

Protocolo de Luces de Semáforo - Traffic Light Protocol (TLP)

Version 2.0

Definiciones y guías de uso de los estándares FIRST

1.Introducción

- A. El Protocolo de Luces de Semáforo (*"Traffic Light Protocol"* o TLP) se creó para fomentar un mayor intercambio de información potencialmente sensible y una colaboración más eficaz. El intercambio de información se produce desde una fuente de información hacia uno o varios destinatarios. TLP es un conjunto de cuatro etiquetas utilizadas para indicar los límites del intercambio que deben respetar los destinatarios. Únicamente las etiquetas enumeradas en este estándar son válidas para el FIRST.
- B. Las cuatro etiquetas TLP son: TLP:RED, TLP:AMBER, TLP:GREEN y TLP:CLEAR. En su forma escrita, NO DEBEN contener espacios y DEBERÍAN ir en mayúsculas. Las etiquetas TLP DEBEN mantener su formato original, aunque se utilicen en otros idiomas: el contenido puede ser traducido, pero las etiquetas no.
- C. TLP proporciona un esquema sencillo e intuitivo para indicar con quién se puede compartir información potencialmente confidencial. TLP no es un esquema de clasificación formal. TLP tampoco se diseñó para gestionar términos de licencia, ni el tratamiento de la información o las reglas de cifrado. Las etiquetas TLP y sus definiciones no pretenden tener ningún efecto sobre la libertad de información o las leyes de transparencia de ninguna jurisdicción.
- D. TLP está optimizado para facilitar tanto su adopción, como su lectura por humanos, así como el intercambio de información entre personas; también puede usarse en sistemas automatizados de intercambio de información, como [MISP](#) o [IEP](#).

- E. TLP es diferente de la regla de [Chatham House](#), pero puede utilizarse combinado con ésta cuando proceda. Cuando una reunión se celebra bajo la regla de Chatham House, los participantes tienen el derecho de utilizar la información que reciben, pero no se puede revelar ni la identidad ni la afiliación del orador, ni de ningún otro participante.
- F. La fuente es responsable de garantizar que los destinatarios de la información etiquetada con TLP comprendan y puedan seguir las directrices de intercambio de información TLP.**
- G. La fuente es libre de especificar restricciones adicionales para el intercambio. Estas deben ser respetadas por los destinatarios.**
- H. Si un destinatario necesita compartir información más ampliamente de lo permitido por la etiqueta TLP original bajo el que la recibió, DEBE obtener explícitamente de la fuente un permiso adicional para el uso no cubierto que desee darle.**

2.Uso

- A. Cómo utilizar TLP en mensajería (como el correo electrónico y la mensajería instantánea)**

Los mensajes etiquetados mediante TLP DEBEN indicar la etiqueta TLP concreta de la información, así como cualquier restricción adicional, inmediatamente antes de la propia información. En los correos electrónicos la etiqueta TLP DEBERÍA incluirse en el asunto. Cuando corresponda también deberá indicarse el final del texto al que se aplica la etiqueta TLP.

- B. Cómo utilizar TLP en documentos**

Los documentos con etiqueta TLP DEBEN indicar la etiqueta TLP de la información, así como cualquier restricción adicional, en el encabezado y pie de cada página. La etiqueta TLP DEBERÍA tener un tamaño de fuente de 12 puntos o superior para los usuarios con visión reducida. Se recomienda situar las etiquetas TLP justificadas a la derecha.

- C. Cómo utilizar TLP en los sistemas de intercambio automatizado de información**

El uso de TLP en los sistemas de intercambio automatizado de información no tiene una definición concreta: se deja abierto a los diseñadores de estos sistemas de intercambio, pero DEBE hacerse siempre conforme a este estándar.

D. Codificación de colores TLP en RGB, CMYK y Hexadecimal

	Fuente RGB:			Fondo RGB:			Fuente CMYK:				Fondo CMYK:				Fuente Hexadecimal:	Fondo Hexadecimal:
	R	G	B	R	G	B	C	M	Y	K	C	M	Y	K		
TLP:RED	255	43	43	0	0	0	0	83	83	0	0	0	0	100	#FF2B2B	#000000
TLP:AMBER	255	192	0	0	0	0	0	25	100	0	0	0	0	100	#FFC000	#000000
TLP:GREEN	51	255	0	0	0	0	79	0	100	0	0	0	0	100	#33FF00	#000000
TLP:CLEAR	255	255	255	0	0	0	0	0	0	0	0	0	0	100	#FFFFFF	#000000

Nota sobre la codificación de colores: cuando hay muy poco contraste de color entre el texto y el fondo, las personas con visión reducida tienen dificultades para leer el texto o podrían no verlo en absoluto. TLP está diseñado para adaptarse a las personas con visión reducida. Las fuentes DEBERÍAN adherirse a la codificación de colores TLP para garantizar un contraste de colores suficiente para dichos lectores.

3. Definiciones TLP

Comunidad: en el contexto de TLP, una comunidad es un grupo que comparte objetivos, prácticas y relaciones informales de confianza. Una comunidad puede ser tan amplia como todos los profesionales de ciberseguridad de un país (o de un sector o de una región).

Organización: en el contexto de TLP, una organización es un grupo que comparte una afiliación común por membresía formal y está sujeto a unas políticas comunes establecidas por la organización. Una organización puede ser tan amplia como todos los miembros de una organización de intercambio de información, pero rara vez será más amplia.

Clientes: en el contexto de TLP, los clientes son aquellas personas o entidades que reciben servicios de ciberseguridad de una organización. Los clientes están incluidos por defecto en TLP:AMBER para que los destinatarios puedan también compartir la información a sus propios clientes (y así sucesivamente), con el fin de que los clientes tomen medidas para protegerse. Para los equipos con responsabilidad nacional, esta definición incluirá a las partes interesadas y a los miembros de su comunidad o constituyentes.

- A. **TLP:RED** = Únicamente para los ojos y oídos de los destinatarios *individuales*, sin que sea posible más divulgación. Las fuentes pueden utilizar TLP:RED cuando la información no pueda ser utilizada eficazmente sin un riesgo significativo para la privacidad, la reputación o las operaciones de las organizaciones implicadas. Por lo tanto, los destinatarios no podrán compartir la información TLP:RED con nadie más. En el contexto de una reunión, por ejemplo, la información TLP:RED se limitará a los presentes en la reunión.
- B. **TLP:AMBER** = Divulgación limitada, los destinatarios solamente podrán difundir esta información en base a la necesidad de conocer dentro de su *organización* y con sus *clientes*. La opción **TLP:AMBER+STRICT** limita la posibilidad de intercambio únicamente a la *organización*. Las fuentes pueden utilizar TLP:AMBER cuando la información requiera asistencia para poder ser utilizada con eficacia, pero conlleve riesgos para la privacidad, la reputación o las operaciones si se compartiese fuera de las organizaciones involucradas. Los destinatarios podrán compartir la información TLP:AMBER con los miembros de su propia organización y sus clientes, pero únicamente cuando sea necesario en base a la necesidad de conocer para proteger a su organización y sus clientes y evitar daños mayores. Nota: si la fuente desea limitar el intercambio **solo a la organización**, deberá utilizar TLP:AMBER+STRICT.
- C. **TLP:GREEN** = Divulgación limitada, los destinatarios pueden difundirla dentro de su comunidad. Las fuentes pueden utilizar TLP:GREEN cuando la información sea útil para aumentar la concienciación dentro de su comunidad más amplia. Los destinatarios podrán compartir la información TLP:GREEN con sus iguales y con organizaciones asociadas dentro de su comunidad, pero no a través de canales de acceso público. La información TLP:GREEN no podrá compartirse fuera de la comunidad. Nota: cuando no se defina «comunidad», se entenderá por comunidad la comunidad de ciberseguridad/defensa.
- D. **TLP:CLEAR** = Los destinatarios podrán difundirla a todo el *mundo*, no hay límite alguno a su divulgación. Las fuentes pueden utilizar TLP:CLEAR cuando la información conlleve un riesgo mínimo o nulo de uso indebido, de conformidad con las normas y procedimientos aplicables a la divulgación pública. Sujeta a las normas habituales sobre derechos de autor, la información de TLP:CLEAR puede compartirse sin restricciones.

Observaciones:

1. El presente documento utiliza los términos NO DEBE (MUST NOT), DEBE (MUST) y DEBERÍA (SHOULD) con el sentido definido en el [RFC 2119](#).
2. Los comentarios o sugerencias sobre este documento pueden enviarse a tlp-sig@first.org.

Translation: Javier Fernández-Sanguino, Banco de España-CSIRT, ES
Jose Luis Otones, Banco de España-CSIRT, ES
Oscar Fabián Prieto González, Indra-CSIRT, CO
Ángel González, INCIBE-CERT, ES

Reviewers: Javier Fernández-Sanguino, Banco de España-CSIRT, ES
Ángel González, INCIBE-CERT, ES
Ruben Olague, Grupo Santander, ES
José Vila, Generalitat Valenciana, ES