01 | Objetivo

O objetivo deste documento é definir a utilização do mecanismo TLP nos documentos e publicações da ESCO e seus membros.

02 | Procedimento

2.1 Âmbito

- Portais Institucionais e plataformas de backoffice de apoio aos processos da atividade;
- Site e plataformas web;
- Documentos da ESCO e e-mail;

2.2 Guia de Uso e Definições

A proteção e divulgação da informação sensível devem seguir princípios de segurança da informação que possam ser usados de uma forma responsável e intuitiva. Nesse sentido, a ESCO respeita o Traffic Light Protocol (TLP), designadamente o FIRST Standards Definitions and Usage Guidance — Version 2.0 enquanto norma orientadora para a classificação da informação no âmbito da sua missão de CSIRT.

O TLP providencia um esquema fácil para indicar quando (Proteção) e como (Disseminação) a informação pode ser partilhada com a comunidade de cibersegurança a nível nacional e internacional. Este protocolo adota um esquema de cores (semáforo) para indicar os diferentes níveis de sensibilidade e ações expectáveis, que devem ser obrigatoriamente respeitadas no manuseamento da informação.

O TLP define um quadro de classificação de informação imprescindível para a confiança entre pares, baseado no compromisso de respeito pelas suas regras por todos os intervenientes.

É por isso basilar na forma como a comunidade de cibersegurança comunica, partilha e atua na proteção das redes e sistemas de informação.

A fonte é responsável por garantir que os destinatários da informação TLP compreendam as normas de partilha do TLP para que possam segui-las.

Se um destinatário necessitar partilhar uma informação para além do que a classificação TLP original permite, deve obrigatoriamente obter permissão explicita da fonte original.

Mais informações sobre o protocolo TLP: https://www.first.org/tlp/

2.3 Destinatários

- Trabalhadores docentes internos e externos;
- Trabalhadores não docentes internos e externos;
- Outras pessoas com vínculo temporário com a ESCO;
- Utilizadores nacionais ou internacionais credenciados na ESCO.

2.4 Traffic Light Protocol

O TLP foi criado para facilitar a partilha de informações usando um conjunto de designações para garantir que informações sensíveis sejam compartilhadas com o público apropriado.

Emprega quatro cores para indicar os limites de partilha. Podemos usar TLP no email, documentos e para cada tipo de uso existem as recomendações indicadas.

Classificação da Informação	Proteção da Informação (Quando usar?)	Disseminação da Informação (Como partilhar?)	Observações
TLP:RED Não deve ser divulgado, restrito somente aos participantes.	Quando a informação é muito sensível e terceiros não podem agir de forma eficaz sobre a informação. Qualquer mau uso da informação pode causar impactos na privacidade, reputação ou operações de uma das partes.	Os destinatários não podem partilhar a informação com mais ninguém para além dos destinatários especificados no contexto da partilha (conversa, reunião, etc..). Preferencialmente, a informação deve ser partilhada verbalmente ou pessoalmente.	Estes limites devem obrigatoriamente ser respeitados. O não respeito por esta classificação resulta, para além de graves danos em terceiros, numa quebra de confiança entre as partes.
TLP:AMBER Divulgação limitada, restrita às organizações dos participantes.	Quando é necessário apoio para agir de forma eficaz sobre a informação, mas ainda assim há riscos para a privacidade, reputação ou operações se esta for divulgada fora das organizações envolvidas. Apenas as fontes podem especificar limites adicionais para a partilha (para isso devem ser contactados).	Os destinatários só podem partilhar informações **TLP:AMBER** com membros da organização e os seus clientes num regime de need-to-know-basis. **Nota: TLP:AMBER+STRICT** restringe a partilha apenas para a própria organização.	Estes limites devem obrigatoriamente ser respeitados. O não respeito resulta, para além dos danos em terceiros, numa quebra de confiança entre as partes.
TLP:GREEN Divulgação limitada, restrito à comunidade.	Quando a partilha da informação é útil para a sensibilização de todas as entidades e pontos de contacto da comunidade ou setor.	Informação **TLP:GREEN** não pode ser divulgada fora de uma comunidade. Os destinatários podem partilhar a informação com membros da própria organização, parceiros e pontos de contacto da comunidade e setor, mas nunca através de canais públicos ou para o público em geral.	Estes limites devem obrigatoriamente ser respeitados. O não respeito por esta classificação resulta, para além de possíveis danos em terceiros, numa quebra da confiança entre as partes.
TLP:CLEAR Divulgação não é limitada	Quando a partilha da informação implica pouco ou nenhum risco, de acordo com as regras e procedimentos aplicados na divulgação de informação pública.	A partilha da informação não tem qualquer restrição, embora sujeita a direitos de autor.	

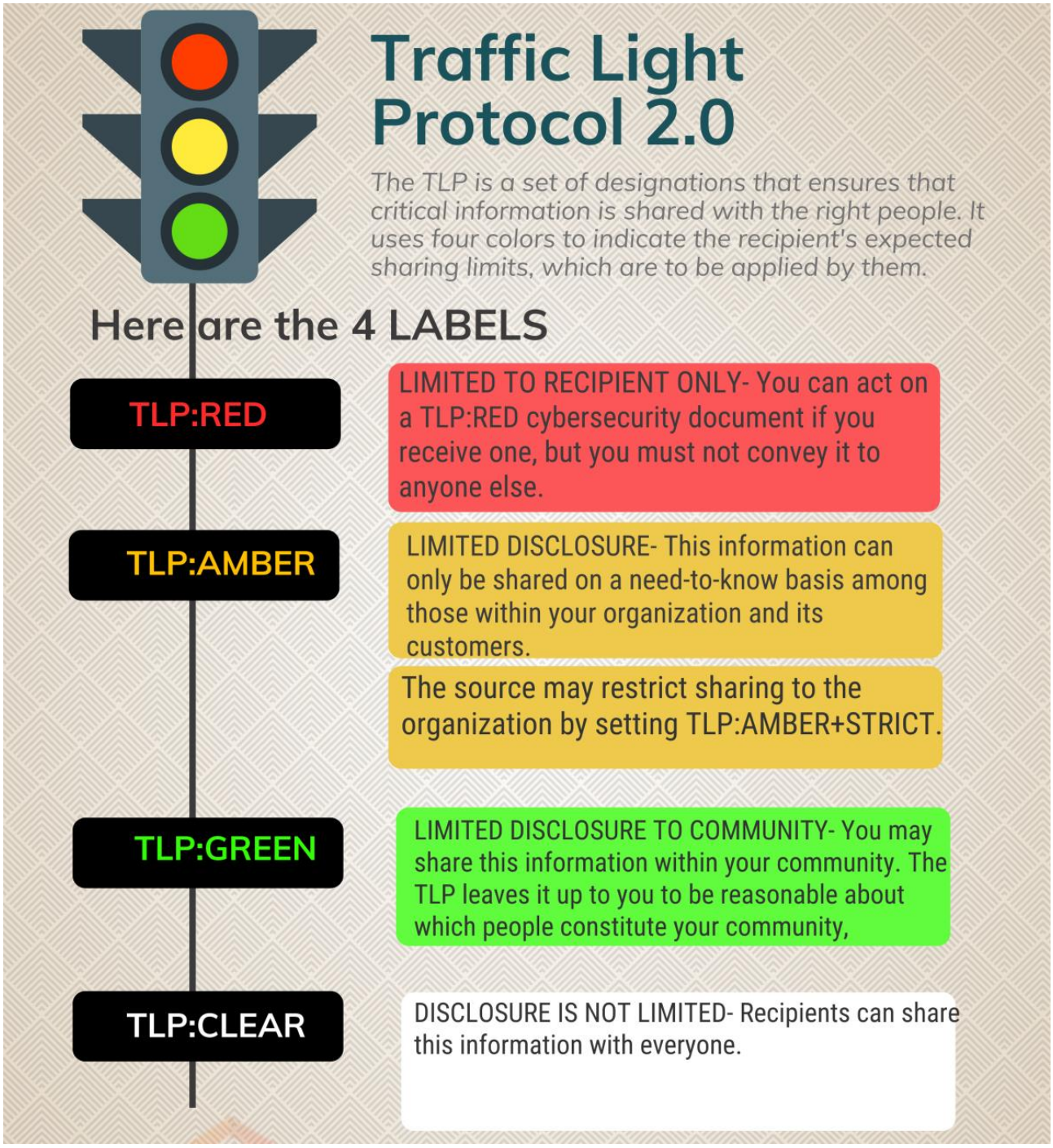
Por defeito, à falta da classificação da informação, consideramos todos os documentos como **TLP:CLEAR**.

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

Organização: Sob o TLP, uma organização é um grupo que partilha 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 partilha 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 a que os destinatários possam partilhar informações adiante, permitindo que os clientes possam tomar ações para se proteger. Para equipas com responsabilidade nacional esta definição inclui as partes interessadas (stakeholders) e o público-alvo (constituents).

FIRST TRAFFIC LIGHT PROTOCOL (TLP) Version 2.0	TLP: WHITE	TLP: GREEN	TLP: AMBER	TLP: AMBER+STRICT	TLP: RED
May be shared with those with a need-to-know within a formal organization of which the recipient is a member (company, ISAC, …)	✓	✓	✓	✓	✗
May be shared with those with a need-to-know in organizations to which the recipient provides cybersecurity services	✓	✓	✓	✗	✗
May be shared with members of wider security community	✓	✓	✗	✗	✗
May be shared without limits	✓	✗	✗	✗	✗



03 | Termos e definições

- CSIRT – Computer Security Incident Response Team - Resposta a incidentes de segurança informática
- ESCO – Escola de Serviços e Comércio do Oeste
- TLP - Traffic Light Protocol