



TRAFFIC LIGHT PROTOCOL (TLP)

Guia de Uso e Definições do Padrão do FIRST

1. Introdução

- a. O Traffic Light Protocol (TLP) foi criado para facilitar o compartilhamento mais amplo de informações potencialmente sensíveis e a colaboração mais efetiva. O compartilhamento de informações ocorre a partir de uma fonte em direção a um ou mais destinatários. O TLP é um conjunto de quatro marcações (labels) usadas para indicar os limites de compartilhamento a serem aplicados pelos destinatários. Somente as marcações listadas neste padrão são consideradas válidas pelo FIRST.
- b. As quatro marcações do TLP são: TLP:RED, TLP:AMBER, TLP:GREEN e TLP:CLEAR. Em sua forma escrita elas NUNCA DEVEM (MUST) conter espaços e DEVEM (SHOULD) ser em letras maiúsculas. As marcações TLP DEVEM OBRIGATORIAMENTE (MUST) permanecer em sua forma original mesmo quando usadas em outros idiomas: o conteúdo pode ser traduzido, mas as marcações não devem ser traduzidas.
- c. O TLP provê um esquema simples e intuitivo para indicar com quem informações potencialmente sensíveis podem ser compartilhadas. O TLP não é um esquema formal de classificação. O TLP não foi projetado para tratar termos de licenciamento, nem regras de criptografia ou de tratamento de informações. As marcações TLP e suas definições não têm intenção de ter qualquer efeito sobre a liberdade de acesso à informação ou leis de transparência ("sunshine" laws) em qualquer jurisdição.
- d. O TLP é otimizado para fácil adoção, facilidade de leitura e compartilhamento entre pessoas; ele pode ser utilizado em sistemas automatizados de troca de informações, como MISP e IEP.
- e. O TLP é diferente da regra de "Chatham House", mas pode ser usado em conjunto quando apropriado. Quando uma reunião é conduzida sob as regras de "Chatham House" os participantes são livres para usar a informação recebida, mas nem a identidade nem a afiliação do(s) orador(es) ou de quaisquer outros participantes pode ser revelada.
- f. A fonte é responsável por garantir que os destinatários de uma informação marcada com TLP compreendam e possam seguir as orientações de compartilhamento.
- g. A fonte tem liberdade para especificar restrições adicionais de compartilhamento. Estas restrições devem ser respeitadas pelos destinatários.





h. Se um destinatário necessitar compartilhar uma informação mais amplamente do que o indicado pela marcação TLP que veio na informação, ele deve obrigatoriamente (must) obter permissão explícita da fonte.

2. Uso

a. Como usar TLP em mensagens (como *email* e *chat*)

Mensagens com marcação TLP DEVEM OBRIGATORIAMENTE (MUST) indicar a marcação TLP da informação, bem como quaisquer restrições adicionais, imediatamente antes da informação em si. A marcação TLP DEVE (SHOULD) estar na linha de assunto (subject) do email. Quando necessário, também garanta que o final do texto ao qual a marcação TLP se aplica está indicado.

b. Como usar TLP em documentos

Documentos com marcação TLP DEVEM OBRIGATORIAMENTE (MUST) indicar a marcação TLP da informação, bem como qualquer restrição adicional, no cabeçalho e no rodapé de cada página. A marcação TLP DEVE (SHOULD) ser em fonte tamanho 12 ou maior, por conta de usuários com baixa visão. É recomendável alinhar as marcações TLP à direita.

c. Como usar TLP em trocas automatizadas de informações

O uso de TLP em trocas automatizadas de informações não é definido: isto é deixado para aqueles que projetam tais trocas, mas DEVE OBRIGATORIAMENTE (MUST) ser de acordo com este padrão.

d. Código de cores para o TLP em RGB, CMYK e Hex

	RGB: font			RGB: background			CMYK: font				CMYK: background				Hex:	Hex:
	R	G	В	R	G	В	С	М	Υ	K	С	М	Υ	K	TOTIL	background
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 o código de cores: quando existe muito pouco contraste de cores entre o texto e o fundo, aqueles com baixa visão tem muita dificuldade de ler o texto ou nem conseguem enxergá-lo. O TLP é projetado para atender as necessidades daqueles com baixa visão. As fontes DEVEM (SHOULD) aderir ao código de cores do TLP para garantir contraste suficiente para estes leitores.







3. Definições do TLP

Comunidade: Sob o TLP, uma comunidade é um grupo que compartilha objetivos, práticas e relacionamentos informais de confiança. Uma comunidade pode ser tão ampla quanto todos os profissionais de segurança cibernética em um país (ou em um setor ou região).

Organização: Sob o TLP, uma organização é um grupo que compartilha uma mesma afiliação através de um processo formal de filiação e que está sujeito a um conjunto de políticas em comum definidas pela organização. Uma organização pode ser tão ampla quanto todos os membros de uma organização para compartilhamento de informações, mas raramente mais ampla que isso.

Clientes: Sob o TLP, clientes são as pessoas ou entidades que recebem serviços de segurança cibernética de uma organização. Clientes são incluídos por padrão no TLP:AMBER, de modo que os destinatários possam compartilhar informações adiante, permitindo que os clientes possam tomar ações para se proteger. Para times com responsabilidade nacional esta definição inclui as partes interessadas (stakeholders) e o público-alvo (constituents).

- **TLP:RED** = Somente para os olhos e ouvidos dos <u>indivíduos</u> destinatários, não é permitido compartilhamento nenhum. Fontes podem usar TLP:RED quando não é possível atuar sobre a informação sem colocar em risco significativo a privacidade, reputação ou operações das organizações envolvidas. Destinatários não podem compartilhar informações TLP:RED com mais ninguém. No contexto de uma reunião, por exemplo, informações TLP:RED são limitadas àqueles presentes na reunião.
- b. **TLP:AMBER** = Divulgação limitada, destinatários só podem disseminar para aqueles que necessitam saber (need-to-know basis) dentro de sua própria organização e com seus clientes. Note que o TLP:AMBER+STRICT restringe o compartilhamento apenas para a própria organização. Fontes podem usar o TLP:AMBER quando é necessário apoio para agir de maneira efetiva sobre a informação, mas ainda assim há riscos para a privacidade, reputação ou operações das organizações envolvidas. Destinatários podem compartilhar TLP:AMBER com membros de sua própria organização e com seus clientes, mas somente com aqueles que necessitam saber da informação (need-to-know basis) para proteger sua organização e seus clientes e evitar danos continuados. Nota: se a fonte quiser restringir o compartilhamento somente para a organização ela deve especificar TLP:AMBER+STRICT.
- c. TLP:GREEN = Divulgação limitada, destinatários podem divulgar dentro de sua comunidade. Fontes podem usar TLP:GREEN quando a informação é útil para a conscientização dentro de sua comunidade mais ampla. Destinatários podem compartilhar informações TLP:GREEN com seus pares e organizações parceiras dentro de sua comunidade, mas não por meio de canais publicamente acessíveis. Informações TLP:GREEN não podem ser compartilhadas fora de uma comunidade. Nota: quando a "comunidade" não estiver definida, assume-se que é a comunidade de segurança/defesa cibernética.
- d. **TLP:CLEAR** = Destinatários podem disseminar para o mundo, não há limites na divulgação. Fontes podem usar TLP:CLEAR quando há um risco mínimo ou não há previsão de risco de mau uso da informação, de acordo com regras e procedimentos aplicáveis para divulgação pública. Desde que respeitadas as regras padrão de direitos autorais, as informações TLP:CLEAR podem ser compartilhadas sem restrições.



TLP:CLEAR

Notas:

1. Este documento usa DEVE OBRIGATORIAMENTE (MUST) e DEVE (SHOULD) conforme definido pela <u>RFC-2119</u>.

2. Comentários ou sugestões sobre este documento podem ser enviadas (em inglês) para tlpsig@first.org.

Translation: Cristine Hoepers, CERT.br/NIC.br, BR

Review: Edilson Lima, Emilio Nakamura, CAIS/RNP, BR

Marcos Vinicio Rabello da Silva, Kildane de Souza Castro, CSIRT PETROBRAS, BR

Klaus Steding-Jessen, Miriam von Zuben, CERT.br/NIC.br, BR