Iº WEBINÁRIO

GABINETE DE SEGURANÇA INSTITUCIONAL

GOVERNO FEDERAL
BRASIL
UNIÃO E RECONSTRUÇÃO

Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo
- CTIR Gov -

Comunicação Efetiva

AGENDA

01 Comunicação

- A importância da confiança na comunicação entre integrantes da Rede
- Canais de comunicação

02 Traffic Light Protocol

- Objetivos do Protocolo?
- A utilização do TLP na Rede

03 Contatos

- Como notificar o CTIR
- Como o CTIR notifica
- Whois
- Melhor contato

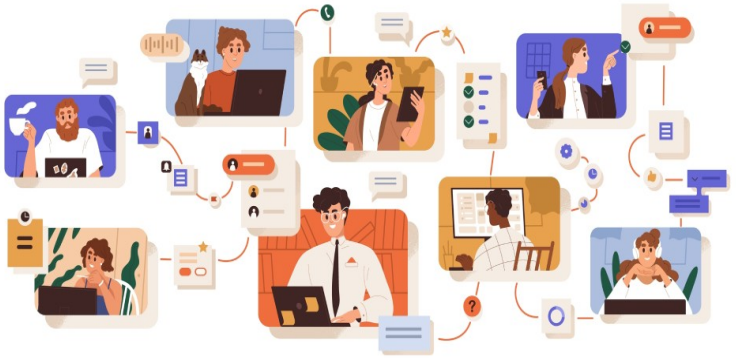
04 Automatização

- Vantagens e desvantagens
- Impactos no processo de resposta a incidentes
- O CTIR recomenda?

COMUNICAÇÃO

COMUNICAÇÃO

Em um contexto formal, a comunicação é estruturada e segue padrões específicos para garantir clareza, precisão e eficácia.

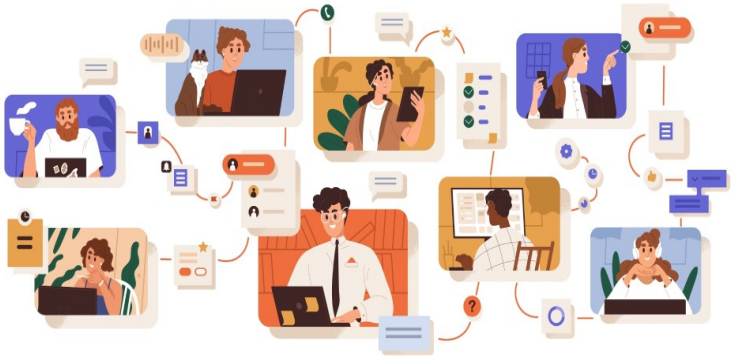


COMUNICAÇÃO

Em um contexto formal, a comunicação é estruturada e segue padrões específicos para garantir clareza, precisão e eficácia.

Mas ela também deve:

Ser oportuna;



COMUNICAÇÃO

Em um contexto formal, a comunicação é estruturada e segue padrões específicos para garantir clareza, precisão e eficácia.

Mas ela também deve:

Ser oportuna;

Ser objetiva;

COMUNICAÇÃO

Em um contexto formal, a comunicação é estruturada e segue padrões específicos para garantir clareza, precisão e eficácia.

Mas ela também deve:

Ser oportuna;

Ser objetiva; e

Baseada em fatos;

CONFIANÇA NA COMUNICAÇÃO

Em um contexto organizacional ou institucional, confiança envolve a expectativa de que uma entidade ou sistema cumprirá suas obrigações e responsabilidades de maneira previsível e ética, conforme as normas e padrões estabelecidos.

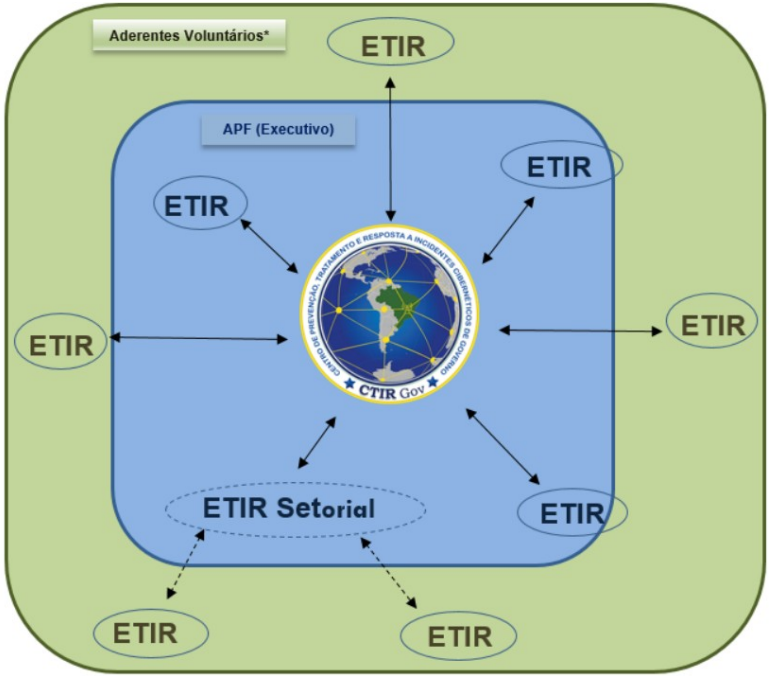
CONFIANÇA NA COMUNICAÇÃO

Em um contexto organizacional ou institucional, confiança envolve a expectativa de que uma entidade ou sistema cumprirá suas obrigações e responsabilidades de maneira previsível e ética, conforme as normas e padrões estabelecidos.

A confiança é um elemento fundamental em todas as formas de interação social e é essencial para o funcionamento eficaz de sociedades, economias e organizações, pois reduz a incerteza e facilita a cooperação.

CONFIANÇA NA COMUNICAÇÃO

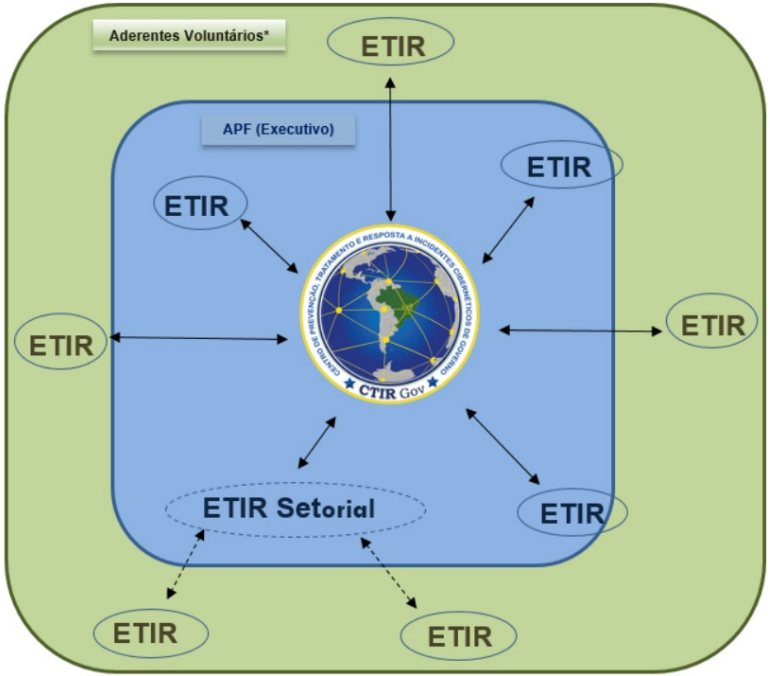
No âmbito da ReGIC essa confiança deve ser potencializada haja vista a natureza das ETIR pertencentes à Rede.



CONFIANÇA NA COMUNICAÇÃO

No âmbito da ReGIC essa confiança deve ser potencializada haja vista a natureza da ETIR pertencentes à Rede.

Assim, a confiança na Rede será fortalecida por meio de uma comunicação que seja:

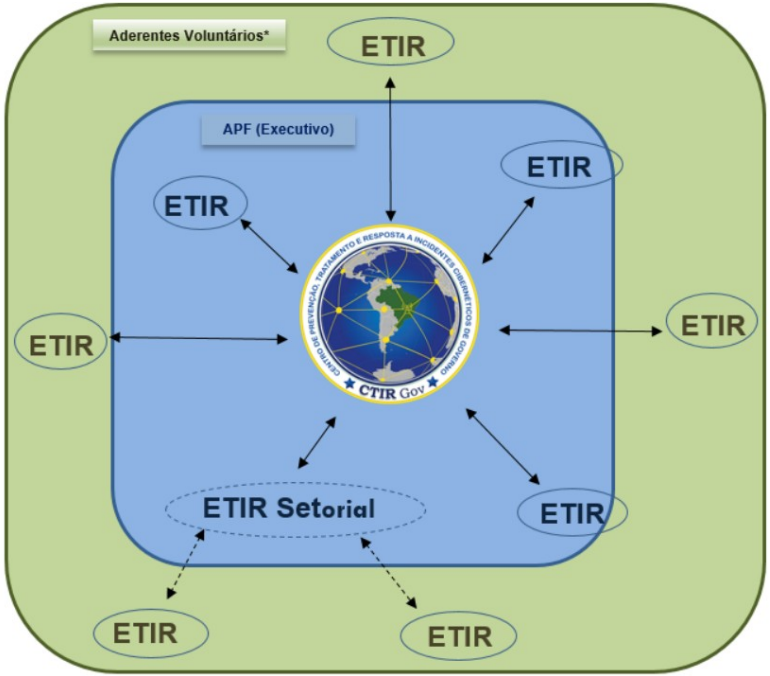


CONFIANÇA NA COMUNICAÇÃO

No âmbito da ReGIC essa confiança deve ser potencializada haja vista a natureza da ETIR pertencentes à Rede.

Assim, a confiança na Rede será fortalecida por meio de uma comunicação que seja:

- Oportuna;

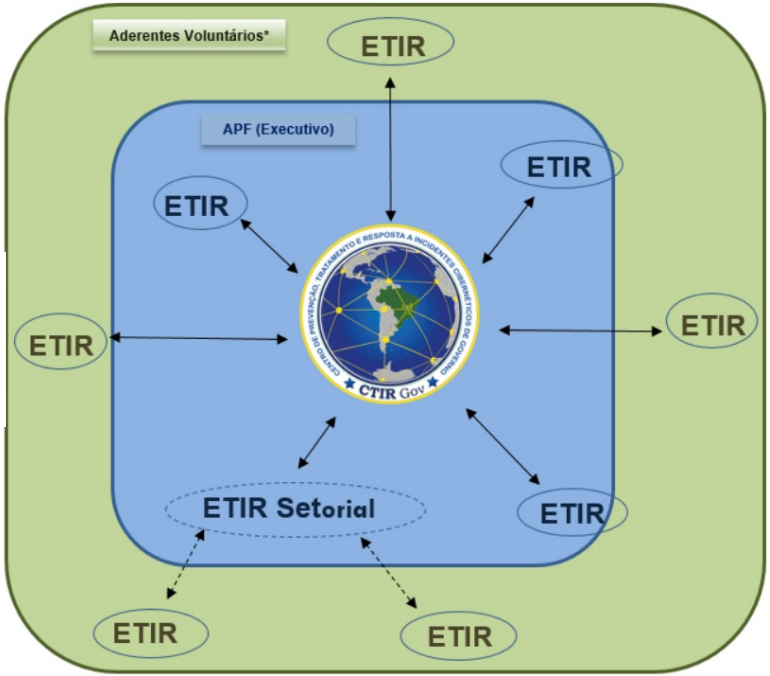


CONFIANÇA NA COMUNICAÇÃO

No âmbito da ReGIC essa confiança deve ser potencializada haja vista a natureza da ETIR pertencentes à Rede.

Assim, a confiança na Rede será fortalecida por meio de uma comunicação que seja:

- Oportuna;
- Baseada em evidências;

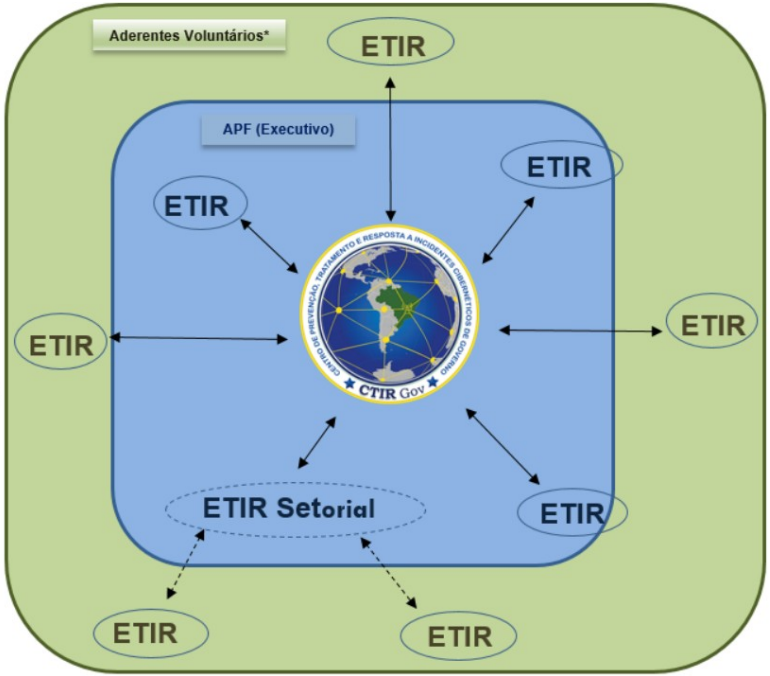


CONFIANÇA NA COMUNICAÇÃO

No âmbito da ReGIC essa confiança deve ser potencializada haja vista a natureza da ETIR pertencentes à Rede.

Assim, a confiança na Rede será fortalecida por meio de uma comunicação que seja:

- Oportuna;
- Baseada em evidências;
- Ética;

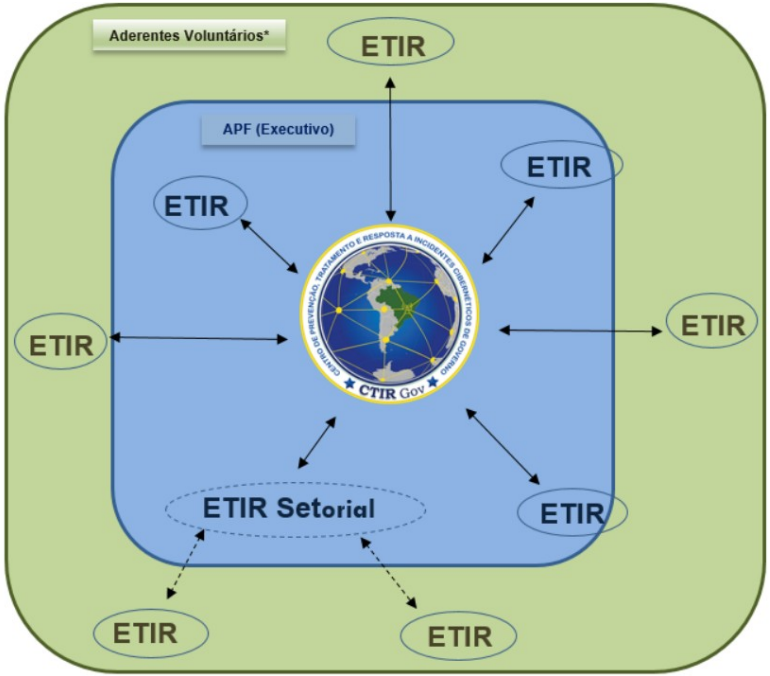


CONFIANÇA NA COMUNICAÇÃO

No âmbito da ReGIC essa confiança deve ser potencializada haja vista a natureza da ETIR pertencentes à Rede.

Assim, a confiança na Rede será fortalecida por meio de uma comunicação que seja:

- Oportuna;
- Baseada em evidências;
- Ética;
- Objetiva;

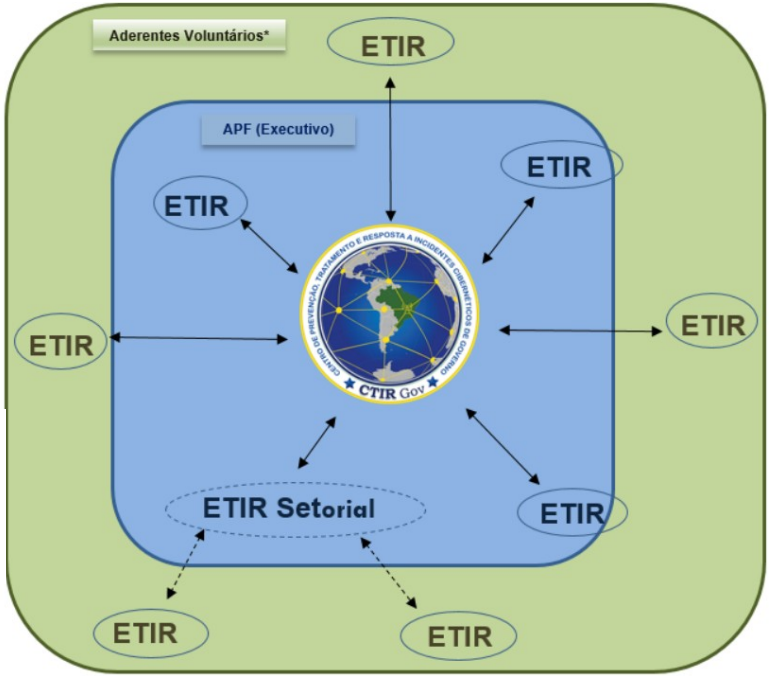


CONFIANÇA NA COMUNICAÇÃO

No âmbito da ReGIC essa confiança deve ser potencializada haja vista a natureza da ETIR pertencentes à Rede.

Assim, a confiança na Rede será fortalecida por meio de uma comunicação que seja:

- Oportuna;
- Baseada em evidências;
- Ética;
- Objetiva;
- Baseada na discrição;

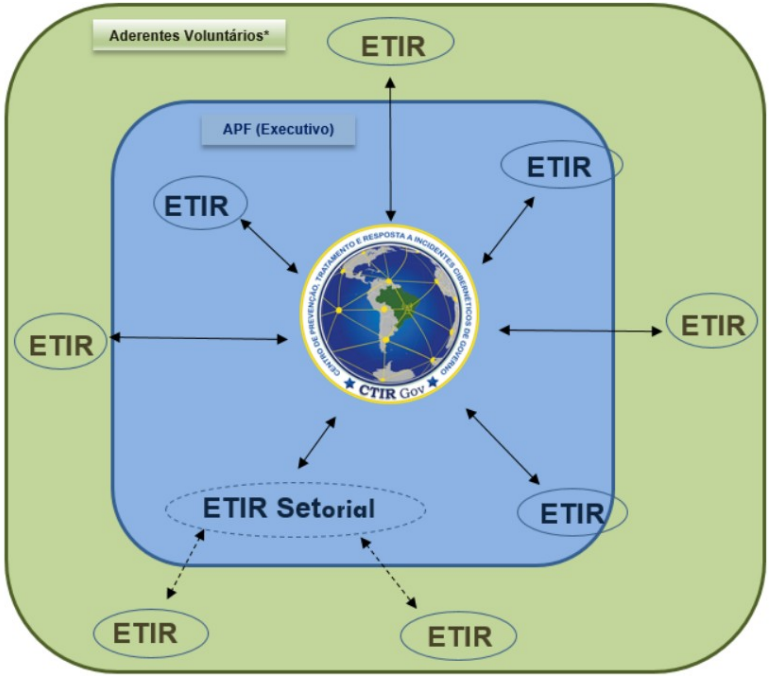


CONFIANÇA NA COMUNICAÇÃO

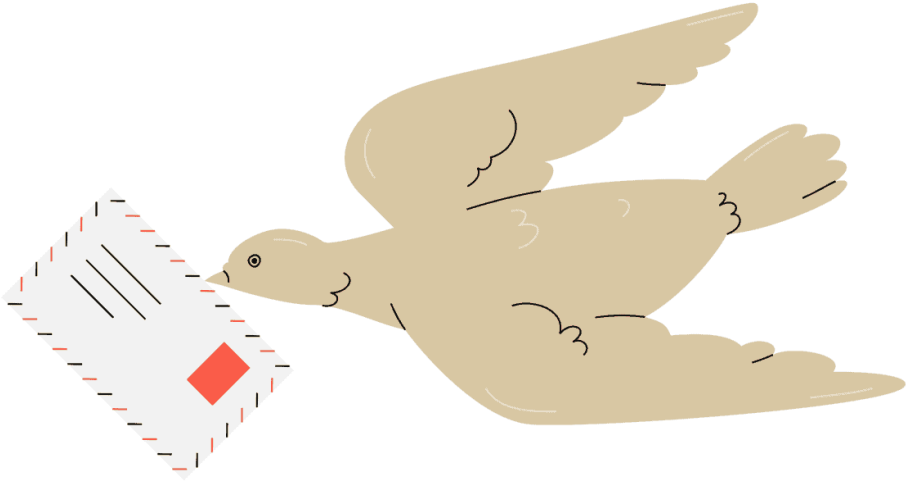
No âmbito da ReGIC essa confiança deve ser potencializada haja vista a natureza da ETIR pertencentes à Rede.

Assim, a confiança na Rede será fortalecida por meio de uma comunicação que seja:

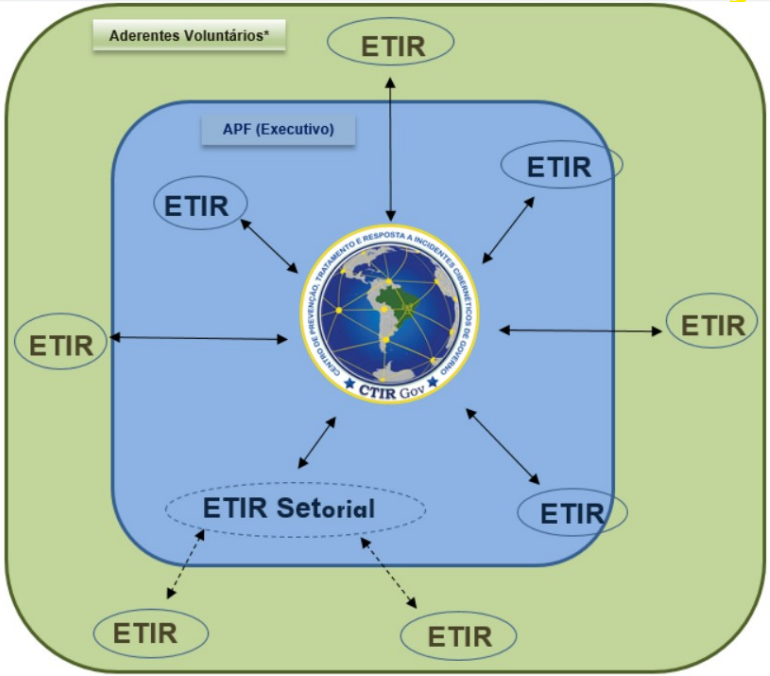
- Oportuna;
- Baseada em evidências;
- Ética;
- Objetiva;
- Baseada na discrição; e
- Segura;



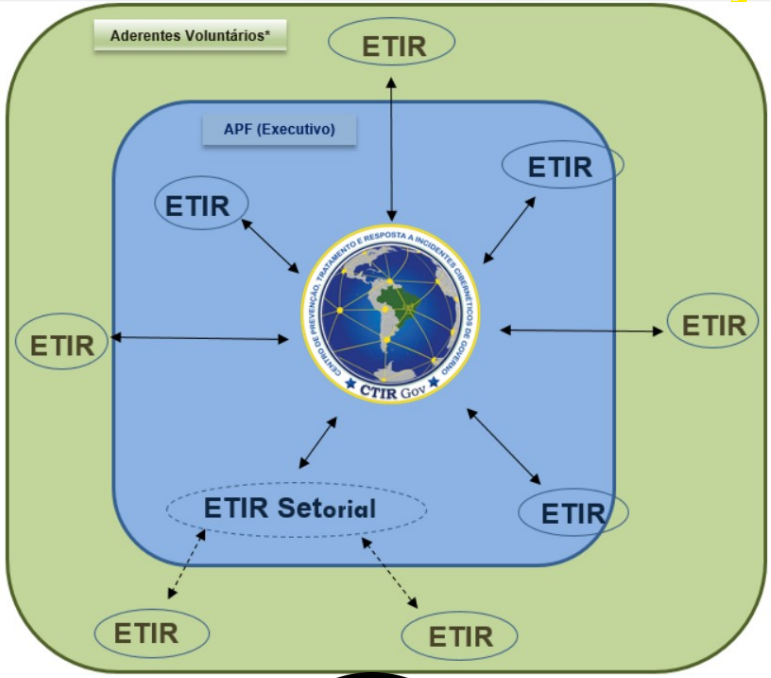
CANAIS DE COMUNICAÇÃO



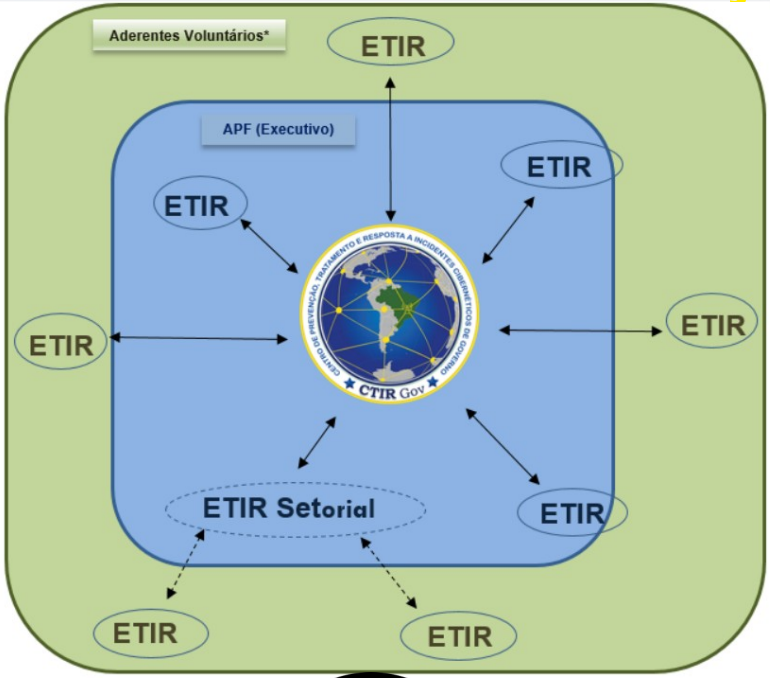
CANAIS DE COMUNICAÇÃO



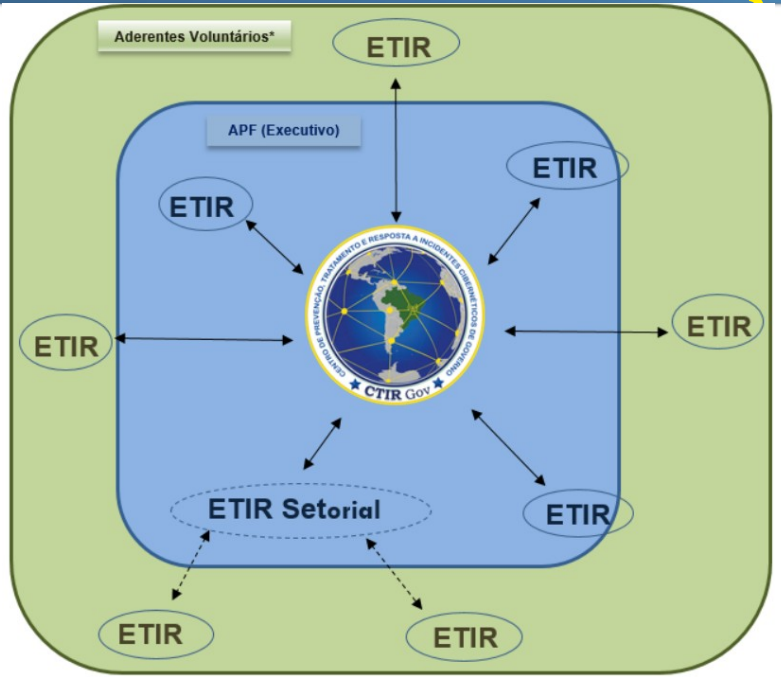
CANAIS DE COMUNICAÇÃO



CANAIS DE COMUNICAÇÃO



CANAIS DE COMUNICAÇÃO



Traffic Light Protocol

Traffic Light Protocol

O **TLP** (*Traffic Light Protocol*) é um padrão global, mantido pelo **FIRST** (*Forum of Incident Response and Security Teams*), para indicar os limites de compartilhamento de informações entre partes interessadas.

https://www.cert.br/tlp/

Traffic Light Protocol

O **TLP** é:

≠

Esquemas de classificação de documentos

Traffic Light Protocol

O **TLP** é:

≠

Velocidade ou prioridade de tráfego da informação

Traffic Light Protocol

A fonte é responsável por assegurar que o destinatário saiba o que é o TLP

Traffic Light Protocol

O TLP indica?

TLP: RED somente para os olhos e ouvidos dos indivíduos destinatários, não é permitido compartilhamento nenhum;

Traffic Light Protocol

O TLP indica?

TLP: RED somente para os olhos e ouvidos dos indivíduos destinatários, não é permitido compartilhamento nenhum;

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;

Traffic Light Protocol

O TLP indica?

TLP: RED somente para os olhos e ouvidos dos indivíduos destinatários, não é permitido compartilhamento nenhum;

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;

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;

Traffic Light Protocol

O TLP indica?

TLP: RED somente para os olhos e ouvidos dos indivíduos destinatários, não é permitido compartilhamento nenhum;

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**;**

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;

TLP: GREEN Divulgação limitada, destinatários podem divulgar dentro de sua comunidade;

Traffic Light Protocol

O TLP indica?

TLP: RED somente para os olhos e ouvidos dos indivíduos destinatários, não é permitido compartilhamento nenhum;

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**;**

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;

TLP: GREEN Divulgação limitada, destinatários podem divulgar dentro de sua comunidade;

TLP: WHITE ou **TLP:CLEAR** Não há limites na divulgação.

https://www.cert.br/tlp/

Traffic Light Protocol

O TLP indica?

TLP:RED

NÃO DEVE SER DIVULGADO
- SOMENTE PARA OS **OLHOS E OUVIDOS DO INDIVÍDUO** DESTINATÁRIO

TLP:AMBER

DIVULGAÇÃO LIMITADA A **QUEM PRECISA SABER**:
- EM SUA ORGANIZAÇÃO
- EM SEU PÚBLICO-ALVO OU CLIENTES

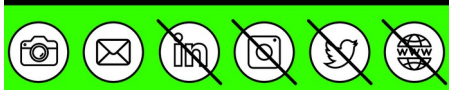
⚠ **AO REPASSAR** MUDE PARA **TLP:AMBER+STRICT**

TLP:AMBER+STRICT

DIVULGAÇÃO LIMITADA A **QUEM PRECISA SABER**:
- SOMENTE INTERNA À **SUA ORGANIZAÇÃO**
- **NÃO** COMPARTILHAR COM PÚBLICO-ALVO OU CLIENTES

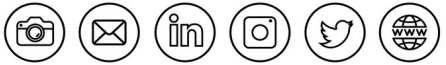
TLP:GREEN

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



TLP:CLEAR

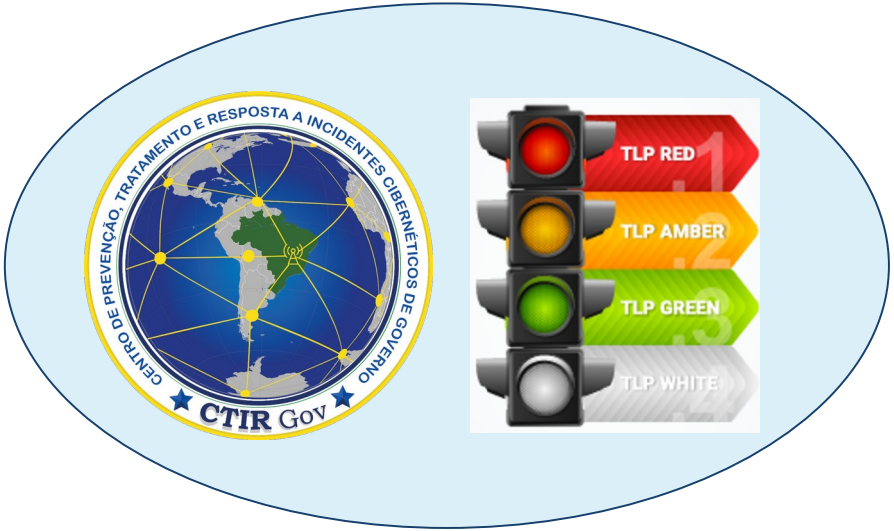
NÃO HÁ LIMITES NA DIVULGAÇÃO



https://www.cert.br/tlp/

Traffic Light Protocol

O CTIR Gov adota o TLP em sua comunicação



https://www.gov.br/ctir/pt-br/assuntos/tlp

Contatos

Contatos

Como notificar o CTIR Gov?

ctir@ctir.gov.br

Contatos

Notificações do CTIR Gov

CTIR Gov consulta melhores contato

Contatos

Notificações do CTIR Gov

RFC 3912

Saiba mais em https://www.rfc-editor.org/rfc/rfc3912.txt

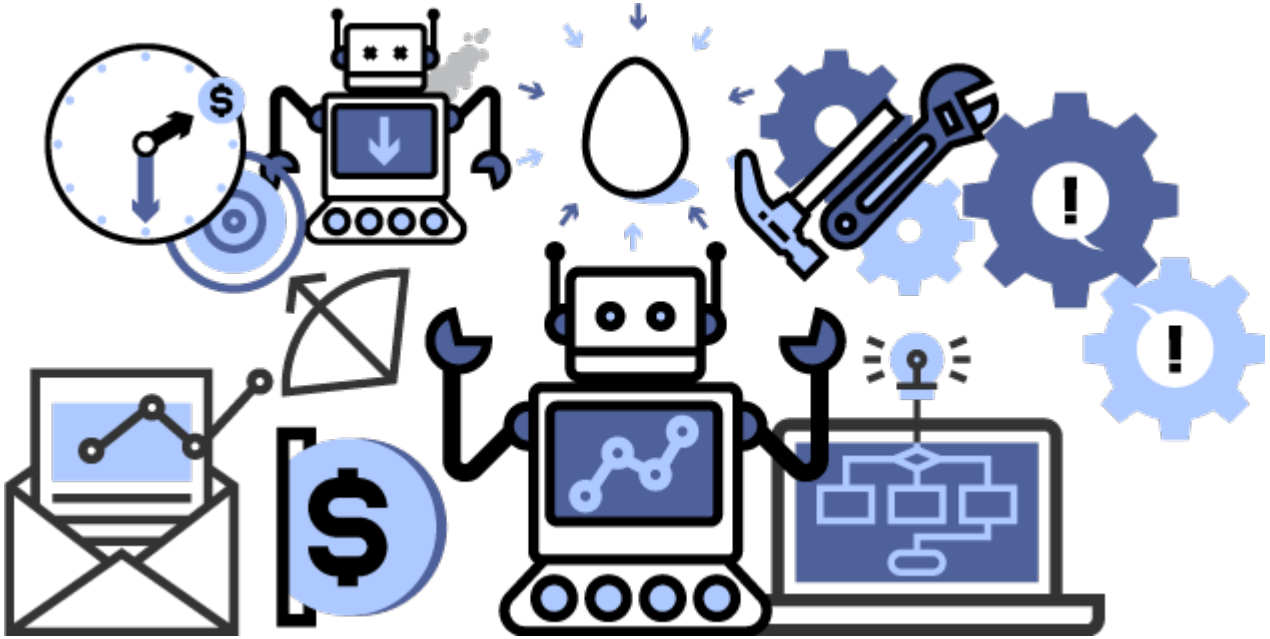
Contatos

Notificações do CTIR Gov

CTIR Gov consulta contato

Consulte em https://registro.br/tecnologia/ferramentas/whois/

Automatização



Automatização

Vantagem

Automatização

Desvantagem na resposta a incidentes

Formato do assunto fora do padrão

Automatização

Desvantagem na resposta a incidentes

Formato do assunto fora do padrão

#4[redacted]4: Chamado R[redacted]4 aberto!

#4[redacted]1: [Ticket#2024050[redacted]] Seu Chamado foi Resolvido!!!

Automatização

Desvantagem na resposta a incidentes

Formato do assunto fora do padrão

#4[redacted]4: Chamado R[redacted]4 aberto!

#4[redacted]1: [Ticket#2024050[redacted]] Seu Chamado foi Resolvido!!!

7. Solicitamos que referências futuras a esta notificação preservem o "Assunto" desta mensagem.

Colocamo-nos à disposição para auxiliá-los no que for necessário.

--
Atenciosamente,

Equipe CTIR Gov <ctir@ctir.gov.br>
www.ctir.gov.br
INOC-DBA (VOIP): 10954*810

##
O Centro de Tratamento de Incidentes de Segurança de Redes de Computadores da Administração Pública Federal - CTIR Gov, subordinado ao Departamento de Segurança da Informação e Comunicações - DSIC, da Casa Militar da Presidência da República, tem como finalidade atender aos incidentes de segurança de redes de computadores da Administração Pública Federal (domínios gov.br, jus.br, leg.br, mil.br e mp.br).
##
CTIR Gov [redacted]

Automatização

Desvantagem na resposta a incidentes

Mensagens que não contribuem

Prezado(a) CTIR Seu chamado n.º R[redacted]64 foi registrado e será tratado pela Central de Serviços.

Descrição:
Requisição de análise de possível incidente de segurança da informação.

Detalhes da descrição:
Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo, CTIR: [redacted]
Email received from: ctir@ctir.gov.br [ctir@ctir.gov.br]
Cc: [redacted]

Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo, CTIR: [redacted]

Automatização

Impactos no processo de resposta a incidentes

Automatização

Impactos no processo de resposta a incidentes

Automatização

O CTIR Gov recomenda automatizar resposta a incidentes?

Atividade Voluntária

Atividade Voluntária

1 - Faça uma consulta ao Whois e verifique se a sua organização possui um contato técnico, se sim, verifique se este é realmente o contato correto, caso contrário solicite a atualização junto ao Registro.br

2 - Verifique na sua organização se o melhor contato em caso de um incidente cibernético está cadastro na base de dados do CTIR Gov, se não, entre em contato com o CTIR e atualize o contato da sua organização.

Obrigado!

Site: www.gov.br/ctir

Notificações: *ctir@ctir.gov.br*

Outros assuntos: *ctirgov@presidencia.gov.br*