nic.br cgi.br | cert.br

8º Fórum Brasileiro de CSIRTs

10 de setembro de 2019

São Paulo / SP

Padrões Globais para Tratamento de Incidentes, Troca de Informações e Maturidade: como Utilizá-los para Facilitar o seu Dia a Dia

Dra. Cristine Hoepers
Gerente Geral
cristine@cert.br

cert.br nic.br cgi.br

TLP:WHITE

Núcleo de Informação e Coordenação do Ponto BR – NIC.br

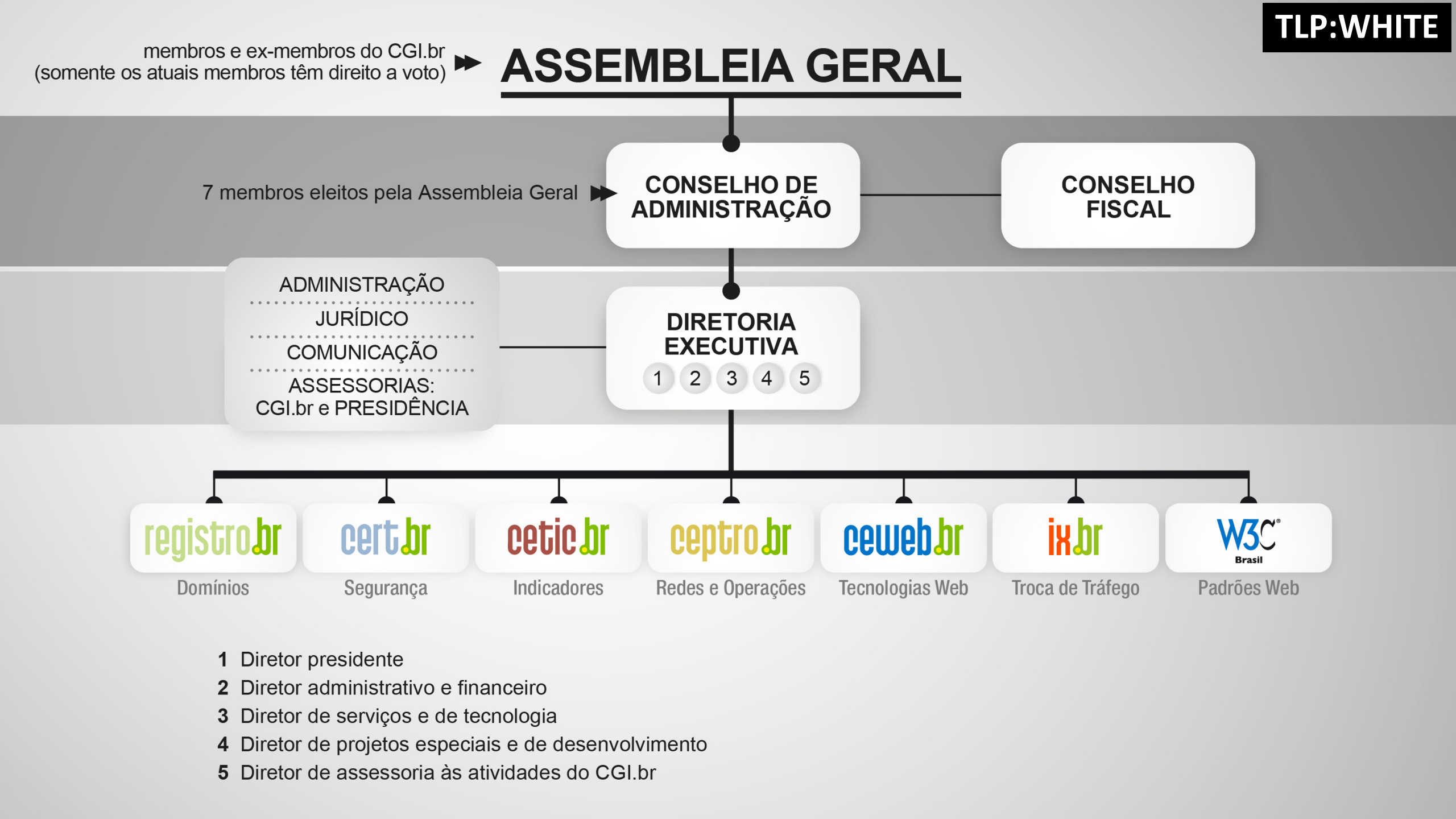
Pessoa jurídica de direito privado, sem fins lucrativos, criada para implementar as decisões e os projetos do Comitê Gestor da Internet no Brasil - CGI.br.

Dentre seus objetivos estão:

- o registro e manutenção dos nomes de domínios que usam o <.br> , e a distribuição de números de Sistema Autônomo (ASN) e endereços IPv4 e IPv6 no País, por meio do Registro.br;
- **atender aos requisitos de segurança e emergências na Internet Brasileira em articulação e cooperação com as entidades e os órgãos responsáveis, atividades do CERT.br;**
- projetos que apoiem ou aperfeiçoem a infraestrutura de redes no País, como a interconexão direta entre redes (IX.br) e a distribuição da Hora Legal brasileira (NTP.br). Esses projetos estão a cargo do Ceptro.br;
- promover estudos e recomendar procedimentos, normas e padrões técnicos e operacionais, para a segurança das redes e serviços de Internet, bem assim para a sua crescente e adequada utilização pela sociedade.

https://www.nic.br/sobre/
https://www.nic.br/estatuto-nic-br/

TLP:WHITE



1 Diretor presidente
2 Diretor administrativo e financeiro
3 Diretor de serviços e de tecnologia
4 Diretor de projetos especiais e de desenvolvimento
5 Diretor de assessoria às atividades do CGI.br

cert.br

Tratamento de Incidentes	Treinamento e Conscientização	Análise de Tendências
▶ Articulação	▶ Cursos	▶ *Honeypots* Distribuídos
▶ Análise Técnica	▶ Palestras	▶ SpamPots
▶ Apoio à recuperação	▶ Boas Práticas	▶ Processamento de *threat feeds*
	▶ Reuniões	

FIRST Improving Security Together MEMBER

APWG RESEARCH PARTNER www.antiphishing.org

CARNEGIE MELLON UNIVERSITY SOFTWARE ENGINEERING INSTITUTE

SEI Partner Network

The Honeynet PROJECT

Criação:

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

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

[1]https://www.nic.br/grupo/historico-gts.htm | [2]https://www.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.

Foco das Atividades

- Atuar como ponto de contato nacional para notificação de incidentes
- Auxiliar na análise técnica e compreensão de ataques e ameaças
- Estabelecer um trabalho colaborativo com outras entidades
- Aumentar a capacidade de detecção de incidentes, correlação de eventos e determinação de tendências
- Transferir o conhecimento adquirido através de cursos, boas práticas e materiais de conscientização

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

TLP:WHITE

Número crescente

- Diversos países
- Diversos setores
- Variados níveis de maturidade

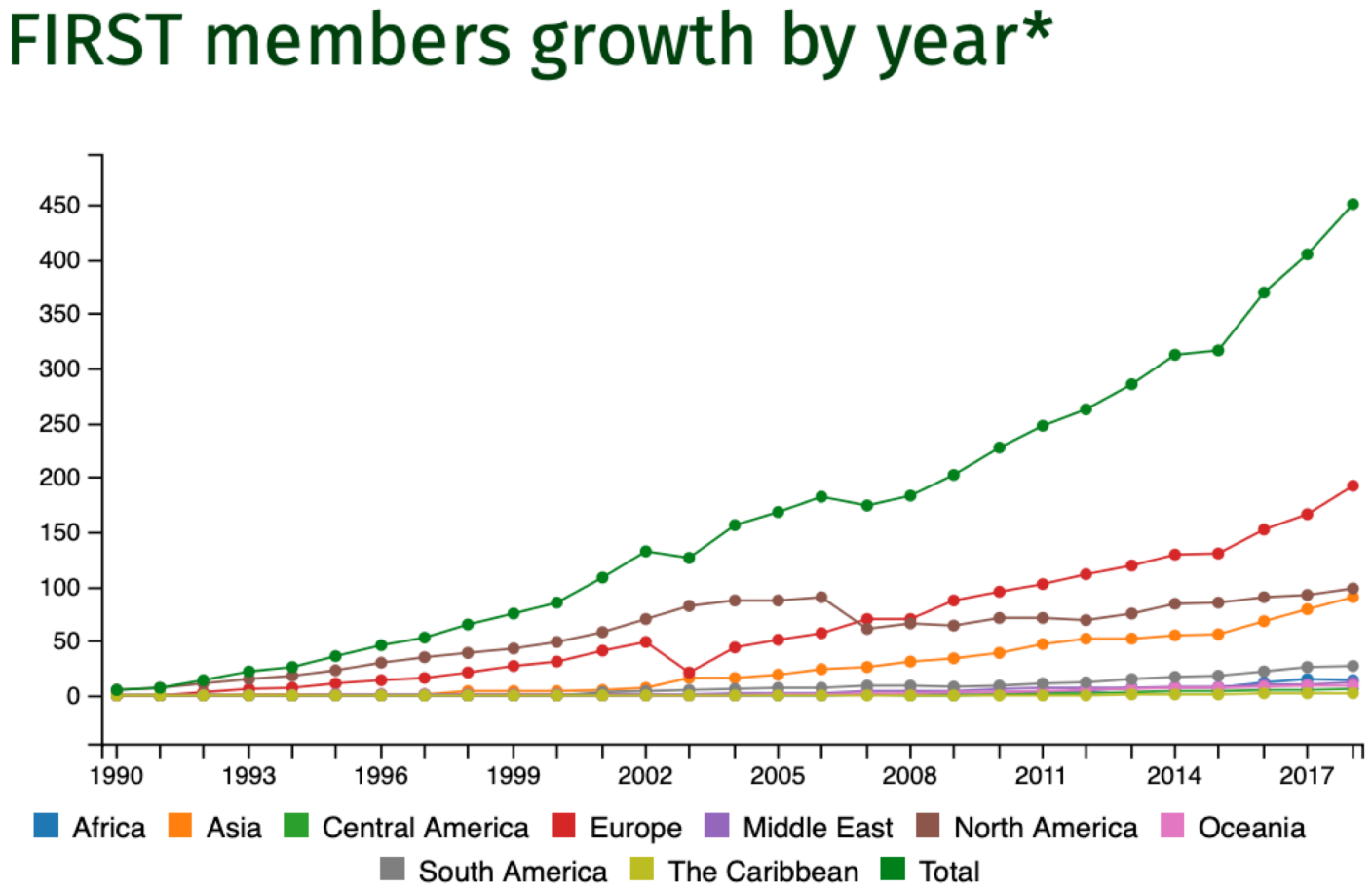
Confiança (*trust*) é pré-requisito para cooperação

Desafios na comunicação

- Como comunicar expectativa de confidencialidade?
- Como identificar serviços disponíveis?
- Como quantificar maturidade e qualidade do serviço?

Adicionalmente

- Como identificar habilidades e conhecimentos necessários aos profissionais dessa área?



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

Fonte: *FIRST History*, *link* visitado em 08/09/2019
https://www.first.org/about/history

TLP:WHITE

Caminho sendo adotado:
Padrões e Guias Construídos pela Comunidade

Organizações envolvidas

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

Iniciativas

- FIRST:
  - **TLP (*Traffic Light Protocol*)**
  - **CSIRT *Services Framework***
  - PSIRT *Services Framework*
  - *Information Exchange Policy* (IEP)
- *Open* CSIRT *Foundation* e TF-CSIRT *Trusted Introducer*
  - **SIM3 (*Security Incident Management Maturity Model*)**
- GFCE
  - *Global CSIRT Maturity Framework* (utiliza SIM3)
- ENISA
  - ENISA CSIRT *maturity assessment model* (utiliza SIM3)

TLP
Traffic Light Protocol

cert.br nic.br cgi.br

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

TLP:WHITE

O que é?

– um conjunto de designações

– 4 cores para indicar os limites de compartilhamento

Por que?

– facilitar a adoção e a colaboração mais frequente

– aumentar a legibilidade

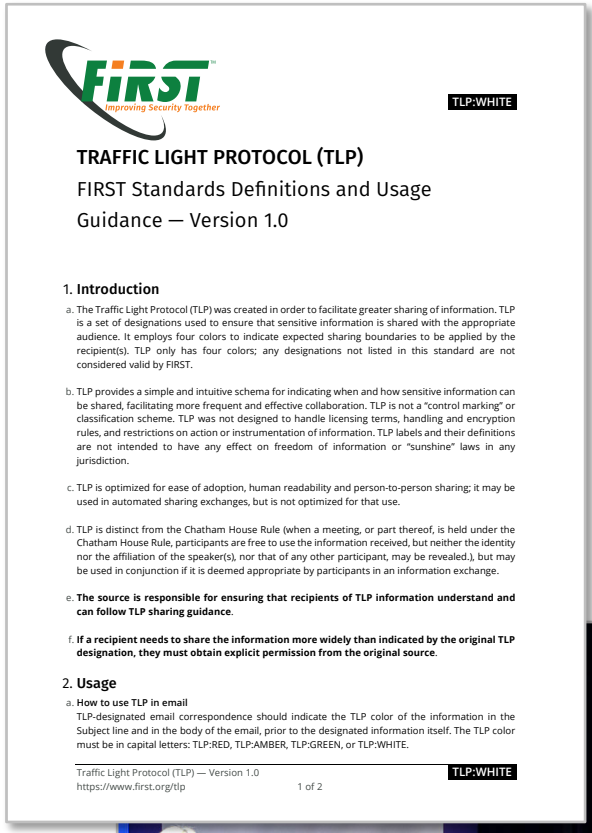
– facilitar compartilhamento entre pessoas

Onde usar?

– documentos, *e-mails*, *slides*, notificações

– plataformas de CTI, como MISP

– qualquer outro lugar (ex: Conferência do FIRST)



FIRST Improving Security Together

TLP:WHITE

TRAFFIC LIGHT PROTOCOL (TLP)

FIRST Standards Definitions and Usage Guidance — Version 1.0

1. **Introduction**

a. The Traffic Light Protocol (TLP) was created in order to facilitate greater sharing of information. TLP is a set of designations used to ensure that sensitive information is shared with the appropriate audience. It employs four colors to indicate expected sharing boundaries to be applied by the recipient(s). TLP only has four colors; any designations not listed in this standard are not considered valid by FIRST.

b. TLP provides a simple and intuitive schema for indicating when and how sensitive information can be shared, facilitating more frequent and effective collaboration. TLP is not a "control marking" or classification scheme. TLP was not designed to handle licensing terms, handling and encryption rules, and restrictions on action or instrumentation of information. TLP labels and their definitions are not intended to have any effect on freedom of information or "sunshine" laws in any jurisdiction.

c. TLP is optimized for ease of adoption, human readability and person-to-person sharing; it may be used in automated sharing exchanges, but is not optimized for that use.

d. TLP is distinct from the Chatham House Rule (when a meeting, or part thereof, is held under the Chatham House Rule, participants are free to use the information received, but neither the identity nor the affiliation of the speaker(s), nor that of any other participant, may be revealed.), but may be used in conjunction if it is deemed appropriate by participants in an information exchange.

e. **The source is responsible for ensuring that recipients of TLP information understand and can follow TLP sharing guidance.**

f. **If a recipient needs to share the information more widely than indicated by the original TLP designation, they must obtain explicit permission from the original source.**

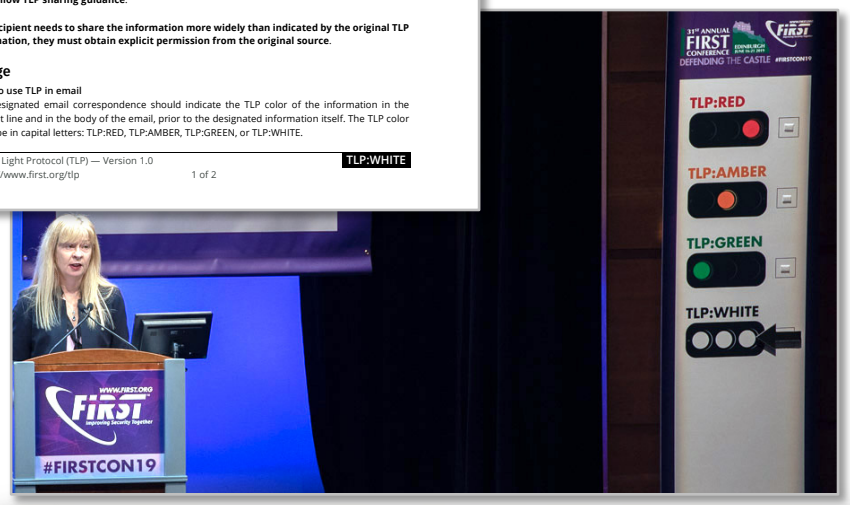
2. **Usage**

a. **How to use TLP in email**

TLP-designated email correspondence should indicate the TLP color of the information in the Subject line and in the body of the email, prior to the designated information itself. The TLP color must be in capital letters: TLP:RED, TLP:AMBER, TLP:GREEN, or TLP:WHITE.

Traffic Light Protocol (TLP) — Version 1.0 TLP:WHITE

https://www.first.org/tlp 1 of 2



Traffic Light Protocol (TLP): **Padrão do FIRST — Versão 1.0**

TLP:WHITE

Objetivo

- São 492 times de 92 países
- Criar interpretações consistentes entre comunidades diferentes
  - o valor está em tirar ambiguidades inerentes à cultura ou idioma dos CSIRTs envolvidos no compartilhamento de informações

Tradução oficial para português brasileiro

- Realizada pelo CERT.br e pelo CAIS/RNP
  - conforme regras do FIRST
- *Online* em:
  - https://www.first.org/tlp/
  - https://www.first.org/tlp/docs/tlp-v1-pt-br.pdf

TRAFFIC LIGHT PROTOCOL (TLP)
Guia de Uso e Definições do Padrão do FIRST — Versão 1.0

1. Introdução

3. Definições do TLP

a. TLP:RED = Não deve ser divulgado, restrito somente aos participantes.
As fontes podem usar o TLP:RED quando as outras partes não puderem agir de forma efetiva sobre a informação, e qualquer mau uso da informação possa causar impactos na privacidade, reputação ou operações de uma das partes. Destinatários não podem compartilhar informações TLP:RED com ninguém além dos presentes na troca de informações, reunião ou conversa específica na qual a informação foi originalmente divulgada. No contexto de uma reunião, por exemplo, informações TLP:RED são limitadas aos presentes na reunião. Na maioria das vezes, o TLP:RED deve (*should*) ser usado para trocar informações pessoalmente ou de forma oral.

b. TLP:AMBER = Divulgação limitada, restrita às organizações dos participantes.
As fontes podem usar 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 se esta for divulgada fora das organizações envolvidas. Destinatários só podem compartilhar informações TLP:AMBER com membros de suas próprias organizações e com clientes que necessitam saber desta informação para se proteger ou evitar danos futuros. **As fontes são livres para especificar limites adicionais para o compartilhamento: estes limites devem obrigatoriamente (*must*) ser respeitados**.

c. TLP:GREEN = Divulgação limitada, restrito à comunidade.
As fontes podem usar TLP:GREEN quando a informação é útil para a conscientização de todas as organizações participantes, bem como para seus pares no setor ou comunidade. Destinatários podem compartilhar informações TLP:GREEN com seus pares dentro do seu setor ou comunidade, mas não através de canais publicamente acessíveis. Informações nesta categoria podem ser circuladas amplamente dentro de uma comunidade em particular. Informações TLP:GREEN não podem ser divulgadas fora de uma comunidade.

d. TLP:WHITE = Divulgação não é limitada.
As fontes podem usar TLP:WHITE quando o risco de mau uso da informação é mínimo ou não há previsão de risco de mau uso, de acordo com regras e procedimentos aplicáveis para divulgação pública. Informação TLP:WHITE pode ser distribuída sem restrições, desde que respeitadas as regras padrão de direitos autorais.

Notas:
1. Este documento utiliza deve (*should*) e deve obrigatoriamente (*must*) conforme definido pela RFC-2119.
2. Comentários ou sugestões sobre este documento podem ser enviadas (em inglês) para tlp-sig@first.org.

Traffic Light Protocol (TLP) – Versão 1.0 (Tradução para Português Brasileiro) TLP:WHITE
https://www.first.org/tlp 2 de 2

Traffic Light Protocol (TLP): **Definições**

TLP:WHITE

Cor	Quando deve ser usado?	Como pode ser compartilhado?
TLP:RED **Não deve ser divulgado**, restrito somente aos participantes.	As fontes podem usar o TLP:RED quando as outras partes não puderem agir de forma efetiva sobre a informação, e qualquer mau uso da informação possa causar impactos na privacidade, reputação ou operações de uma das partes.	Destinatários não podem compartilhar informações TLP:RED com ninguém além dos presentes na troca de informações, reunião ou conversa especifica na qual a informação foi originalmente divulgada. No contexto de uma reunião, por exemplo, informações TLP:RED são limitadas aos presentes na reunião. Na maioria das vezes, o TLP:RED deve (*should*) ser usado para trocar informações pessoalmente ou de forma oral.
TLP:AMBER **Divulgação limitada**, restrita às organizações dos participantes.	As fontes podem usar 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 se esta for divulgada fora das organizações envolvidas.	Destinatários só podem compartilhar informações TLP:AMBER com membros de suas próprias organizações e com clientes que necessitam saber desta informação para se proteger ou evitar danos futuros. **As fontes são livres para especificar limites adicionais para o compartilhamento: estes limites devem obrigatoriamente (*must*) ser respeitados.**
TLP:GREEN **Divulgação limitada**, restrito à comunidade.	As fontes podem usar TLP:GREEN quando a informação é útil para a conscientização de todas as organizações participantes, bem como para seus pares no setor ou comunidade.	Destinatários podem compartilhar informações TLP:GREEN com seus pares dentro do seu setor ou comunidade, mas não através de canais publicamente acessíveis. Informações nesta categoria podem ser circuladas amplamente dentro de uma comunidade em particular. Informações TLP:GREEN não podem ser divulgadas fora de uma comunidade .
TLP:WHITE **Divulgação não é limitada**.	As fontes podem usar TLP:WHITE quando o risco de mau uso da informação é mínimo ou não há previsão de risco de mau uso, de acordo com regras e procedimentos aplicáveis para divulgação publica.	Informação TLP:WHITE pode ser distribuída sem restrições, desde que respeitadas as regras padrão de direitos autorais.

CSIRT *Services Framework*

cert.br nic.br cgi.br

TLP:WHITE

CSIRT *Services Framework v2.0*

Descrição em alto nível dos possíveis serviços que possam ser oferecidos

- por um CSIRT
- por outros times que tenham serviços relacionados com gestão de incidentes

Substituirá o famoso "CSIRT Services"

Visão do FIRST sobre o que são boas práticas

- Objetiva auxiliar times a
  - identificar e definir as principais categorias de serviços
  - um ponto de partida para a padronização de termos e definições a serem usados pela comunidade
- O que esse documento **não** é
  - não explica como implantar um CSIRT
  - não aborda maturidade ou qualidade de um CSIRT

https://www.first.org/education/csirt_services_framework_v2.0

CSIRT *Services Framework v2.0*: **Visão das Áreas e Serviços**

TLP:WHITE

Information Security Event Management

- Monitoring and Detection
- Analyzing

Information Security Incident Management

- Accepting Reports
- Analyzing Incidents
- Analyzing artefacts and forensic evidence
- Mitigation and recovery
- Coordination

Vulnerability Management

- Vulnerability Discovery
- Report Intake
- Analysis
- Coordination
- Disclosure
- Response

Situational Awareness

- Data Acquisition
- Analysis and Synthesis
- Communication

Knowledge Transfer

- Awareness Building
- Training and Education
- Exercises
- Technical and Policy Advisory

CSIRT *Services Framework v2.0:*
Estrutura, Autores e Próximos passos

TLP:WHITE

Estrutura

Formato de cada área

- *Service Area*
  - *Service*
    - *Function*
      - *Sub-Function*

Próximos passos (*hopefully*! :-)

- Aberto para comentários até 30 de setembro
- Versão final no primeiro semestre de 2020
- Trabalhos futuros (SIG)
  - matriz de competências
  - material de treinamento

Autores

Editor

- Klaus-Peter Kossakowski, Hamburg University of Applied Science

Coordenadores de área

- Olivier Caleff, openCSIRT Foundation (FR)
- Cristine Hoepers, CERT.br (BR)
- Amanda Mullens, CISCO (US)
- Samuel Perl, CERT/CC (US)
- Daniel Roethlisberger, Swisscom (CH)
- Robin M. Ruefle, CERT/CC (US)
- Mark Zajicek, CERT/CC (US)

Contribuidores

- Vilius Benetis, NRD CIRT (LT)
- Angela Horneman, CERT/CC (US)
- Allen Householder, CERT/CC (US)
- Art Manion, CERT/CC (US)
- Sigitas Rokas, NRD CIRT (LT)
- Mary Rossell, Intel (US)
- Désirée Sacher, Finanz Informatik (DE)
- Krassimir T. Tzvetanov, Fastly (US)

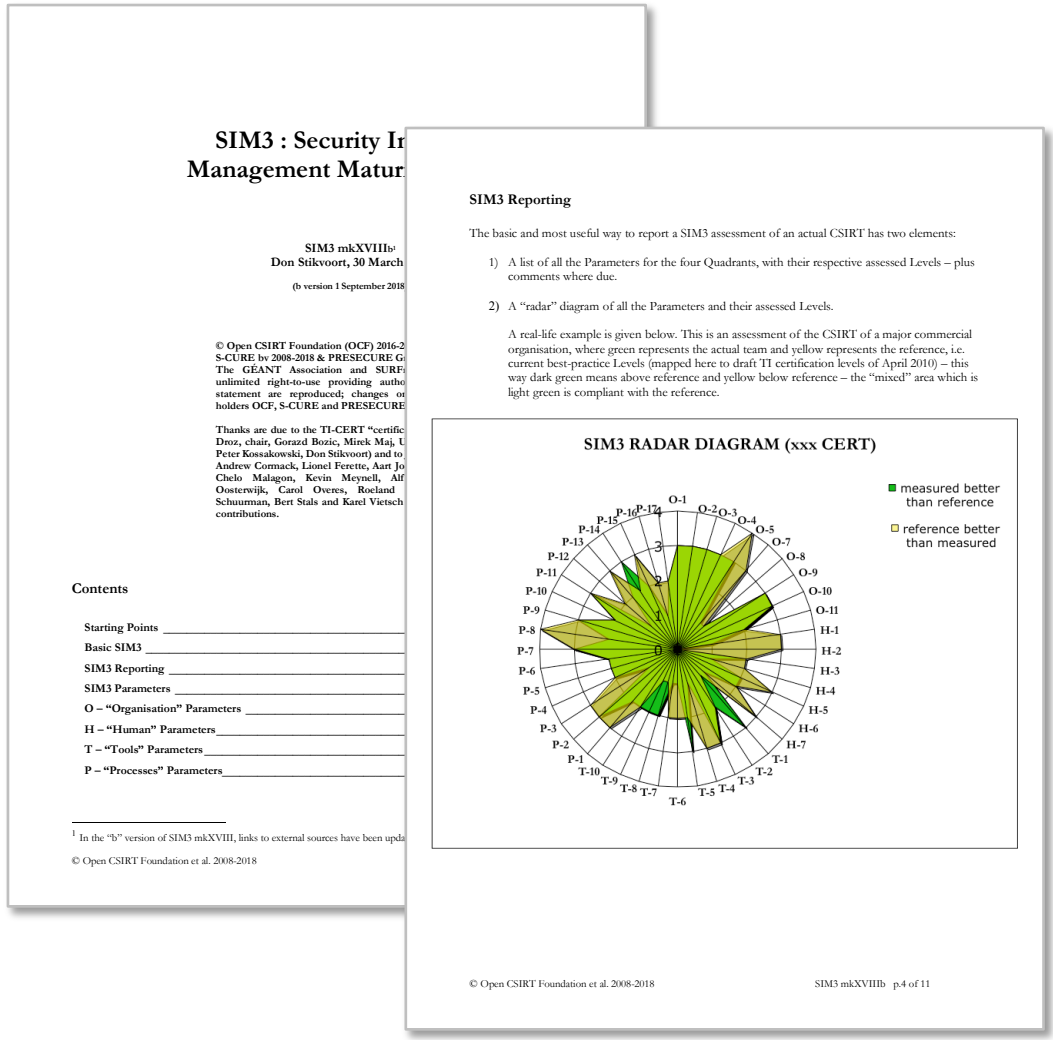
SIM3
Security Incident Management Maturity Model

cert.br nic.br cgi.br

TLP:WHITE

SIM3 – *Security Incident Management Maturity Model*

- Quatro pilares
  - Prevenção
  - Detecção
  - Resolução
  - Controle de qualidade e *feedback*
- Quatro quadrantes
  - O – Organisation (11 parâmetros)
  - H – Human (7 parâmetros)
  - T – Tools (10 parâmetros)
  - P – Processes (17 parâmetros)
- Quem usa
  - TF-CSIRT Trusted Introducer
  - ENISA, requerimento para CERTs Nacionais (NIS Directive)
  - Nippon CSIRT Association
  - FIRST: será adotado no processo de filiação



SIM3 : Security In
Management Matur

SIM3 mkXVIIIb[1]
Don Stikvoort, 30 March

(b version 1 September 2018

© Open CSIRT Foundation (OCF) 2016-2
S-CURE bv 2008-2018 & PRESECURE G
The GÉANT Association and SURF
unlimited right-to-use providing autho
statement are reproduced; changes or
holders OCF, S-CURE and PRESECURE

Thanks are due to the TI-CERT "certific
Droz, chair, Gorazd Bozic, Mirek Maj, U
Peter Kossakowski, Don Stikvoort) and to
Andrew Cormack, Lionel Ferette, Aart Jo
Chelo Malagon, Kevin Meynell, Alf
Oosterwijk, Carol Overes, Roeland
Schuurman, Bert Stals and Karel Vietsch
contributions.

Contents

Starting Points
Basic SIM3
SIM3 Reporting
SIM3 Parameters
O – "Organisation" Parameters
H – "Human" Parameters
T – "Tools" Parameters
P – "Processes" Parameters

[1] In the "b" version of SIM3 mkXVIII, links to external sources have been upda

© Open CSIRT Foundation et al. 2008-2018

SIM3 Reporting

The basic and most useful way to report a SIM3 assessment of an actual CSIRT has two elements:

1) A list of all the Parameters for the four Quadrants, with their respective assessed Levels – plus comments where due.
2) A "radar" diagram of all the Parameters and their assessed Levels.

A real-life example is given below. This is an assessment of the CSIRT of a major commercial organisation, where green represents the actual team and yellow represents the reference, i.e. current best-practice Levels (mapped here to draft TI certification levels of April 2010) – this way dark green means above reference and yellow below reference – the "mixed" area which is light green is compliant with the reference.

SIM3 RADAR DIAGRAM (xxx CERT)

© Open CSIRT Foundation et al. 2008-2018 SIM3 mkXVIIIb p.4 of 11

https://opencsirt.org/maturity/sim3/
https://www.thegfce.com/initiatives/c/csirt-maturity-initiative/documents/reports/2019/06/12/maturity-framework-for-national-csirts

SIM3: **Parâmetros**

0 = not available / undefined / unaware

1 = implicit (known/considered but not written down, “between the ears”)

2 = explicit, internal (written down but not formalized in any way)

3 = explicit, formalized on authority of CSIRT head (rubberstamped or published)

4 = explicit, audited on authority of governance levels above the CSIRT head (subject to control process/audit/enforcement)

Como usar:

- Os parâmetros são em comum
- Cada comunidade escolhe os níveis de maturidade para seu contexto

ENISA CSIRT Maturity - Self-assessment Tool
https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-capabilities/csirt-maturity

Parameter number	Parameter description	Parameter number	Parameter description
O-1	Mandate	T-6	Resilient E-Mail
O-2	Constituency	T-7	Resilient Internet Access
O-3	Authority	T-8	Incident Prevention Toolset
O-4	Responsibility	T-9	Incident Detection Toolset
O-5	Service Description	T-10	Incident Resolution Toolset
O-7	Service Level Description	P-1	Escalation to Governance Level
O-8	Incident Classification	P-2	Escalation to Press Function
O-9	Integration in existing CSIRT Systems	P-3	Escalation to Legal Function
O-10	Organisational Framework	P-4	Incident Prevention Process
O-11	Security Policy	P-5	Incident Detection Process
H-1	Code of Conduct/Practice/Ethics	P-6	Incident Resolution Process
H-2	Personnel Resilience	P-7	Specific Incident Processes
H-3	Skillset Description	P-8	Audit/Feedback Process
H-4	Internal Training	P-9	Emergency Reachability Process
H-5	External Technical Training	P-10	Best Practice E-mail and Web Presence
H-6	(External) Communication Training	P-11	Secure Information Handling Process
H-7	External Networking	P-12	Information Sources Process
T-1	IT Resources List	P-13	Outreach Process
T-2	Information Sources List	P-14	Reporting Process
T-3	Consolidated E-Mail System	P-15	Statistics Process
T-4	Incident Tracking System	P-16	Meeting Process
T-5	Resilient Phone	P-17	Peer-to-Peer Process

Referências adicionais

- TF-CSIRT Trusted Introducer Listing of operational Teams
  https://www.trusted-introducer.org/processes/registration.html
- TF-CSIRT Trusted Introducer Accreditation
  https://www.trusted-introducer.org/processes/accreditation.html
- ENISA CSIRT Maturity assessment
  https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-capabilities/csirt-maturity
- ENISA CSIRT maturity assessment model
  https://www.enisa.europa.eu/publications/study-on-csirt-maturity
- ENISA Maturity Evaluation Methodology for CSIRTs
  https://www.enisa.europa.eu/publications/study-on-csirt-maturity-evaluation-process

Obrigada

cristine@cert.br

Notificações para: cert@cert.br

@certbr

www.cert.br

10 de setembro de 2019

nic.br cgi.br

www.nic.br | www.cgi.br