nic.br cgi.br

cert.br

LAC-CSIRTs / LACNIC 38

October 5th, 2022

Santa Cruz de La Sierra, BO

Computer Emergency Response Team Brazil

National CSIRT of Last Resort

Services Provided to the Community

Incident Management

- Coordination
- Technical Analysis
- Mitigation and Recovery Support

Situational Awareness

- Data Acquisition
  - Distributed Honeypots
  - SpamPots
  - Threat feeds
- Information Sharing

Knowledge Transfer

- Awareness
  - Development of Best Practices
  - Outreach
- Training
- Technical and Policy Advisory

Affiliations and Partnerships:

SEI
Partner
Network

Creation:

August/1996: CGI.br publishes a report with a proposed model for incident management for the country[1]

June/1997: CGI.br creates CERT.br (at that time called NBSO – NIC BR Security Office) based on the report's recommendations[2]

[1] https://cert.br/sobre/estudo-cgibr-1996.html | [2] https://nic.br/pagina/gts/157

Mission

To increase the level of security and incident handling capacity of the networks connected to the Internet in Brazil.

Constituency

Any network that uses Internet Resources allocated by NIC.br

- IP addresses or ASNs allocated to Brazil
- domains under the ccTLD .br

Governance

Maintained by **NIC.br** – The Brazilian Network Information Center

- all activities are funded by .br domain registration

NIC.br is the **executive branch of CGI.br** – The Brazilian Internet Steering Committee

- a multistakeholder organization
- with the purpose of coordinating and integrating all Internet service initiatives in Brazil

https://cert.br/about/
https://cert.br/sobre/filiacoes/
https://cert.br/about/rfc2350/

TLP 2.0
What's New in the Standard and How it Impacts Incident Handling and Threat Information Sharing

Dr. Cristine Hoepers

General Manager

cristine@cert.br

cert.br nic.br cgi.br

TLP:CLEAR

Security Teams, CSIRTs and PSIRTs: **Evolution and Challenges**

A growing community

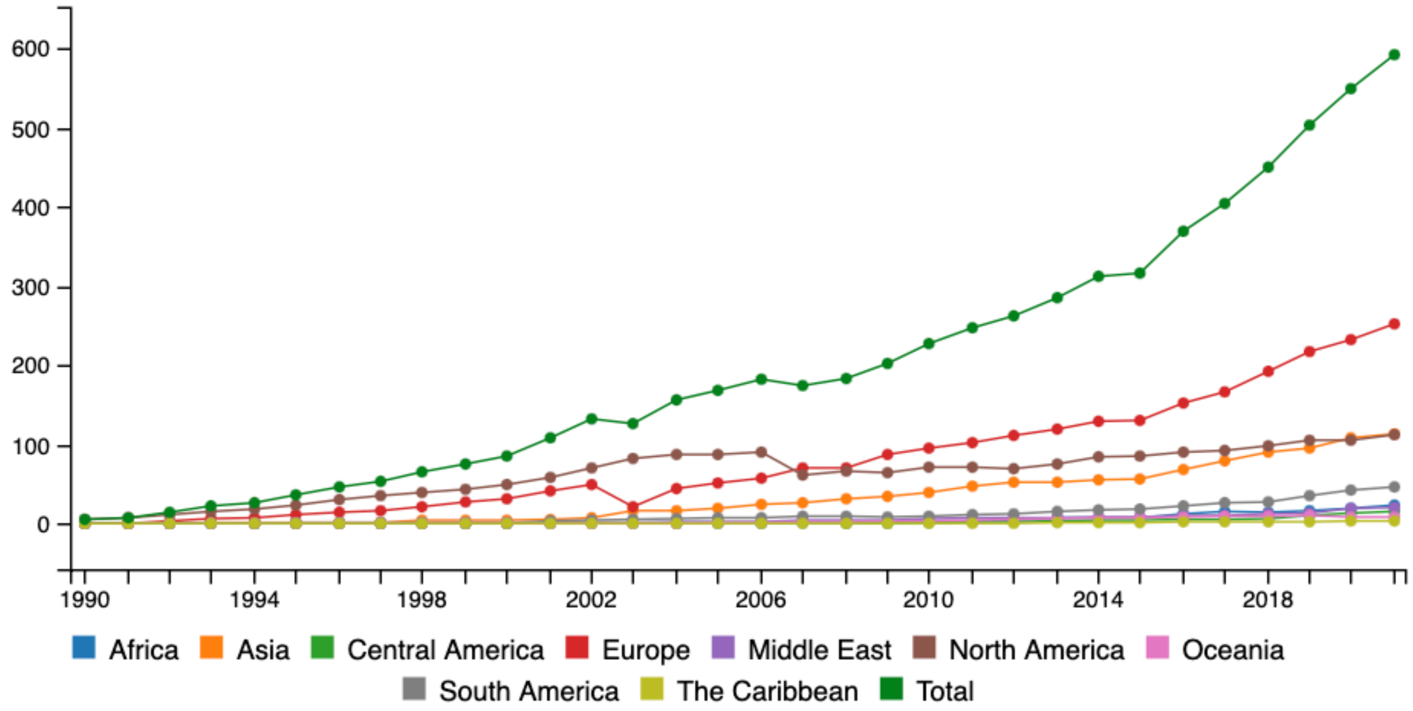
- Several countries
- Diverse sectors
- Different levels of maturity

<u>Trust</u> is key for cooperation

Challenges

- How to appropriately communicate the expectation of confidentiality?
- How to overcome language barriers?
- How to facilitate and encourage information sharing?

FIRST members growth by year*



(*) The statistic measurement method and regional breakdown changed in 2007.

Source: FIRST History, last visited on September 17, 2022
https://www.first.org/about/history

CSIRT/PSIRT Community Standards

Who is involved

- FIRST – Forum of Incident Response and Security Teams
  - SIGs (Special Interest Groups)
- ENISA – European Union Agency for Cybersecurity
- GFCE – Global Forum on Cyber Expertise
- Open CSIRT Foundation
  - TF-CSIRT Trusted Introducer

Standards

- FIRST:
  - CVSS (*Common Vulnerability Scoring System*)
  - **TLP (*Traffic Light Protocol*)**
  - CSIRT *Services Framework*
  - PSIRT *Services Framework*
  - IEP (*Information Exchange Policy*)
  - Passive DNS
  - EPSS (*Exploit Prediction Scoring System*)
- *Open* CSIRT *Foundation*
  - SIM3 (*Security Incident Management Maturity Model*)

Traffic Light Protocol 2.0

cert.br nic.br cgi.br

FIRST Standard:
Traffic Light Protocol (TLP)

What is TLP?

- a set of **labels**
- 4 colors to indicate the **sharing boundaries**
- optimized for ease of adoption, **human readability** and **person-to-person sharing**

Why?

- a simple and intuitive schema
- to facilitate greater sharing of potentially sensitive information and more effective collaboration

Where to use it?

- documents, *e-mails*, *slides*, incident notifications
- information sharing platforms, e.g. MISP
- any other place (ex: conferences and meetings)

TLP:RED
cert.br/tlp/
TLP:AMBER
cert.br/tlp/
TLP:GREEN
cert.br/tlp/
TLP:CLEAR
cert.br/tlp/

https://www.first.org/tlp/ | https://cert.br/tlp/

TLP 2.0: **Why a new version?**

Language improvements

- use the same terms consistently (instead of synonyms)
- less colloquialisms in order to facilitate translations
- clarify the text about sharing boundaries, for example:
  - TLP:RED is for **eyes and ears of individuals** - cannot be used to protect an organization
  - TLP:AMBER and TLP:AMBER+STRICT must be shared on a **need to know basis** only

New content

- definition of terms
  - community, organization and clients
- TLP:AMBER+STRICT
- TLP:WHITE ➡ TLP:CLEAR
- color accessibility improvements
- color table with RGB, CMYK and Hexadecimal

TLP:CLEAR

Definitions:
Community, Organization and Clients

Community: Under TLP, a community is **a group who share common goals, practices, and informal trust relationships.** A community can be as broad as all cybersecurity practitioners in a country (or in a sector or region).

Organization: Under TLP, an organization **is a group who share a common affiliation by formal membership and are bound by common policies set by the organization**. An organization can be as broad as all members of an information sharing organization, but rarely broader.

Clients: Under TLP, clients are those **people or entities that receive cybersecurity services from an *organization***. Clients are **by default included in TLP:AMBER** so that the recipients may share information further downstream in order for clients to take action to protect themselves. For teams with national responsibility this definition includes stakeholders and constituents.

https://www.first.org/tlp/ | https://cert.br/tlp/

TLP:CLEAR

THERE IS NO LIMIT ON DISCLOSURE

https://cert.br/tlp/

TLP:RED

NO FURTHER DISCLOSURE

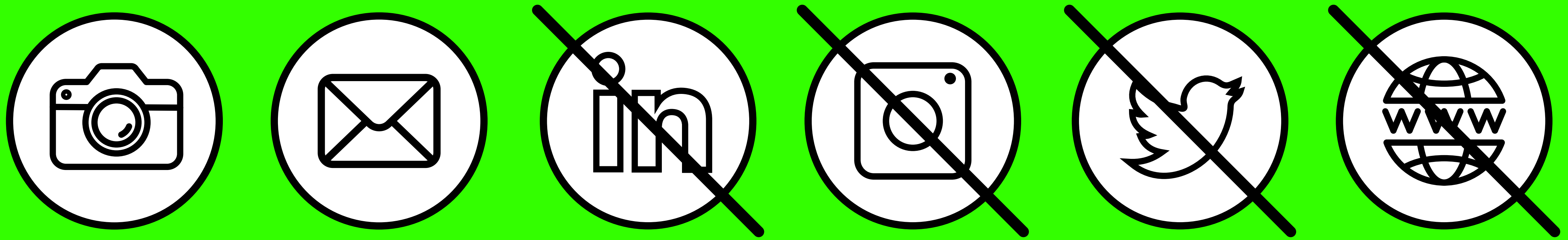
- FOR THE **EYES AND EARS** OF **INDIVIDUAL RECIPIENTS** ONLY

https://cert.br/tlp/

TLP:GREEN

LIMITED DISCLOSURE

- CAN SHARE WITHIN YOUR COMMUNITY
- BUT NOT VIA PUBLICLY ACCESSIBLE CHANNELS



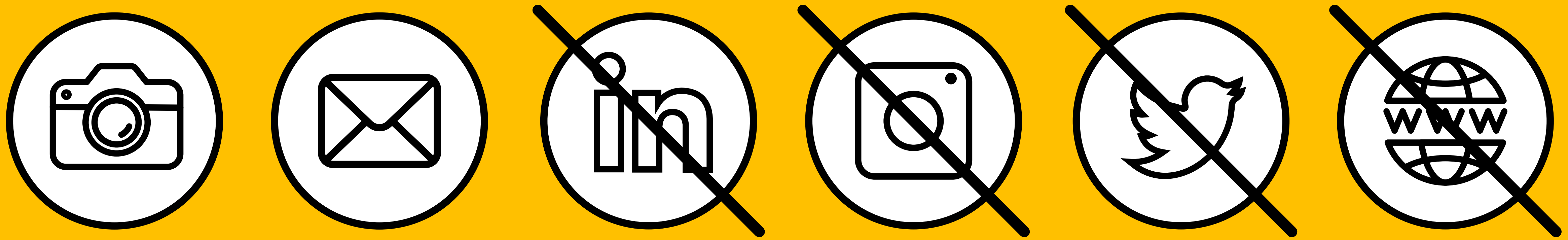
https://cert.br/tlp/

TLP:AMBER

LIMITED DISCLOSURE, **NEED TO KNOW** BASIS

- WITHIN YOUR ORGANIZATION
- WITH YOUR CLIENTS

⚠ **IF SHARING** CONSIDER CHANGING TO **TLP:AMBER+STRICT**

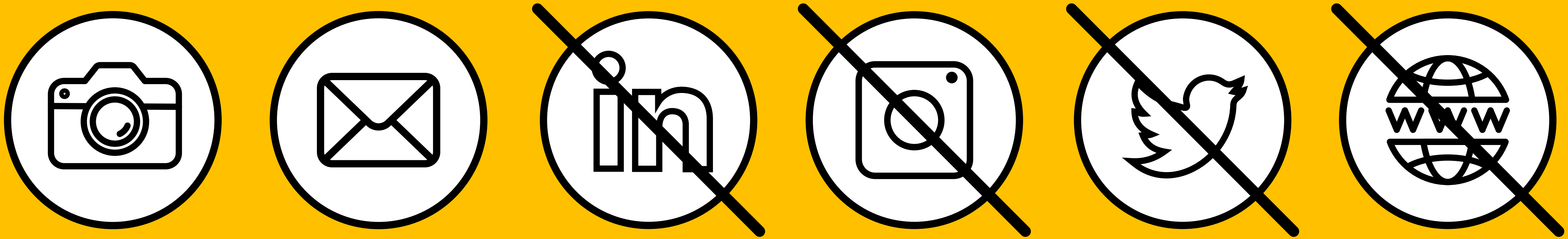


https://cert.br/tlp/

TLP:AMBER+STRICT

LIMITED DISCLOSURE, **NEED TO KNOW** BASIS

- WITHIN **YOUR ORGANIZATION ONLY**
- **DO NOT** SHARE
  WITH CLIENTS OR CONSTITUENCY



https://cert.br/tlp/

TLP	When should it be used?	How can it be shared?
TLP:RED **For the eyes and ears of individual recipients only, no further disclosure.**	Sources may use TLP:RED when information cannot be effectively acted upon without significant risk for the privacy, reputation, or operations of the organizations involved.	Recipients may therefore **not share TLP:RED information with anyone else**. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting..
TLP:AMBER **Limited disclosure, recipients can only spread this on a need-to-know basis within their organization and its clients.**	Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organizations involved.	Recipients **may share TLP:AMBER information with members of their own organization and its clients**, but only on a **need-to-know basis** to protect their organization and its clients and prevent further harm.
TLP:AMBER+STRICT **Limited disclosure, recipients can only spread this on a need-to-know basis within their organization only.**	Sources may use TLP:AMBER+STRICT when information requires support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organizations involved. **If the source wants to restrict sharing to the organization only, they must specify TLP:AMBER+STRICT.**	Recipients **may share TLP:AMBER+STRICT information with members of their own organization only**, but only on a **need-to-know basis** to protect their organization and its clients and prevent further harm.
TLP:GREEN **Limited disclosure, recipients can spread this within their community.**	Sources may use TLP:GREEN when information is useful to increase awareness within their wider community.	Recipients may share TLP:GREEN information with peers and partner organizations within their community, but not via publicly accessible channels. TLP:GREEN information may not be shared outside of the community. Note: when “community” is not defined, assume the cybersecurity/defense community.
TLP:CLEAR **Recipients can spread this to the world, there is no limit on disclosure.**	Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.	Recipients can spread this to the world, there is no limit on disclosure. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.

TLP:CLEAR

TLP SIG:
Next Steps

- **The community needs to adopt TLP 2.0 until January 2023!**
  - **Help to spread the word and to identify who needs to know about the change**
    - **tool developers, CSIRTs, threat sharing communities**
- The SIG will work on documenting “*use cases*”, for example
  - What can be shared with service providers and consulting services?
  - With whom a National or Sector CSIRT might share TLP:AMBER and TLP:AMBER+STRICT?
  - In which cases should a TLP:AMBER be changed to TLP:AMBER+STRICT when sharing with clients?
    - How to avoid TLP:AMBER becoming a TLP:GREEN in practice

Want to help?

- Join the SIG!

  https://www.first.org/global/sigs/tlp/

TLP:CLEAR

Traffic Light Protocol (TLP) Versão 2.0: **Official Translation to Brazilian Portuguese**

Translation

CERT.br/NIC.br

- Cristine Hoepers

Review

CAIS/RNP

- Edilson Lima
- Emilio Nakamura

CSIRT PETROBRAS

- Marcos Vinicio Rabello da Silva
- Kildane de Souza Castro

CERT.br/NIC.br

- Klaus Steding-Jessen
- Miriam von Zuben

TRAFFIC LIGHT PROTOCOL (TLP)

Guia de Uso e Definições do Padrã

1. Introdução

a. O *Traffic Light Protocol* (TLP) foi criado para facilitar o co
informações potencialmente sensíveis e a colaboração n
informações ocorre a partir de uma fonte em direção a
um conjunto de quatro marcações (*labels*) usadas para
compartilhamento a serem aplicados pelos destinatári
neste padrão são consideradas válidas pelo FIRST.

b. As quatro marcações do TLP são: TLP:RED, TLP:AMBE
forma escrita elas NUNCA DEVEM (MUST) conter esp
maiúsculas. As marcações TLP DEVEM OBRIGATORI
forma original mesmo quando usadas em outros id
mas as marcações não devem ser traduzidas.

c. O TLP provê um esquema simples e intuitivo para
potencialmente sensíveis podem ser compartilha
classificação. O TLP não foi projetado para tratar
criptografia ou de tratamento de informações. A
intenção de ter qualquer efeito sobre a liberdad
transparência (*"sunshine" laws*) em qualquer ju

d. O TLP é otimizado para fácil adoção, facilidade
ele pode ser utilizado em sistemas automatiz

e. O TLP é diferente da regra de "*Chatham Hou*
apropriado. Quando uma reunião é conduzi
participantes são livres para usar a informa
afiliação do(s) orador(es) ou de quaisquer

**f. A fonte é responsável por garantir que
com TLP compreendam e possam segu**

**g. A fonte tem liberdade para especifica
Estas restrições devem ser respeitad**

TRAFFIC LIGHT PROTOCOL (TLP) - Versão
https://www.first.org/tlp

Vers
TLP:

**h. Se um destinatário necessitar compartilhar uma informação mais amplament
o indicado pela marcação TLP que veio na informação, ele deve obrigatoriam
(*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 ma
informação, bem como quaisquer restrições adicionais, imediatamente antes da
si. A marcação TLP DEVE (*SHOULD*) estar na linha de assunto (*subject*) do *email*.
necessário, também garanta que o final do texto ao qual a marcação TLP se ap

b. Como usar TLP em documentos

Documentos com marcação TLP DEVEM OBRIGATORIAMENTE (*MUST*) indica
informação, bem como qualquer restrição adicional, no cabeçalho e no rod
marcação TLP DEVE (*SHOULD*) ser em **fonte tamanho 12 ou maior**, por co
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:
aqueles que projetam tais trocas, mas DEVE OBRIGATORIAMENTE (*MU*
padrão.

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

	RGB: font			RGB: background			CMYK: font				CMYK: backgr	
	R	G	B	R	G	B	C	M	Y	K	C	M
TLP:RED	255	43	43	0	0	0	0	83	83	0	0	
TLP:AMBER	255	192	0	0	0	0	0	25	100	0	0	
TLP:GREEN	51	255	0	0	0	0	79	0	100	0	0	
TLP:CLEAR	255	255	255	0	0	0	0	0	0	0		

Nota sobre o código de cores: quando existe muito pouco
fundo, aqueles com baixa visão tem muita dificuldade de
enxergá-lo. O TLP é projetado para atender as necessida
DEVEM (*SHOULD*) aderir ao código de cores do TLP para
leitores.

TRAFFIC LIGHT PROTOCOL (TLP) - Versão 2.0 (Trad
https://www.first.org/tlp

Versão 2.0
TLP:CLEAR

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*).

a. TLP:RED = Somente para os olhos e ouvidos dos indivíduos 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.

TRAFFIC LIGHT PROTOCOL (TLP) - Versão 2.0 (Tradução para Português Brasileiro) TLP:CLEAR
https://www.first.org/tlp
3 de 4

https://www.first.org/tlp/
https://www.first.org/tlp/docs/v2/tlp-pt-br.pdf

References

Standard

– TRAFFIC LIGHT PROTOCOL (TLP) *FIRST Standards Definitions and Usage Guidance — Version 2.0*
https://www.first.org/tlp/

– *Press Release: FIRST Releases Traffic Light Protocol Version 2.0 with important updates*
https://www.first.org/newsroom/releases/20220805

TLP 2.0 Launch at FIRST 2022

– *Traffic Light Protocol 2022: Updates for An Improved Sharing Experience*
Tom Millar (CISA, US), Don Stikvoort (Elsinore, NL), Ted Norminton (CCCS, CA)
FIRST Conference 2022, Duration: 1:07:09
https://youtu.be/2q8IFVOYRjM

CERT.br TLP References

– Use of TLP by CERT.br and links to references
https://cert.br/tlp/

Thank You

cristine@cert.br

Incident reports to: cert@cert.br

@certbr

https://cert.br/

25 anos cert.br

nic.br cgi.br

www.nic.br | www.cgi.br