

ANEXO N°3

Transmisión de información

Taxonomía de TLP

El CSIRT estableció el protocolo TLP (Traffic Light protocol) para la transmisión de la información entre las organizaciones de seguridad cibernética. Este protocolo es especialmente importante en el manejo de incidentes, al momento de compartir información. Los siguientes son las cuatro clasificaciones utilizadas en los diferentes reportes.

a) TLP Blanco

La información puede ser distribuida sin restricciones. La información no supone ningún riesgo de mal uso, dentro de las reglas y procedimientos establecidos para su difusión pública.

b) TLP Verde

Los receptores pueden compartir información con sus pares y organizaciones asociadas dentro de su sector o comunidad, pero no a través de canales de acceso público. La información en esta categoría puede circular ampliamente dentro de una comunidad en particular. Se asume que la información es útil para todas las organizaciones que participan dentro de un sistema, así como con terceros de la comunidad o el sector.

c) TLP Ámbar

Los receptores pueden compartir esta información solo con miembros de su propia organización que necesitan conocerla, y con clientes, proveedores o asociados que necesitan conocerla para protegerse a sí mismos o evitar daños. Esta información no se puede divulgar fuera de la unidad receptora. La información requiere ser distribuida de forma limitada porque supone un riesgo para la privacidad, reputación u operaciones si es compartida fuera de la organización.

d) TLP Rojo

Solo los receptores están autorizados para utilizar la información. No se puede divulgar a terceros. La información está limitada a personas concretas, y podría tener impacto en la privacidad, reputación u operaciones si es mal utilizada.

Link de interés: <https://www.cisa.gov/tlp>