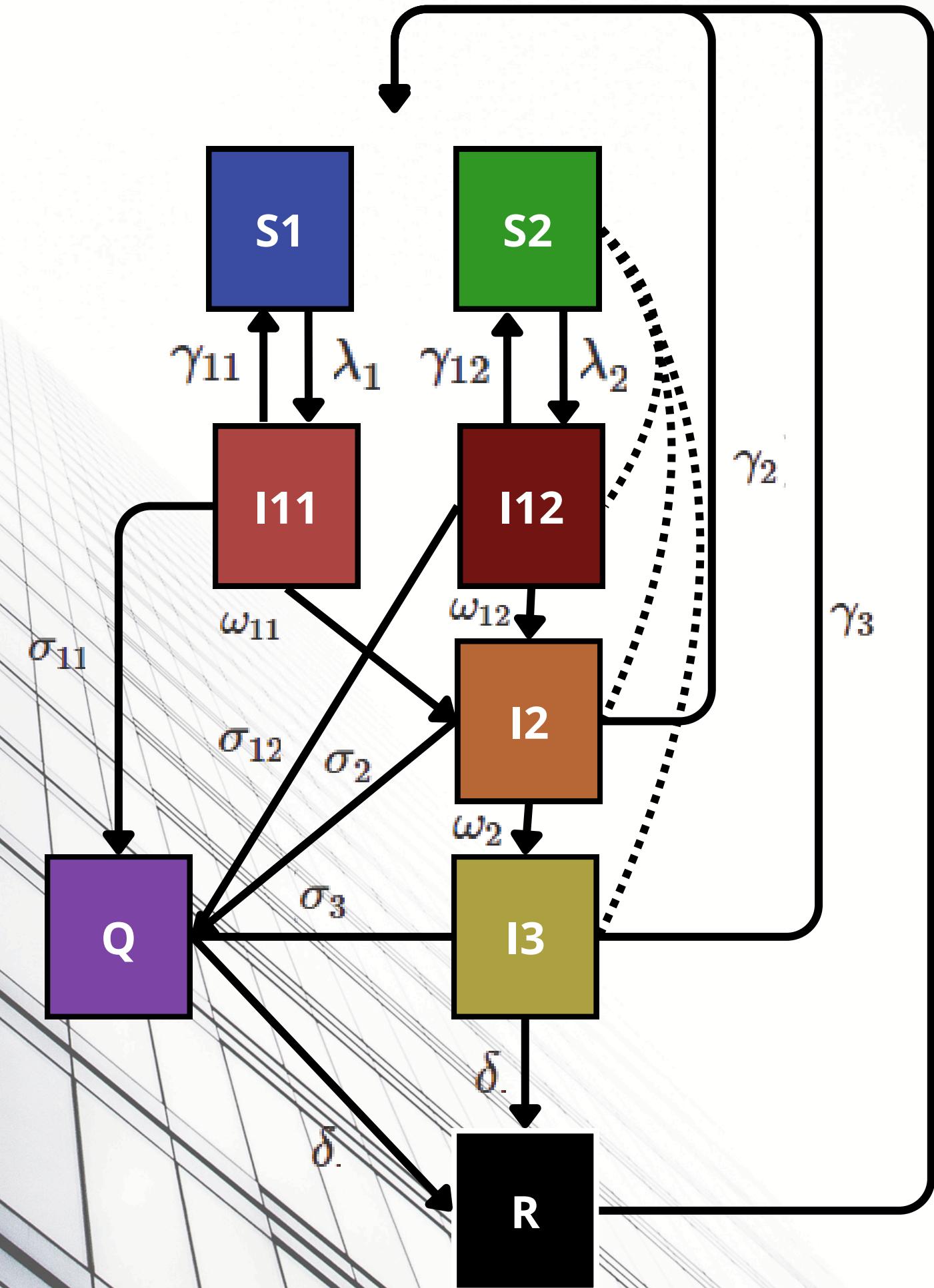
Modelo inicial de WannaCry a partir de teoria



MODELO ESPECIFICO

- Se incorporan diferentes estados de susceptibilidad dependiendo del nivel de conexiones.
- Se incorporan diferentes estados de infección inicial.
- Recuperación de dispositivos removidos
- Remoción final en cuarentena.
-

03



$$N_{\text{eff}} = S_1 + S_2 + I_{11} + I_{12} + I_2 + I_3 + Q$$

$$\lambda_1 = \mu\beta_{p1} + \beta_{l1,11} \frac{I_{11}}{N_{\text{eff}}} + \beta_{l1,12} \frac{I_{12}}{N_{\text{eff}}} + \beta_{l2} \frac{I_2}{N_{\text{eff}}} + \beta_{l3} \frac{I_3}{N_{\text{eff}}}$$

$$\lambda_2 = \mu\beta_{p2} + \beta_{l2,11} \frac{I_{11}}{N_{\text{eff}}} + \beta_{l2,12} \frac{I_{12}}{N_{\text{eff}}} + \beta_{l2} \frac{I_2}{N_{\text{eff}}} + \beta_{l3} \frac{I_3}{N_{\text{eff}}}$$

$$\frac{dS_1}{dt} = -\lambda_1 S_1 + p_{11}\gamma_{11}I_{11} + p_{12}\gamma_{12}I_{12} + p_2\gamma_2I_2 + p_3\gamma_3I_3 + \alpha p R$$

$$\frac{dS_2}{dt} = -\lambda_2 S_2 + (1 - p_{11})\gamma_{11}I_{11} + (1 - p_{12})\gamma_{12}I_{12} + (1 - p_2)\gamma_2I_2 + (1 - p_3)\gamma_3I_3 + \alpha(1 - p)R$$

$$\frac{dI_{11}}{dt} = \lambda_1 S_1 - (\sigma_{11} + \omega_{11} + \gamma_{11})I_{11}$$

$$\frac{dI_{12}}{dt} = \lambda_2 S_2 - (\sigma_{12} + \omega_{12} + \gamma_{12})I_{12}$$

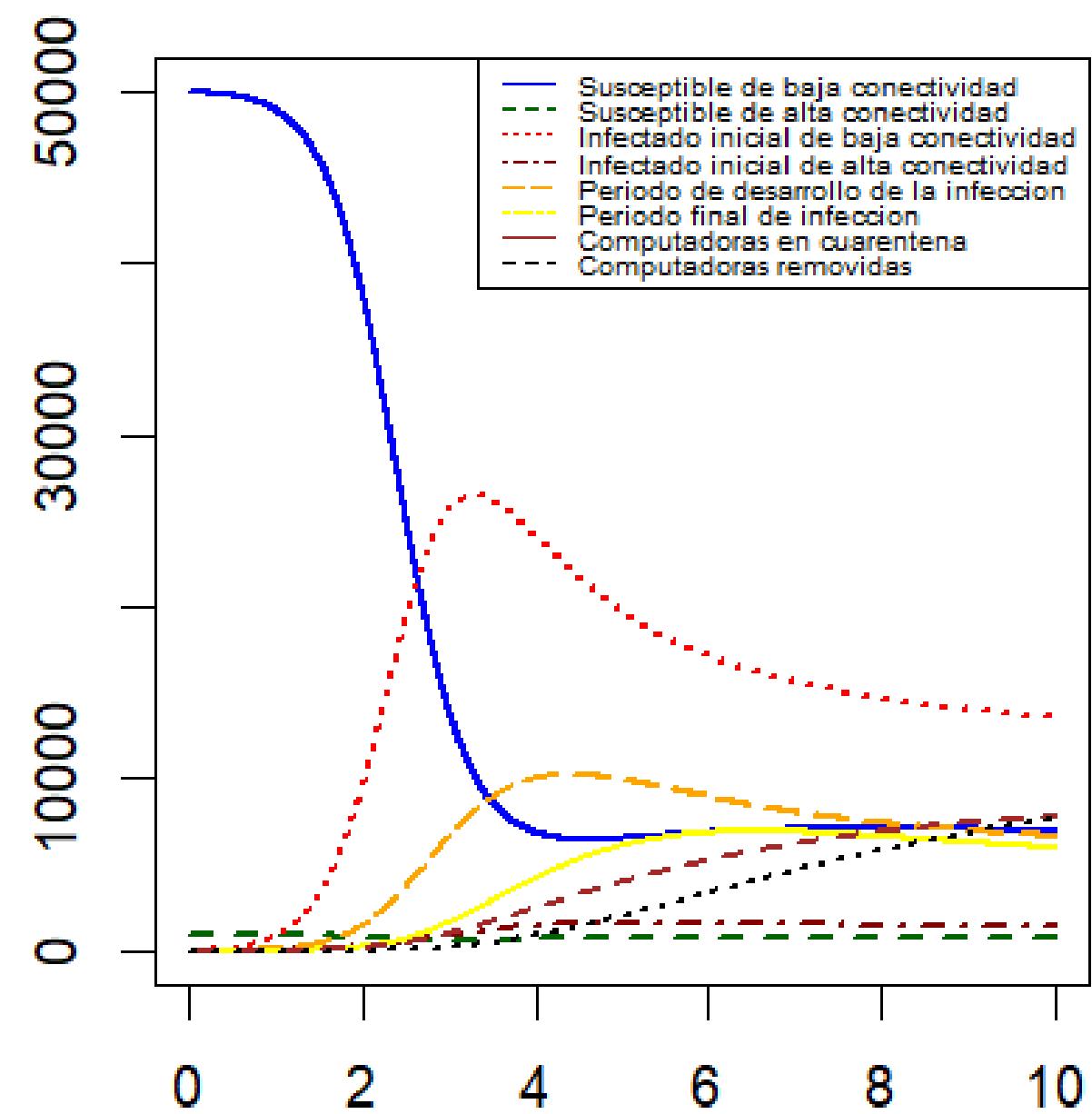
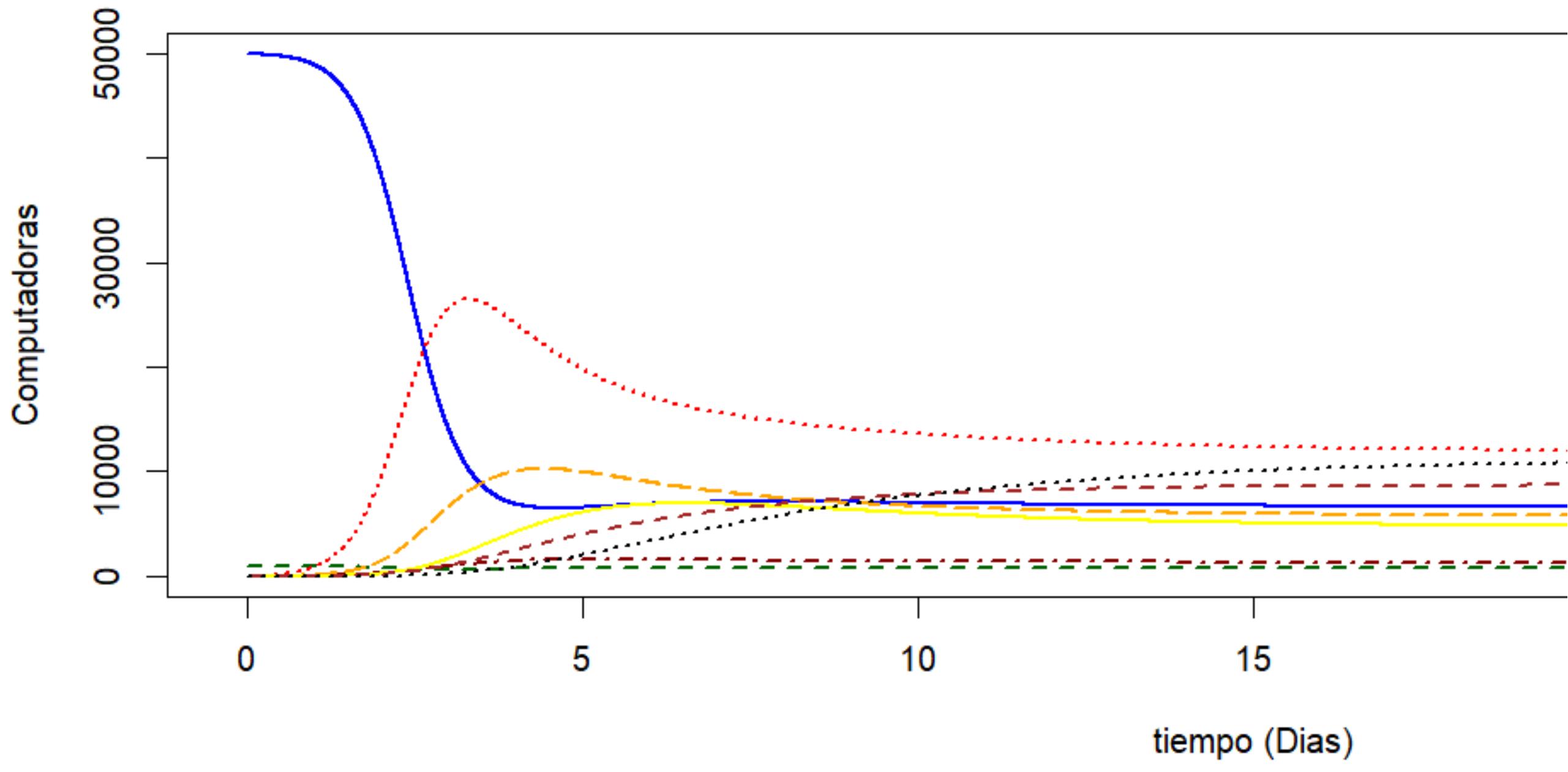
$$\frac{dI_2}{dt} = \omega_{11}I_{11} + \omega_{12}I_{12} - (\sigma_2 + \omega_2 + \gamma_2)I_2$$

$$\frac{dI_3}{dt} = \omega_2I_2 - (\sigma_3 + \gamma_3 + \delta)I_3$$

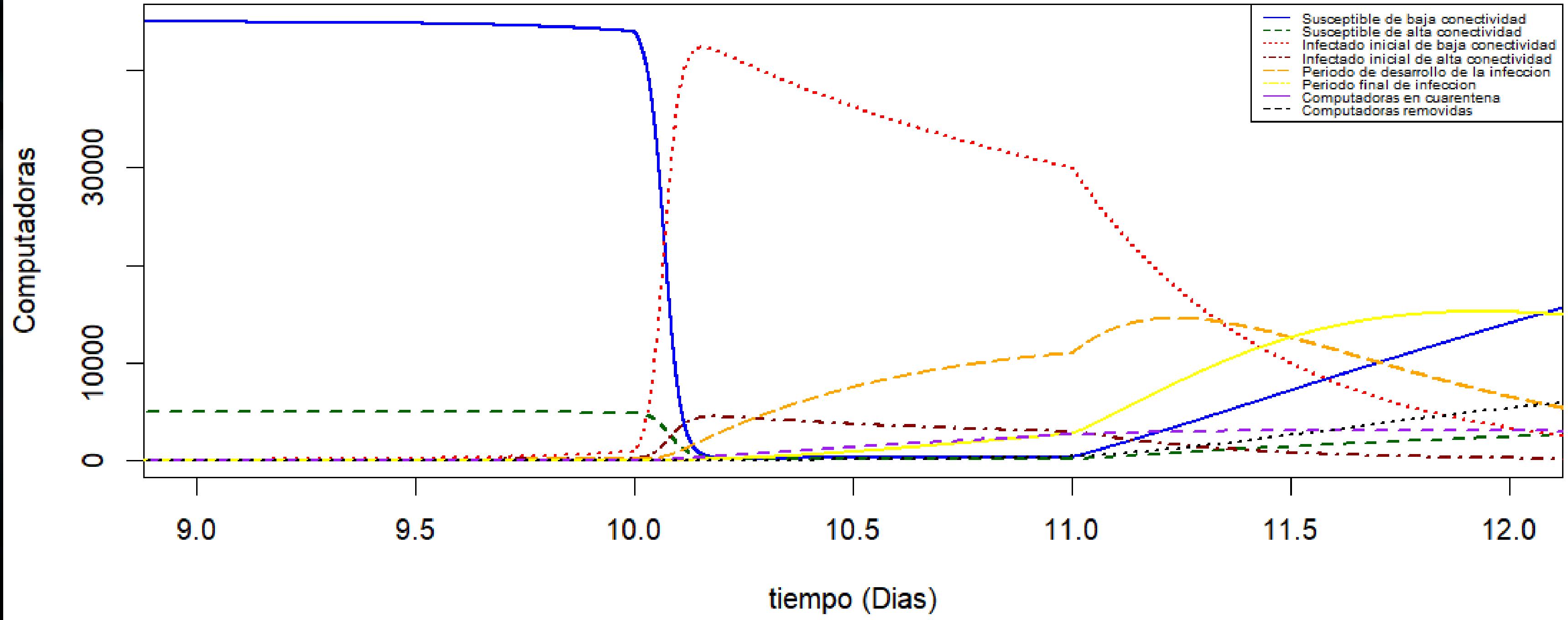
$$\frac{dQ}{dt} = \sigma_{11}I_{11} + \sigma_{12}I_{12} + \sigma_2I_2 + \sigma_3I_3 - \delta Q$$

$$\frac{dR}{dt} = \delta I_3 + \delta Q - \alpha R$$

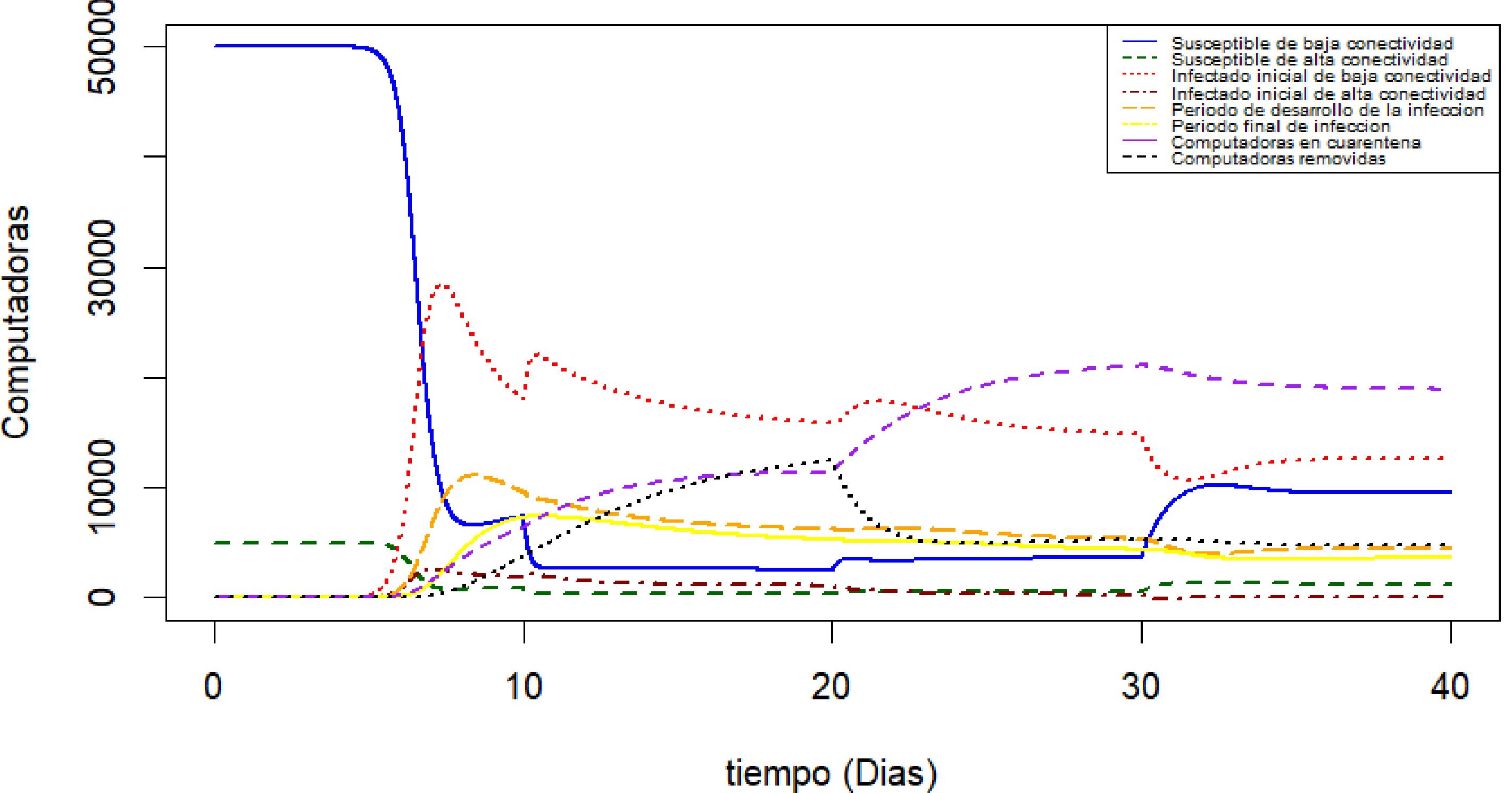
Modelo avanzado de WannaCry a partir de teoria



Simulacion de outbreak de WannaCry en 2017



Simulacion de outbreak de Wannacry y respuesta dinamica en el tiempo



1. El brote empieza el día 10.
2. El inicio del brote es explosivo, alta tasa de infección, además la introducción de infectados es de muchos con alta conectividad.
3. Al inicio del brote por emergencia la gente paga el tratamiento.
4. Pasados 10 días del brote inicial la gente comienza a recuperar sus dispositivos por copias externas y por apoyo de la comunidad.
5. Pasados 10 días del brote se promueve más la cuarentena de los dispositivos una vez se detecta la infección.
6. Pasados 15 días se detiene totalmente el flujo de archivos transmisores de la infección.
7. Pasados 20 días del brote inicial se promueve la actualización de los dispositivos, por lo que la infección deja de tener el éxito inicial.
8. Adicionalmente comienzan a promover aún más la restauración de datos.

CONCLUSIÓN

Actualmente hay estudios como el de Maxat Akbanov y colaboradores que simulan a partir de entornos de pruebas el comportamiento de cada variante de WannaCry y como es su diseminación en un entorno controlado. Mientras que, hay pocos estudios que busquen modelar la dinámica poblacional del brote (como Alesia Chernikova y colaboradores) la pertinencia de aprovechar la plasticidad de estas simulaciones para determinar el comportamiento de brotes y poder extrapolarlo a poblaciones biológicas es clara, por lo que este proyecto sienta las bases para empezar a estudiar brotes informáticos desde una perspectiva biológica.

BIBLIOGRAFIA

- Chen, Q., & Bridges, R. A. (2017, December). Automated behavioral analysis of malware: A case study of wannacry ransomware. In 2017 16th IEEE International Conference on machine learning and applications (ICMLA) (pp. 454-460). IEEE.
- Kao, D. Y., & Hsiao, S. C. (2018, February). The dynamic analysis of WannaCry ransomware. In 2018 20th International conference on advanced communication technology (ICACT) (pp. 159-166). IEEE.
- Chernikova, A., Gozzi, N., Perra, N., Boboila, S., Eliassi-Rad, T., & Oprea, A. (2023). Modeling self-propagating malware with epidemiological models. *Applied Network Science*, 8(1), 52.
- Levén, E., & Segerstedt, A. (2004). Inventory control with a modified Croston procedure and Erlang distribution. *International journal of production economics*, 90(3), 361-367.