nic.br cgi.br | cert.br

GTER 51 | GTS 37

24 de outubro de 2022

São Paulo / SP

TLP:CLEAR

cert.br

Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil

CERT Nacional de Último Recurso

Serviços Prestados à Comunidade

Gestão de Incidentes

- Coordenação
- Análise Técnica
- Suporte à Mitigação e Recuperação

Consciência Situacional

- Aquisição de Dados
  - *Honeypots* Distribuídos
  - SpamPots
  - *Threat feeds*
- Compartilhamento das Informações

Transferência de Conhecimento

- Conscientização
  - Desenvolvimento de Boas Práticas
  - Cooperação, Eventos e Reuniões (*Outreach*)
- Treinamento
- Aconselhamento Técnico e de Políticas

Filiações e Parcerias:

FIRST Improving Security Together MEMBER

ACCREDITED BY TI TRUSTED INTRODUCER

APWG RESEARCH PARTNER www.antiphishing.org

CARNEGIE MELLON UNIVERSITY SOFTWARE ENGINEERING INSTITUTE

SEI Partner Network

HN/P

Criação:

Agosto/1996: CGI.br publica o relatório "Rumo à Criação de uma Coordenadoria de Segurança de Redes na Internet Brasil"[1]

Junho/1997: CGI.br cria o CERT.br (à época chamado NBSO – *NIC BR Security Office*), com base nas recomendações do relatório[2]

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

Missão

Aumentar os níveis de segurança e de capacidade de tratamento de incidentes das redes conectadas à Internet no Brasil.

Público Alvo (*Constituency*)

Redes que utilizam recursos administrados pelo NIC.br

- endereços IP ou ASNs alocados ao Brasil
- domínios sob o ccTLD .br

Governança

Mantido pelo **NIC.br** – Núcleo de Informação e Coordenação do .br

- todas as atividades são sustentadas pelo registro de domínios .br

O NIC.br é o **braço executivo do CGI.br** – Comitê Gestor da Internet no Brasil

- entidade multissetorial
- responsável por coordenar e integrar as iniciativas e serviços da Internet no País

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

TLP 2.0: o que é e por que eu devo me preocupar com isso?

Dra. Cristine Hoepers
Gerente
cristine@cert.br

cert.br nic.br cgi.br

Profissionais de Segurança, CSIRTs e PSIRTs: **Evolução e Desafios**

TLP:CLEAR

Número crescente de profissionais e grupos focados em segurança

- Diversos países e setores
- Variados níveis de maturidade

Regulamentos setoriais de segurança cibernética tem cobrado cooperação e compartilhamento de informações

- Efetividade implica em compartilhar informações como
  - detalhes técnicos sobre ataques e incidentes
  - inteligência de ameaças (*cyber threat intelligence*)
- TLP já está sendo usado em alguns regulamentos

Confiança (*trust*) é pré-requisito para essa cooperação

- Como comunicar, de maneira simples, a expectativa de confidencialidade para um destinatário?

Padrões Construídos pela Comunidade

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*)

https://www.first.org/standards/

Open CSIRT *Foundation*

- SIM3 (*Security Incident Management Maturity Model*)

https://opencsirt.org/csirt-maturity/

Organizações envolvidas

- FIRST – *Forum of Incident Response and Security Teams*
- *Open* CSIRT *Foundation*
  - TF-CSIRT *Trusted Introducer*
- ENISA – *European Union Agency for Cybersecurity*
- GFCE – *Global Forum on Cyber Expertise*

Traffic Light Protocol 2.0

cert.br nic.br cgi.br

TLP:CLEAR

Traffic Light Protocol (TLP):
Troca e Compartilhamento de Dados e Informações

O que é?

– um conjunto de **marcações** (*labels*)
– 4 cores para indicar os **limites de compartilhamento**
– otimizado para **facilidade de adoção e leitura,** e para **trocas entre pessoas**

Por que?

– um esquema simples e intuitivo
– para facilitar a colaboração e um maior compartilhamento de informações potencialmente sensíveis

Onde usar?

– documentos, *e-mails*, *slides*, notificações
– plataformas de *cyber threat inteligence*, como MISP
– qualquer outro lugar (ex.: conferências e reuniões)

https://cert.br/tlp/

TLP:CLEAR

TLP 2.0:
Por que uma nova versão?

- Melhorar a linguagem
  - usar consistentemente os mesmos termos (ao invés de sinônimos)
  - deixar o texto menos coloquial para facilitar as traduções
  - explicitar melhor os limites de compartilhamento, por exemplo:
    - TLP:RED é para indivíduos - não pode usar para proteger a organização
    - TLP:AMBER e TLP:AMBER+STRICT são somente para “quem precisa saber” (*need to know basis*)
- Novo conteúdo
  - definição de termos
    - comunidade, organização e clientes
  - criação do TLP:AMBER+STRICT
  - TLP:WHITE ➡ TLP:CLEAR
  - melhorias na acessibilidade das cores e tabela com definições em RGB, CMYK e Hexadecimal

Obs.: Ficou em consulta pública de nov/2021 a mar/2022

TLP:CLEAR

Definições:
Comunidade, Organização e Clientes

- **Comunidade: 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).

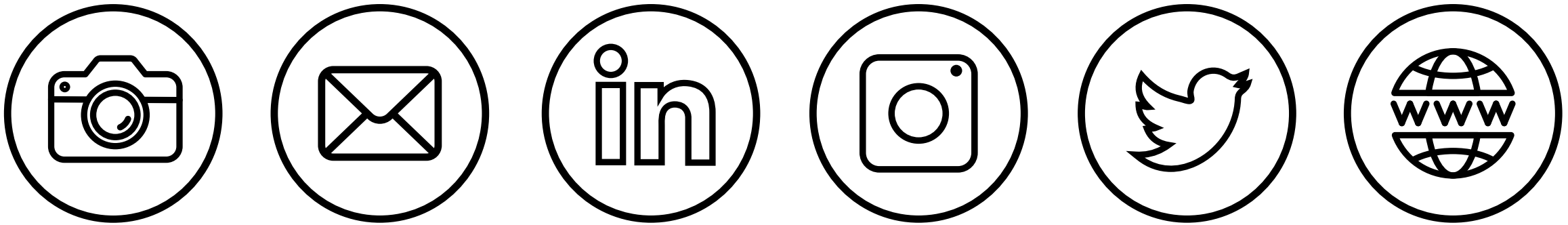
- **Organização:** um grupo que compartilha uma mesma afiliação através de um **processo formal de filiação e que está sujeito a um conjunto de políticas em comum definidas pela organização**. Uma organização pode ser tão ampla quanto todos os membros de uma organização para compartilhamento de informações,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

- **Clientes: 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*).

https://cert.br/tlp/

TLP:CLEAR

NÃO HÁ LIMITES NA DIVULGAÇÃO

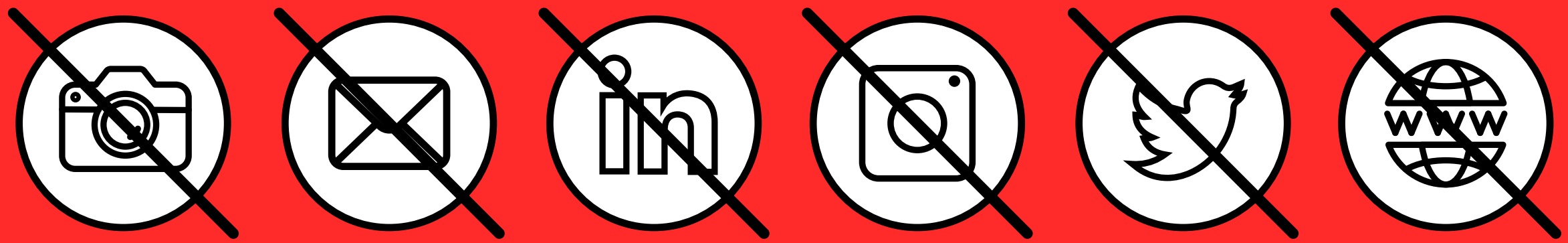


https://cert.br/tlp/

TLP:RED

NÃO DEVE SER DIVULGADO

- SOMENTE PARA OS **OLHOS E OUVIDOS DO INDIVÍDUO** DESTINATÁRIO

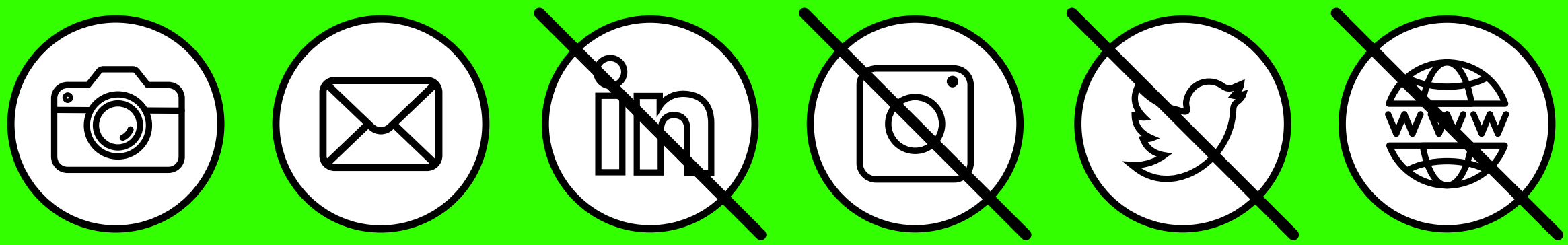


https://cert.br/tlp/

TLP:GREEN

DIVULGAÇÃO LIMITADA:

- À COMUNIDADE DE SEGURANÇA CIBERNÉTICA
- NÃO PODE USAR CANAIS PUBLICAMENTE ACESSÍVEIS



https://cert.br/tlp/

TLP:AMBER

DIVULGAÇÃO LIMITADA A **QUEM PRECISA SABER**:

- EM SUA ORGANIZAÇÃO
- EM SEU PÚBLICO-ALVO OU CLIENTES

⚠ **AO REPASSAR** MUDE PARA **TLP:AMBER+STRICT**

https://cert.br/tlp/

TLP:AMBER+STRICT

DIVULGAÇÃO LIMITADA A **QUEM PRECISA SABER**:

- SOMENTE INTERNA À **SUA ORGANIZAÇÃO**
- **NÃO** COMPARTILHAR
  COM PÚBLICO-ALVO OU CLIENTES

https://cert.br/tlp/

TLP	Quando deve ser usado?	Como pode ser compartilhado?
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.
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.**	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.
TLP:AMBER+STRICT **Divulgação limitada, destinatários só podem disseminar para aqueles que necessitam saber (*need-to-know basis*) e somente dentro de sua própria organização.**	Fontes podem usar o TLP:AMBER+STRICT 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. **Se a fonte quiser restringir o compartilhamento somente para a organização ela deve especificar TLP:AMBER+STRICT.**	Destinatários **podem compartilhar TLP:AMBER+STRICT somente com membros de sua própria organização**, e somente com aqueles que necessitam saber da informação (*need-to-know basis*) para proteger sua organização e evitar danos continuados.
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.**
TLP:CLEAR **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.	Destinatários podem disseminar para o mundo, não há limites na divulgação. Desde que respeitadas as regras padrão de direitos autorais, as informações TLP:CLEAR podem ser compartilhadas sem restrições.

Pontos de Atenção:
Entendimento do Padrão e Exceções

Tenha certeza que o destinatário entende o que é TLP e como usar.

O que diz o padrão:

f. **A fonte é responsável por garantir que os destinatários de uma informação marcada com TLP compreendam e possam seguir as orientações de compartilhamento.**

O TLP não atende exatamente o que você precisa? Especifique ou peça uma exceção.

O que diz o padrão:

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.**

https://cert.br/tlp/

Traffic Light Protocol (TLP) Versão 2.0:
Tradução Oficial - Português Brasileiro

TLP:CLEAR

Tradução

CERT.br/NIC.br

- Cristine Hoepers

Revisão

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

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

Referências

Página do CERT.br com um resumo do TLP e *links* para materiais de referência

– Uso do TLP pelo CERT.br
https://cert.br/tlp/

Palestra de Anúncio do TLP 2.0

– *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

Referências Oficiais

– 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

Novos Materiais da Cartilha do CERT.br

Ajude a Divulgar:

https://cartilha.cert.br/

Obrigada

cristine@cert.br

Notificações para: cert@cert.br

@certbr

https://cert.br/

25 anos cert.br

nic.br cgi.br

www.nic.br | www.cgi.br