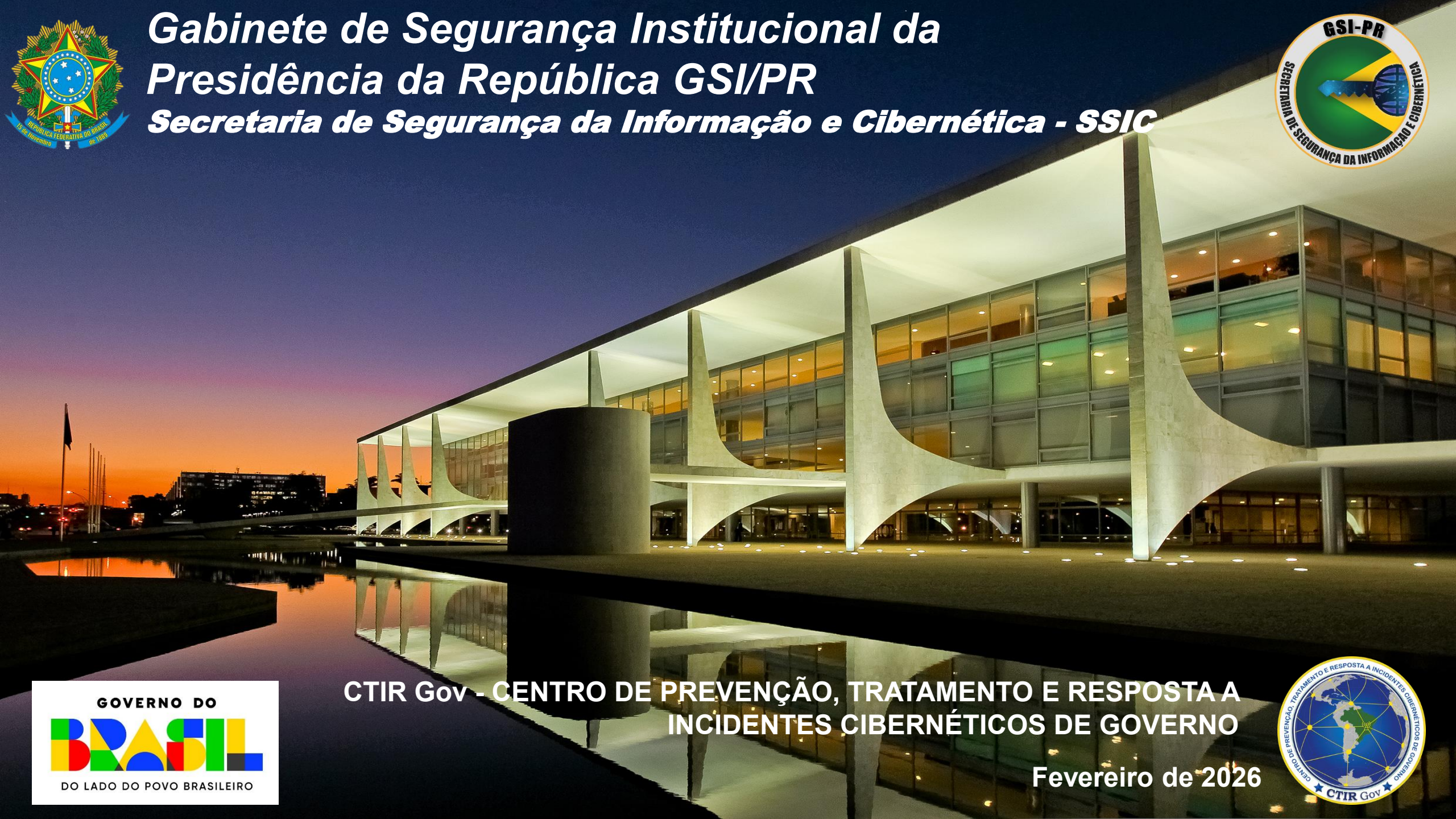
APRESENTAÇÃO DO ROTEIRO	
HORÁRIO	**ATIVIDADE**
10:00 / 10:05	Boas-vindas e Abertura do Webinário
10:05 / 10:30	1 - O CTIR Gov e seu papel 2 - A ReGIC e sua importância
10:30 / 11:15	3 - Divulgação de Informações, alertas e recomendações 4 - O Novo CTIR Em Números 5 - A importância da notificação ao CTIR Gov 6 - Orientações gerais para a melhoria dos processos 7 - Próximos eventos e atividades
11:15 / 11:30	Perguntas e Respostas
11:30	Considerações Finais e Encerramento do Webinário

Gabinete de Segurança Institucional da Presidência da República GSI/PR

Secretaria de Segurança da Informação e Cibernética - SSIC



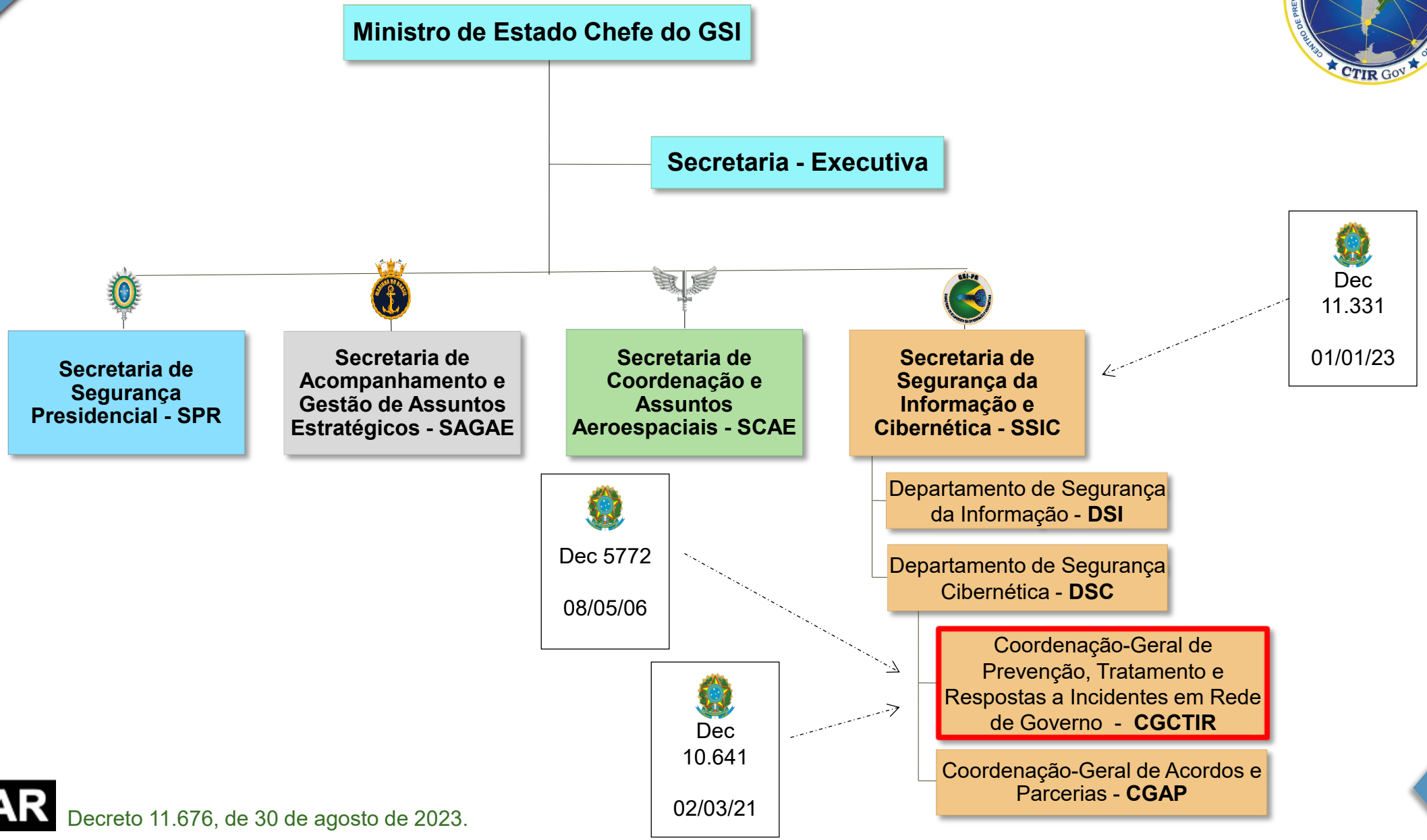
GOVERNO DO BRASIL
DO LADO DO POVO BRASILEIRO

CTIR Gov - CENTRO DE PREVENÇÃO, TRATAMENTO E RESPOSTA A INCIDENTES CIBERNÉTICOS DE GOVERNO

Fevereiro de 2026

CENTRO DE PREVENÇÃO, TRATAMENTO E RESPOSTA A INCIDENTES CIBERNÉTICOS DE GOVERNO (CTIR Gov)

ESTRUTURA ORGANIZACIONAL DO GSI



TLP:CLEAR

Decreto 11.676, de 30 de agosto de 2023.

COMPUTER SECURITY INCIDENT RESPONSE TEAM CSIRT

O que é um **CSIRT** (Computer Security Incident Response Team) ou **ETIR** (Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos) ?

Uma equipe que fornece serviços e suporte, a um grupo definido, para **prevenir**, **lidar** e **responder** a incidentes de segurança cibernética em redes de computadores.

Tipos de times

- CSIRT (Computer Security Incident Response Teams)
  - Interno à organização
  - Coordenação Setorial
  - Coordenação Nacional ⟷ CSIRT de responsabilidade Nacional de Governo
- PSIRT (Product Security Incident Response Teams)
- SOC (Security Operations Centers)
- ISAC (Information Sharing and Analysis Centers)

TLP:CLEAR

FIRST SERVICES FRAMEWORK

SERVICE AREAS

Information Security Incident Management

- Information Security Incident Report Acceptance
- Information Security Incident Analysis
- Artifact and Forensic Evidence Analysis
- Mitigation and Recovery
- Information Security Incident Coordination
- Crisis Management Support

Information Security Event Management

- Monitoring and Detection
- Event Analysis

Vulnerability Management

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

Knowledge Transfer

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

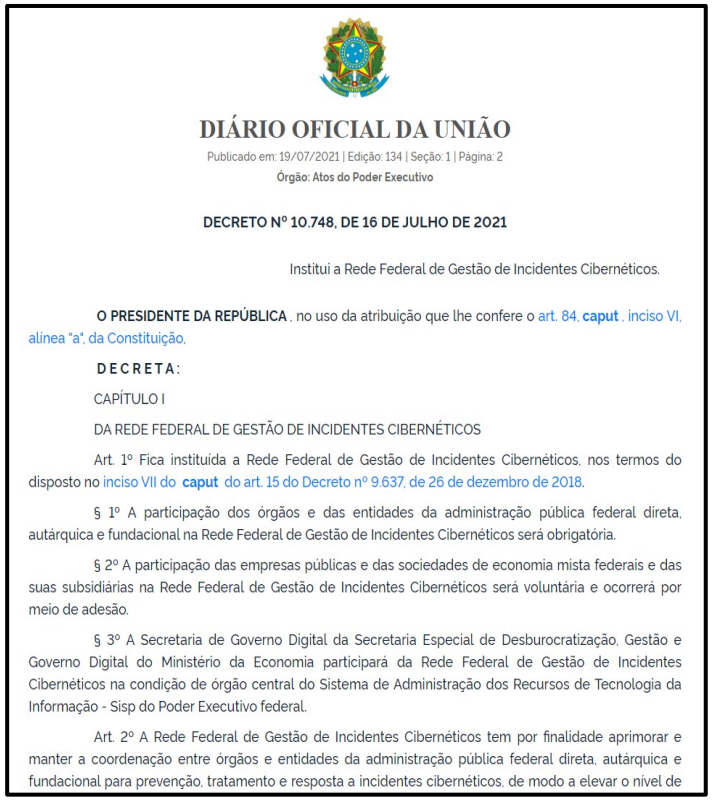
Situational Awareness

- Data Acquisition
- Analysis and Synthesis
- Communication

TLP:CLEAR

Rede Federal de Gestão de Incidentes Cibernéticos – REGIC (Dec. 10.748/21)

REGIC – CRIAÇÃO e CONCEITOS



DIÁRIO OFICIAL DA UNIÃO

Publicado em: 19/07/2021 | Edição: 134 | Seção: 1 | Página: 2

Órgão: Atos do Poder Executivo

DECRETO Nº 10.748, DE 16 DE JULHO DE 2021

Institui a Rede Federal de Gestão de Incidentes Cibernéticos.

O PRESIDENTE DA REPÚBLICA, no uso da atribuição que lhe confere o art. 84, **caput**, inciso VI, alínea "a", da Constituição,

D E C R E T A:

CAPÍTULO I

DA REDE FEDERAL DE GESTÃO DE INCIDENTES CIBERNÉTICOS

Art. 1º Fica instituída a Rede Federal de Gestão de Incidentes Cibernéticos, nos termos do disposto no inciso VII do **caput** do art. 15 do Decreto nº 9.637, de 26 de dezembro de 2018.

§ 1º A participação dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional na Rede Federal de Gestão de Incidentes Cibernéticos será obrigatória.

§ 2º A participação das empresas públicas e das sociedades de economia mista federais e das suas subsidiárias na Rede Federal de Gestão de Incidentes Cibernéticos será voluntária e ocorrerá por meio de adesão.

§ 3º A Secretaria de Governo Digital da Secretaria Especial de Desburocratização, Gestão e Governo Digital do Ministério da Economia participará da Rede Federal de Gestão de Incidentes Cibernéticos na condição de órgão central do Sistema de Administração dos Recursos de Tecnologia da Informação - Sisp do Poder Executivo federal.

Art. 2º A Rede Federal de Gestão de Incidentes Cibernéticos tem por finalidade aprimorar e manter a coordenação entre órgãos e entidades da administração pública federal direta, autárquica e fundacional para prevenção, tratamento e resposta a incidentes cibernéticos, de modo a elevar o nível de

Instituição	• Decreto Nº 10.748, de 16 de julho de 2021
Participação	• Obrigatória (órgãos APF Direta, Autárquica e Fundacional) • Voluntária (empresas públicas e sociedades de economia mista federais) • Convite (Entidades públicas e privadas de interesse do Estado)
Equipes	• ETIR do órgão ou entidade • ETIR de coordenação setorial • CTIR Gov

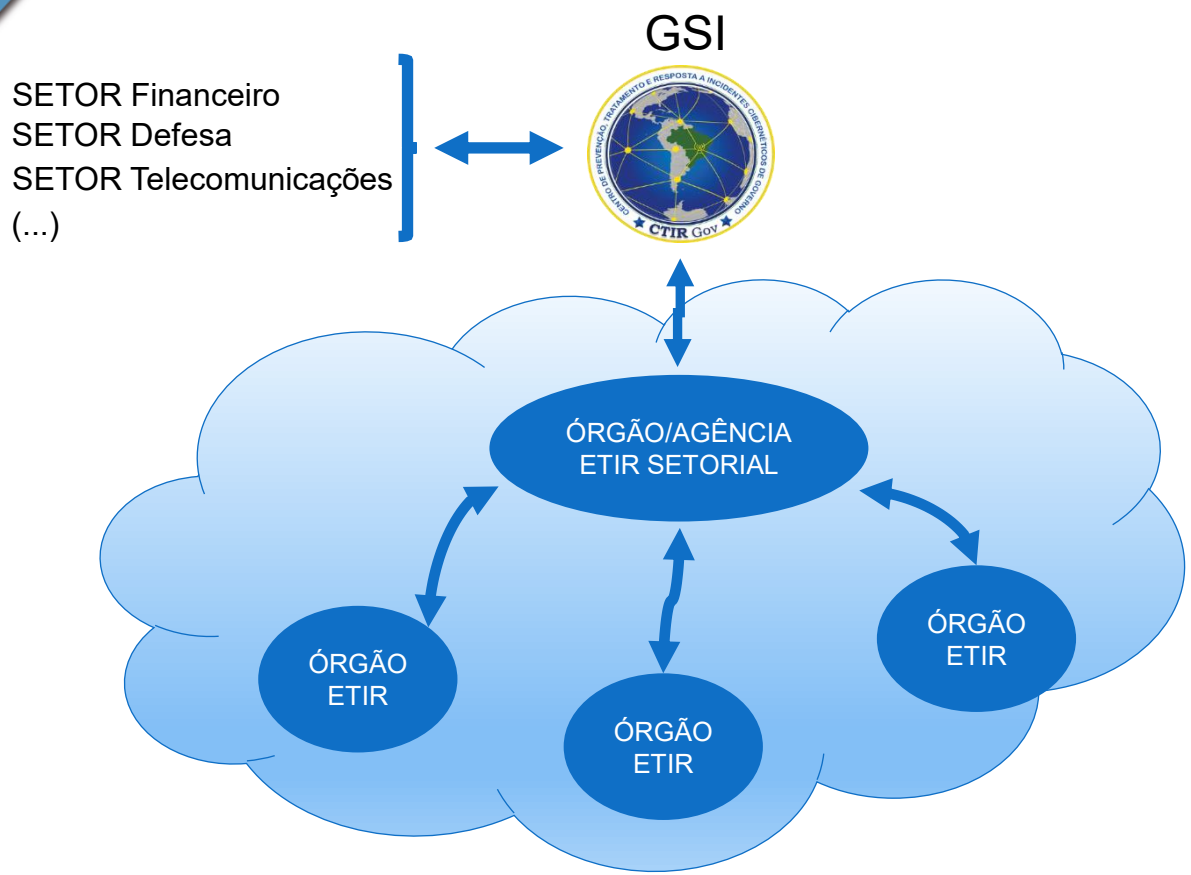
Objetivos:

Elevar o nível de resiliência em Segurança Cibernética

Ratificado pelo TCU via Acórdão Nr 1768/2022 - Plenário

TLP:CLEAR

Decreto 10.748 - REGIC



Art. 10. Compete ao **Gabinete de Segurança Institucional** da Presidência da República:

I - **coordenar** a Rede Federal de Gestão de Incidentes Cibernéticos

Art. 11 – Compete ao DSI/GSI/PR por meio do CTIR Gov:

I – **Coordenar as atividades das ETIRs da REGIC**

II – Articular-se, por meio de plataforma, com as ETIRs

III – **Elaborar, atualizar e divulgar o PLANGIC para órgãos APF**

IV – **Articular-se com órgãos ou unidades correlatos de outros países**

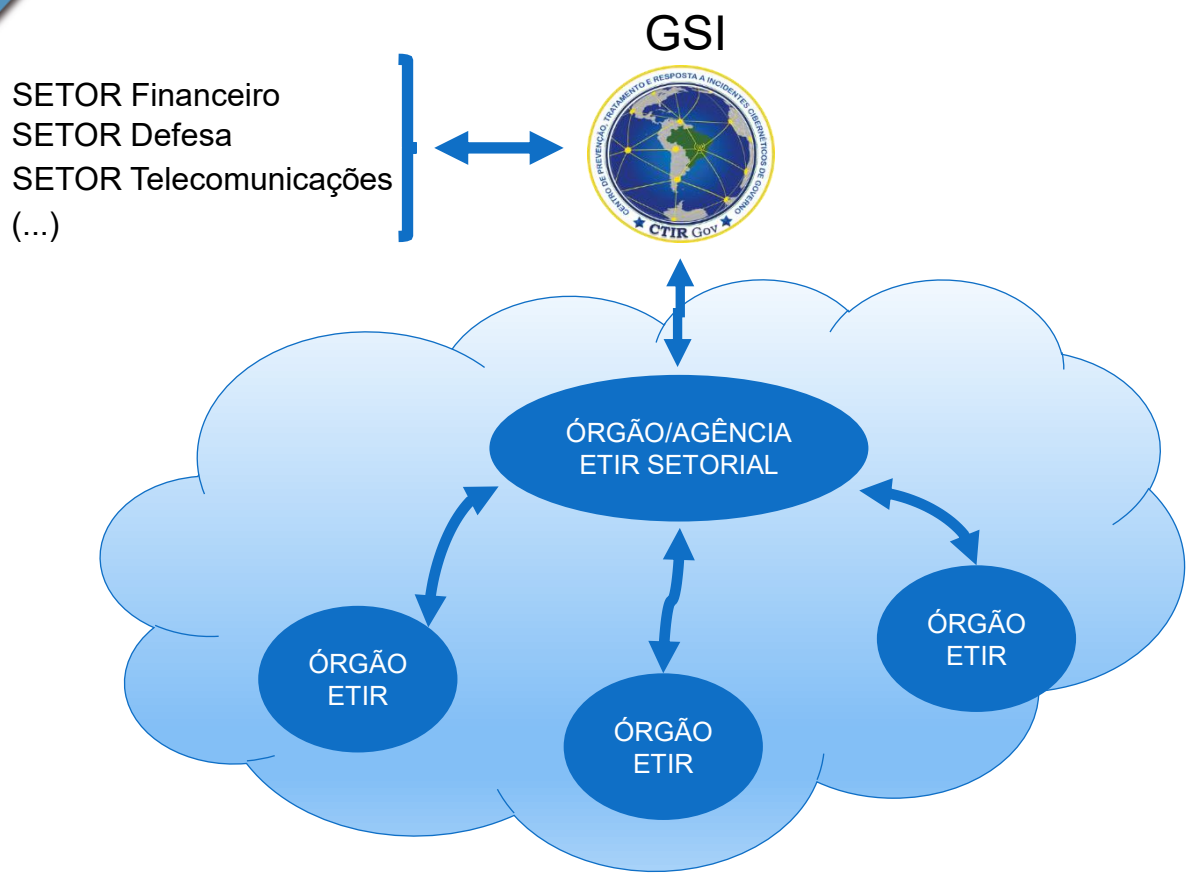
V – Buscar a cooperação internacional, ênfase no compartilhamento

VI – **Difundir alertas, recomendações e estatísticas sobre incidentes**

VII – Manter atualizado o sítio eletrônico do CTIR Gov

REGIC – Principais Competências

Decreto 10.748 - REGIC



Art. 12 – Compete aos órgãos:

I – **Instituir e implementar suas ETIR** nos termos das normas do GSI

II – Apoiar as atividades de suas ETIRs

III – Identificar equipes principais das áreas prioritárias

IV – **Comunicar imediatamente existências de vulnerabilidades ou incidentes que possam impactar os serviços prestados**

V – requerer notificações sobre incidentes de maior impacto

VI **– Notificar Incidentes cibernéticos de maior impacto**

VII - Promover ações de capacitação e profissionalização de suas ETIRs

VIII - Manter atualizada a infraestrutura utilizada por suasETIRs

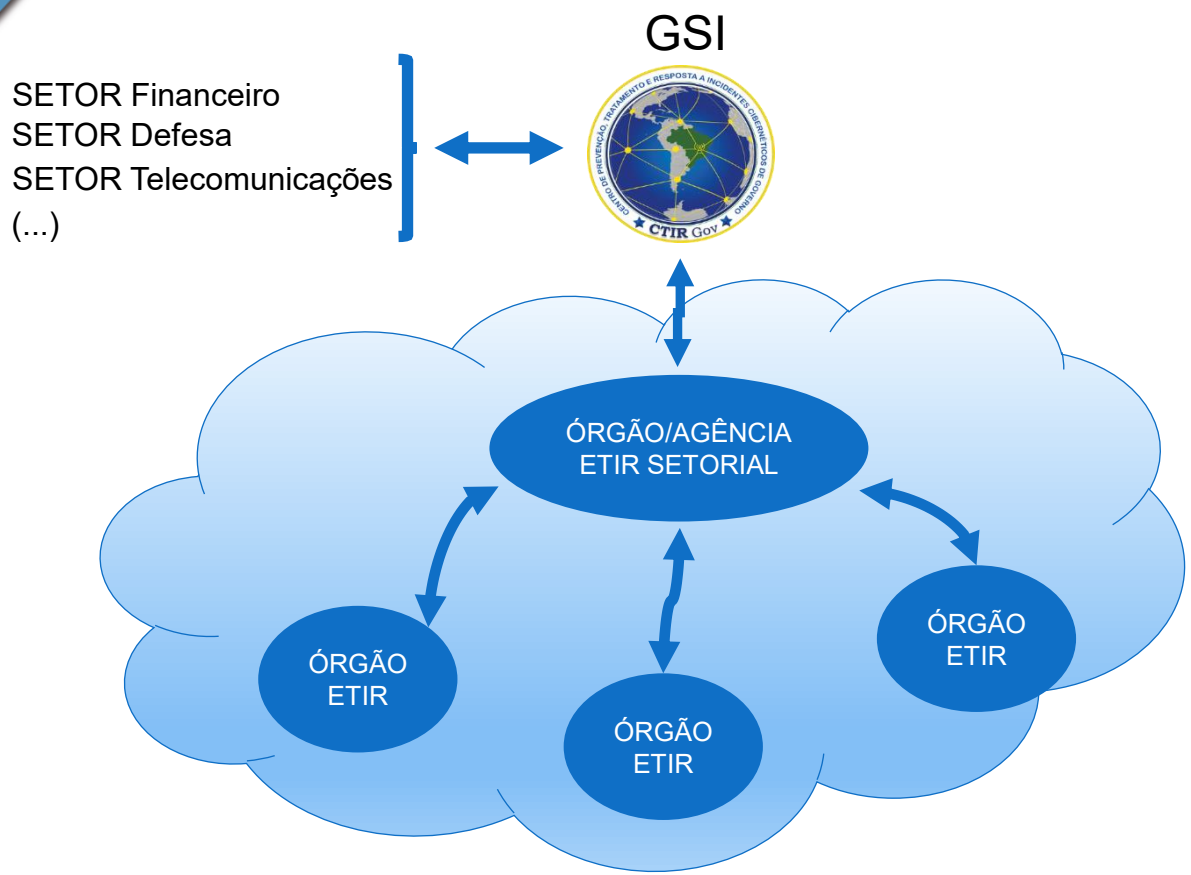
IX – **Sanar, com urgência, vulnerabilidades cibernéticas, em especial aquelas identificadas nos alertas e recomendações**

§ 1º Os incidentes cibernéticos de maior impacto serão estabelecidos com base na classificação de severidade que consta do processo de gestão de riscos de segurança da informação do órgão

TLP:CLEAR

REGIC – Principais Competências

Decreto 10.748 - REGIC



Art. 13 – Compete às agências reguladoras (...) BACEN e CNEN:

I - **Instituir ou designar ETIR de coordenação setorial**

II – Apoiar as atividades de suas ETIRs

III - Identificar equipes principais das áreas prioritárias

IV – Requerer notificações sobre incidentes de maior impacto

V – **Notificar Incidentes cibernéticos de maior impacto**

VI – **analisar os riscos cibernéticos que deverão constar no Plano setorial de gestão de incidentes cibernéticos específico**

VII – Estabelecer a sua forma de articulação com a ETIR setorial

VIII - Identificar outras entidades, públicas ou privadas, relevantes

IX – Fornecer informações relativas às ETIRs das entidades item VIII

X – **Identificar infraestruturas críticas de suas áreas prioritárias**

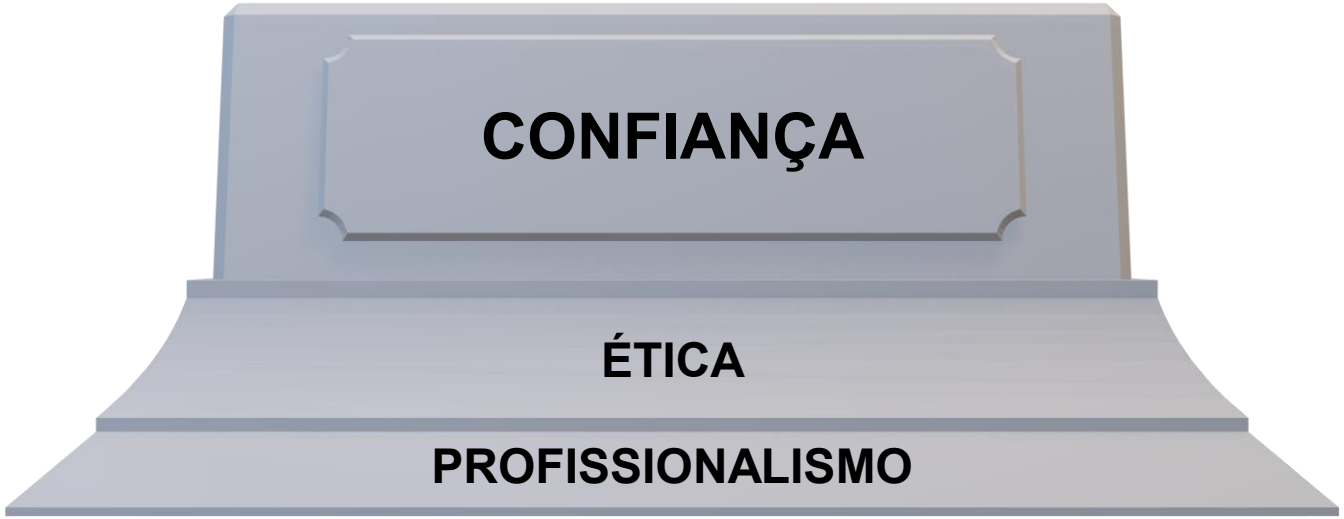
Art. 14 – Compete às equipes de coordenação setoriais:

I – **elaborar o plano setorial de gestão de incidentes cibernéticos**

II – **coordenar as atividades e centralizar as notificações**

TLP:CLEAR

VALORES NO COMPARTILHAMENTO DE INFORMAÇÕES



TLP:CLEAR

Importância da REGIC

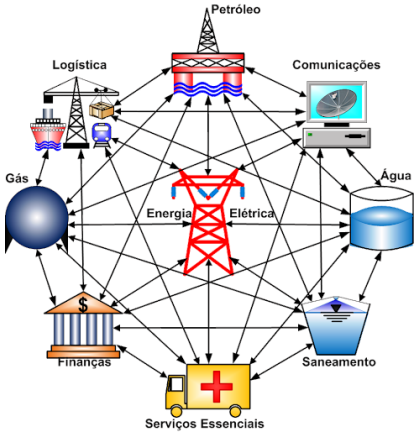
1. Compartilhamento de vulnerabilidades e IoCs

2. Resposta coordenada em caso de incidentes

3. Apoio mútuo na cibersegurança nacional

Sejam embaixadores da REGIC !

REGIC



(COLABORAÇÃO)

TLP:CLEAR

ISAC - (Information Sharing and Analysis Center)

TLP:CLEAR

DIÁRIO OFICIAL DA UNIÃO

Publicado em: 09/04/2025 | Edição: 68 | Seção: 1 | Página: 2

Órgão: Presidência da República/Gabinete de Segurança Institucional

PORTARIA GSI/PR Nº 148, DE 8 DE ABRIL DE 2025

Institui a Diretriz de Estímulo à Criação e Operação de Centros de Análise e Compartilhamento de Informações (*Information Sharing and Analysis Centers*).

- Estímulo à criação de ISACs
- Operacionalização da adesão à REGIC
- Promoção de seminários, treinamentos e outras atividades

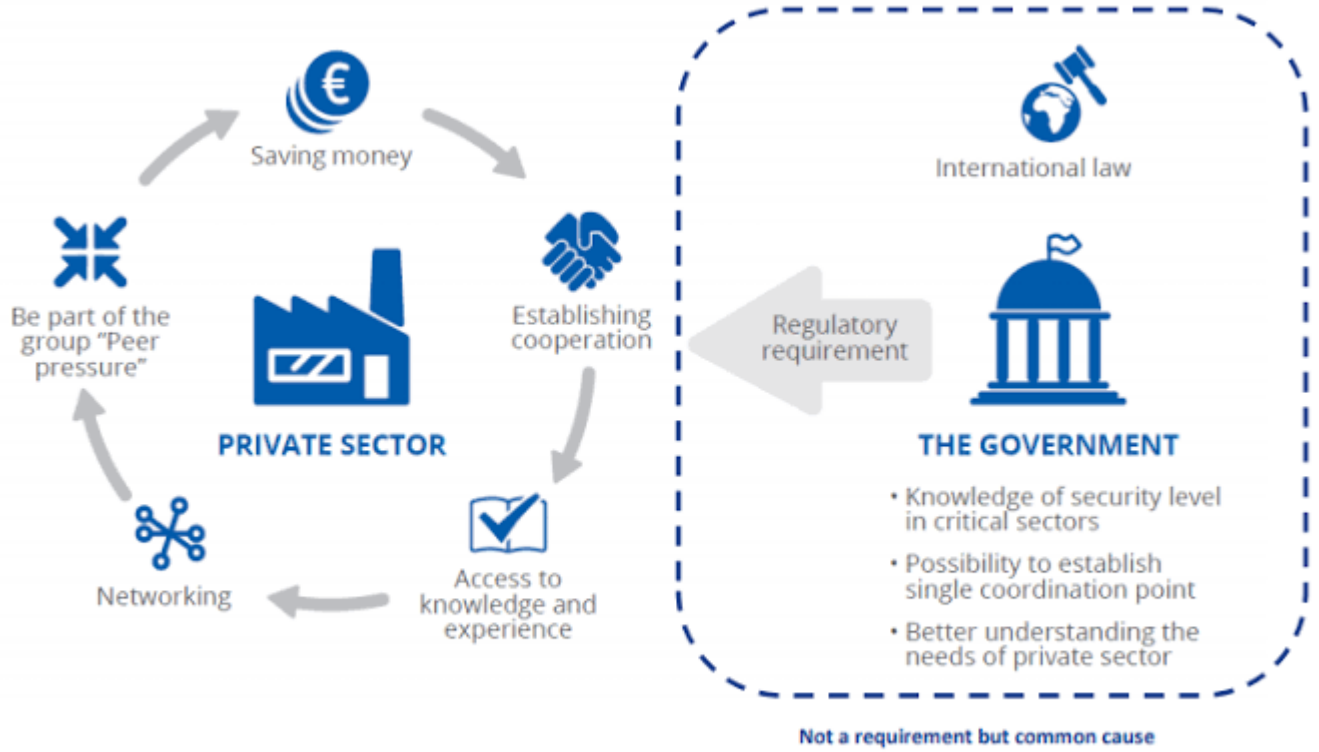


Figure 1: Reasons for the creation of ISACs

TLP:CLEAR

INFORMAÇÕES E ORIENTAÇÕES GERAIS

CTIR GOV - SITE

https://www.gov.br/ctir

Contato Operacional / Operational Contact

- Orientações para Notificação de Incidentes Cibernéticos ao CTIR Gov
- Comunicação de Incidentes de Rede
- Network Incident Reporting
- Comunicación de Incidentes en la Red

Últimos Alertas e Recomendações

Alertas

ALERTA 09/2025
Vulnerabilidades no recurso "Airplay" em produtos Apple

ALERTA 08/2025
Pós-exploração de vulnerabilidades conhecidas em produtos Fortinet

ALERTA 07/2025
Vulnerabilidade crítica no produto FortiSwitch

Recomendações

RECOMENDAÇÃO 03/2025
Estratégias para minimizar o impacto de ataques DDoS

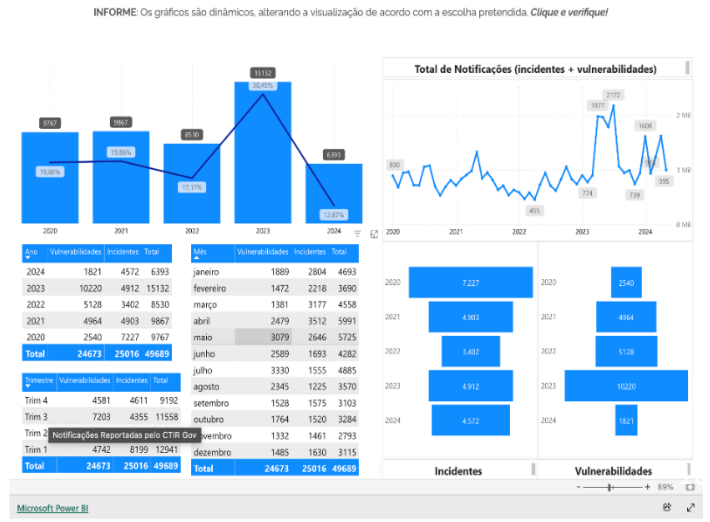
RECOMENDAÇÃO 01/2025
Orientações sobre campanhas de conscientização

RECOMENDAÇÃO 02/2025
Atenção com artefatos maliciosos utilizando a temática "IRPF"

Base Normativa

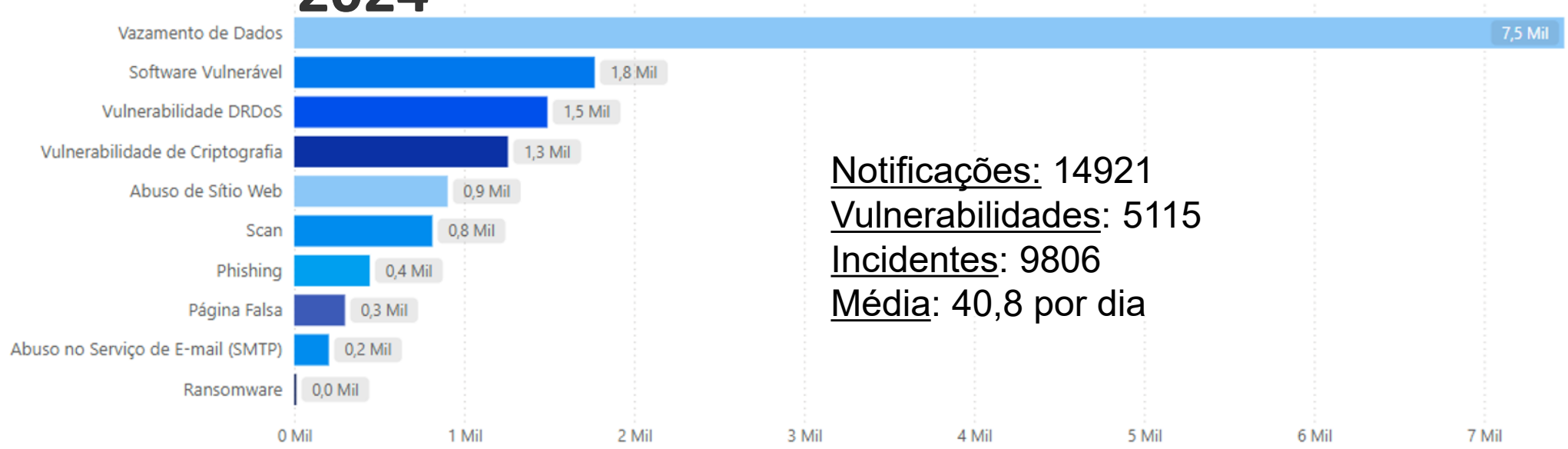
- Instrução Normativa GSI Nº 1, de 27 de maio de 2020
- Norma Complementar nº 05/IN01/DSIC/GSIPR
- Norma Complementar nº 08/IN01/DSIC/GSIPR
- Norma Complementar nº 21/IN01/DSIC/GSIPR

Notificações Reportadas pelo CTIR Gov - 2020 a 2024



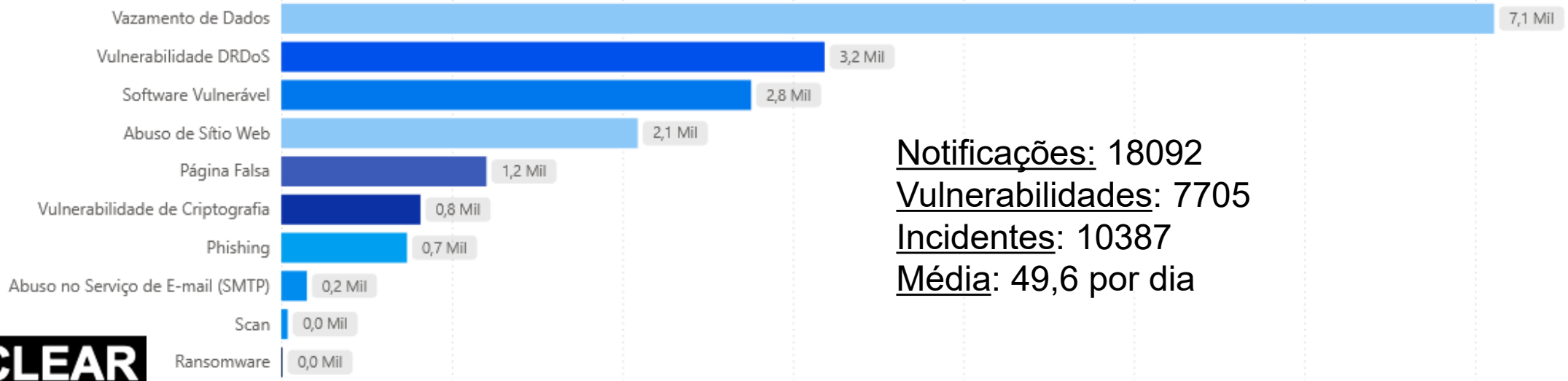
CTIR Gov Em Números

2024



Notificações: 14921
Vulnerabilidades: 5115
Incidentes: 9806
Média: 40,8 por dia

2025



Notificações: 18092
Vulnerabilidades: 7705
Incidentes: 10387
Média: 49,6 por dia

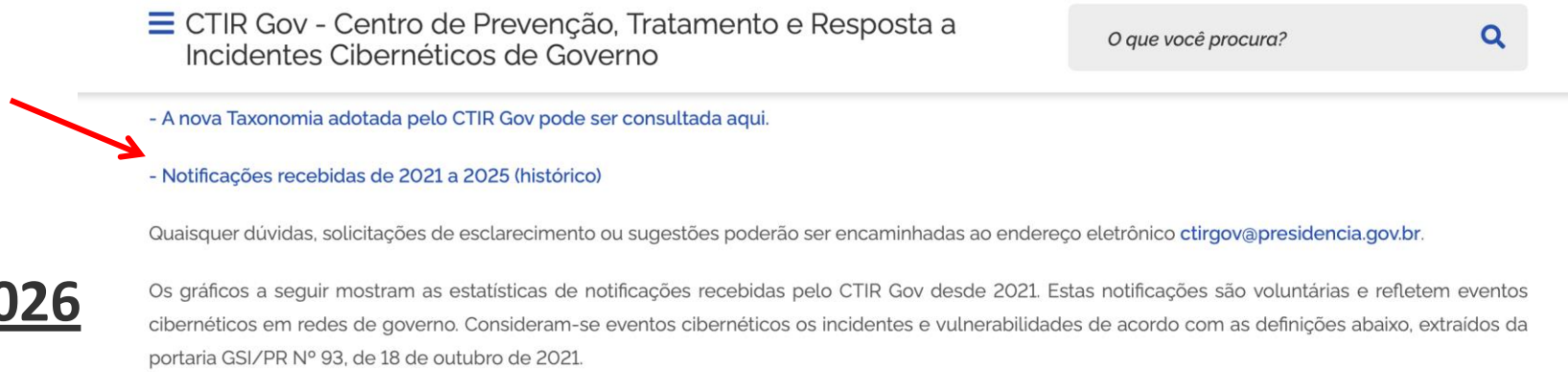
TLP:CLEAR

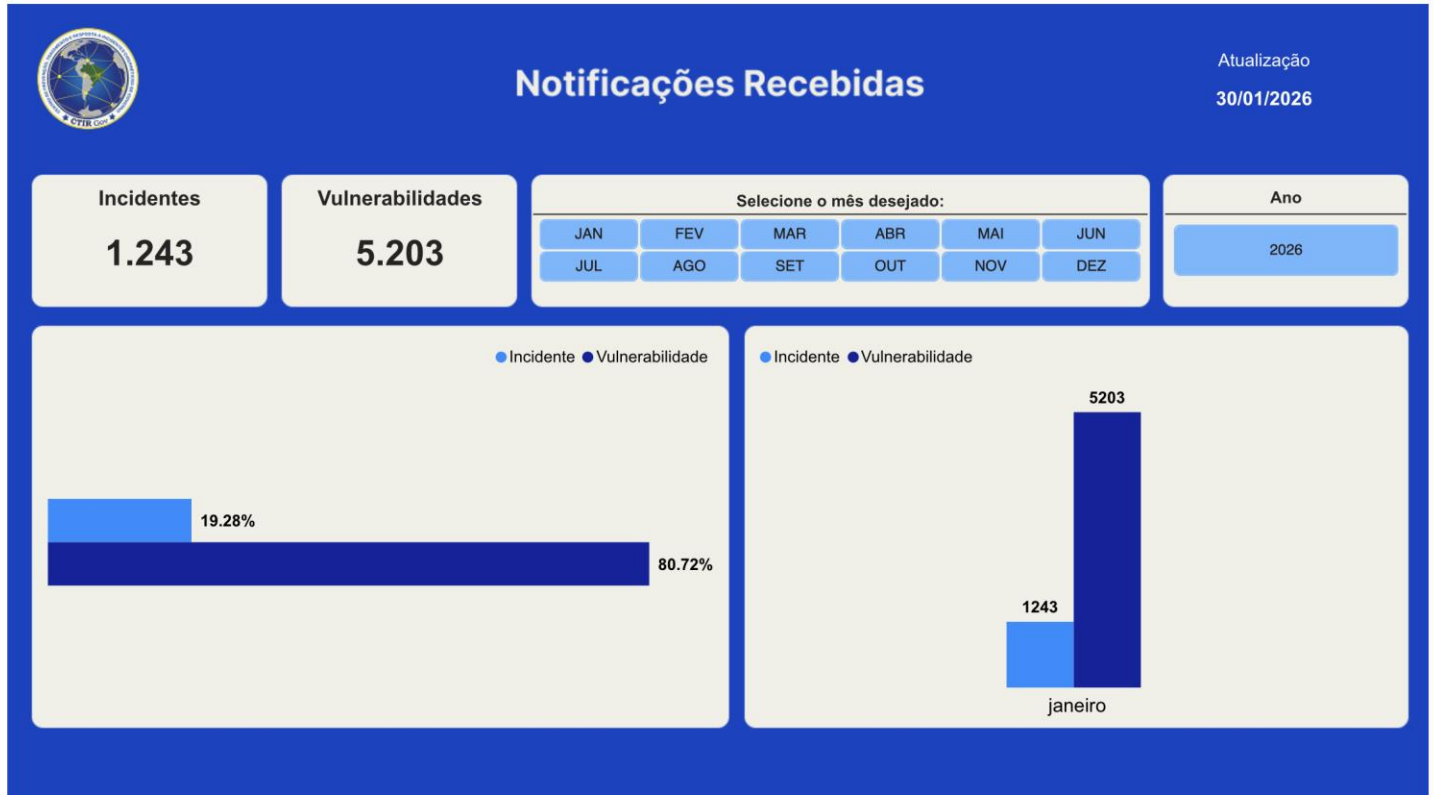
CTIR Gov Em Números

CTIR Gov em Números 2026

- ✓ Nova Taxonomia;
- ✓ Mudanças nas ferramentas; e
- ✓ Automações.

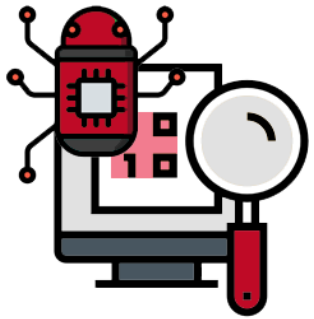
https://www.gov.br/ctir/pt-br/assuntos/em_numeros_2026





TLP:CLEAR

NOTIFICAÇÃO AO CTIR GOV



Comunicação de Incidentes de Rede

Instruções básicas de como notificações de incidentes cibernéticos devem ser enviados ao CTIR Gov.

Publicado em 06/10/2021 18h02 | Atualizado em 30/05/2025 17h34 Compartilhe:

O Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo - CTIR Gov, atende por meio do e-mail: ctir@ctir.gov.br.

INOC-DBA BR: 266031*800 (https://inoc.nic.br/)

Para comunicação através de um canal seguro, por favor utilize a seguinte **chave PGP**:
PGP - CTIR Gov

KeyID: 9F40DFC1 e **Fingerprint**: 9C8E 8DAD 3D81 AF7A C499 F2C2 74B4 F080 9F40 DFC1

Procedimento para comunicação de ocorrência de incidentes de rede:

A comunicação entre os órgãos e instituições da APF e o CTIR Gov deve ocorrer através das ETIR ou por pessoas com esta atribuição, de forma centralizada, preferencialmente por meio de conta de e-mail institucional relacionada a incidentes de segurança, por sugestão: etir@orgao.gov.br.

O ponto único de contato para as notificações de incidentes cibernéticos ao CTIR Gov é o endereço eletrônico: ctir@ctir.gov.br.

Deve-se fazer constar no assunto da notificação o "nome do órgão" e o "tipo do incidente".

A mensagem deve, preferencialmente, seguir as: Orientações para Notificação de Incidentes de Segurança de Rede ao CTIR Gov.

✓ https://www.gov.br/ctir/pt-br/canais_atendimento/comunicacao-de-incidentes-de-rede

NOTIFICAÇÃO AO CTIR GOV

Confiança e Trabalho Conjunto

- ✓ **Desafios em 2026**
- ✓ **Ameaças com IA**
- ✓ **Falta de RH**

TLP:CLEAR

EVENTOS, CAPACITAÇÕES E ATIVIDADES

- ✓ TTX resposta à incidentes
- ✓ Treinamento Teórico-Prático
- ✓ Webinários
- ✓ Encontro de ETIRs Setoriais
- ✓ Colóquios Técnicos para a REGIC
- ✓ Caravanas Federativas

TLP:CLEAR

SAVE THE DATE

- ✓ 2º Webinário (24 e 26/Março): Detecção de ameaças e resposta a incidentes usando serviços nativos de nuvem (Parceria com a AWS)

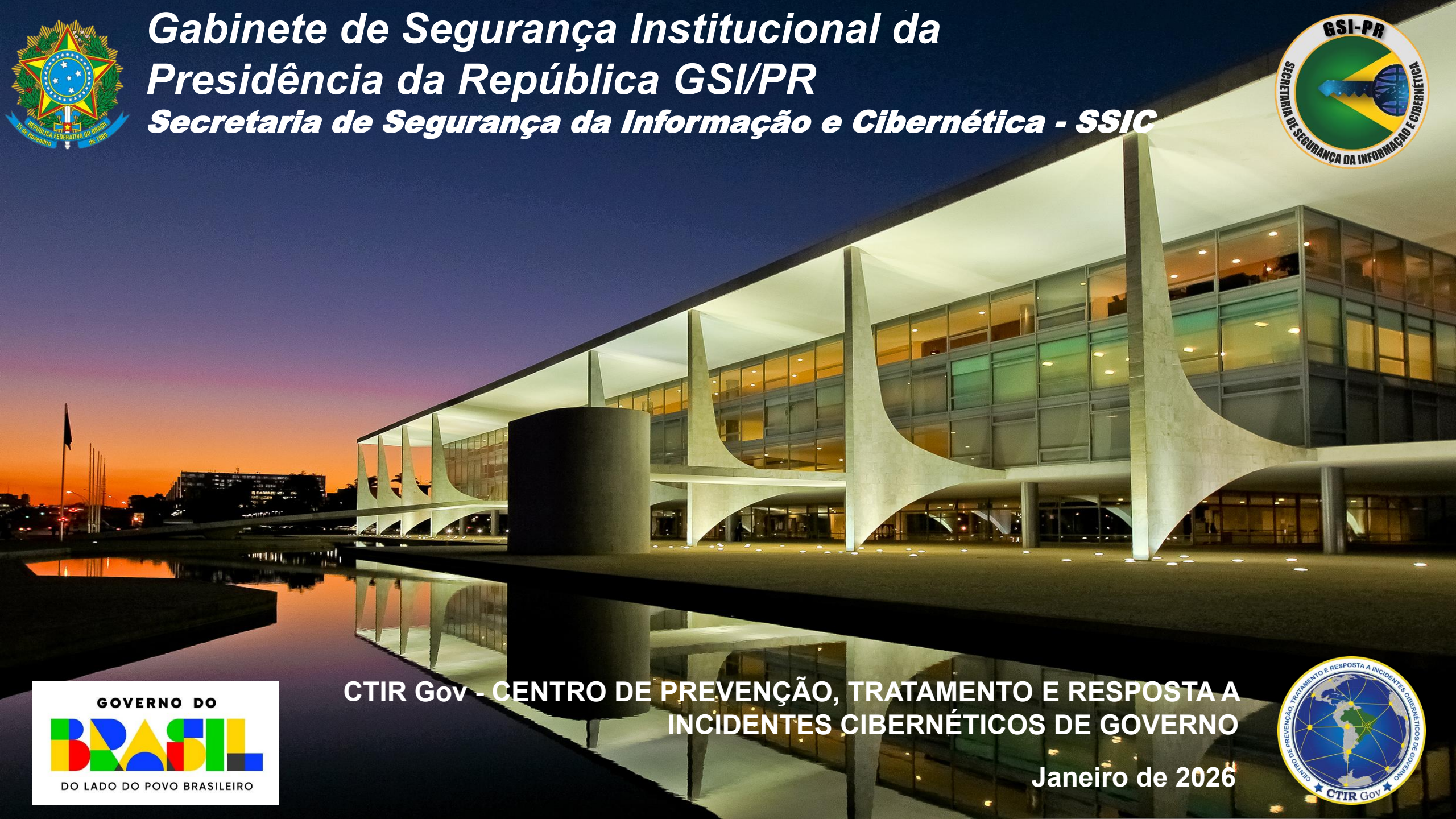
- ✓ 3º Webinário (prev. 29/Abr): Uso do MISP (Parceria com o CESAR School)

ATENÇÃO: É necessário o preenchimento dos formulários de inscrição para cada evento. Divulgação do link apenas internamente à organização !

TLP:CLEAR

Muito obrigado!

JUNIER CAMINHA AMORIM
Coronel (EB)
Coordenador-Geral
junier@presidencia.gov.br
ctirgov@presidencia.gov.br



Gabinete de Segurança Institucional da Presidência da República GSI/PR

Secretaria de Segurança da Informação e Cibernética - SSIC

GOVERNO DO BRASIL
DO LADO DO POVO BRASILEIRO

CTIR Gov - CENTRO DE PREVENÇÃO, TRATAMENTO E RESPOSTA A INCIDENTES CIBERNÉTICOS DE GOVERNO

Janeiro de 2026