GABINETE DE SEGURANÇA INSTITUCIONAL DA PRESIDÊNCIA DA REPÚBLICA

Assessoria Especial de Segurança da Informação

Departamento de Segurança da Informação

Rede Federal de Gestão de Incidentes Cibernéticos

Decreto nº 10.748, de 16/07/2021

Preâmbulo

2004: por proposta do Comitê Gestor de Segurança da Informação (CGSI), o GSI/PR cria o Centro Tratamento de Incidentes de Segurança em Redes de Computadores (CTIR Gov).

2006: criação do Departamento de Segurança da Informação e Comunicações – DSIC, no GSI/PR, ao qual passa a vincular-se o CTIR Gov (Dec. nº 5.772/2018).

2009: NC nº 05/IN01/DSI/GSIPR disciplina a criação de equipes de tratamento e resposta a incidentes em redes computacionais (ETIR) nos órgãos e entidades da APF.

2012: Acórdão nº 1233/2012-TCU-Plenário dispõe que a observância às normas do GSI/PR é obrigação da alta administração dos órgãos e entidades da APF.

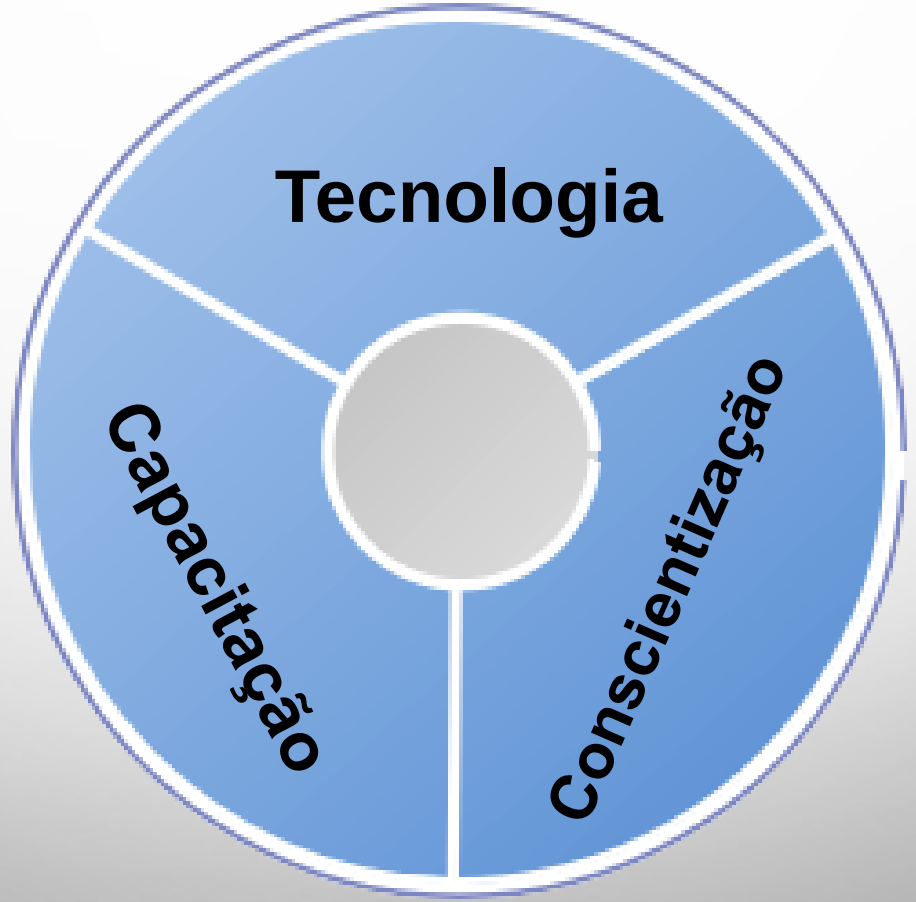
2018: instituição da Política Nacional de Segurança da Informação (PNSI), que positiva a composição da rede de equipes da APF coordenada pelo CTIR Gov (Dec. nº 9.637/2018).

2020: criação da Assessoria Especial de Segurança da Informação (AssESI), como órgão de assistência direta e imediata ao Ministro do GSI/PR, e designação Departamento de Segurança da Informação (DSI) como órgão específico singular (Dec. nº 10.363/2020).

2021: alteração da denominação do CTIR Gov para “Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo” e de ETIR para “equipe de prevenção, tratamento e resposta a incidentes cibernéticos” (Dec. nº 10.641/2021).

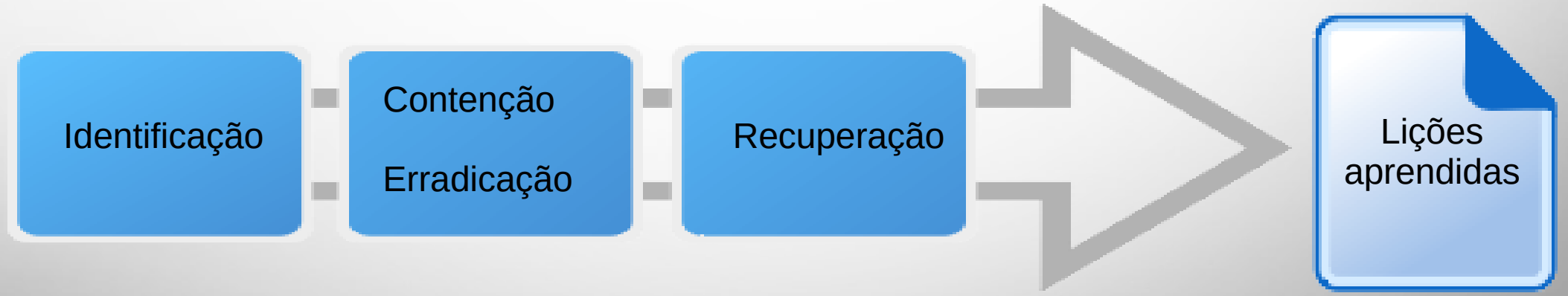
2021: instituição da Rede Federal de Gestão de Incidentes Cibernéticos (ReGIC), com definição de sua composição e governança (Dec. nº 10.748/2021).

Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo



Comunicar para Educar

Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo



Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo

Parceria

Cooperação

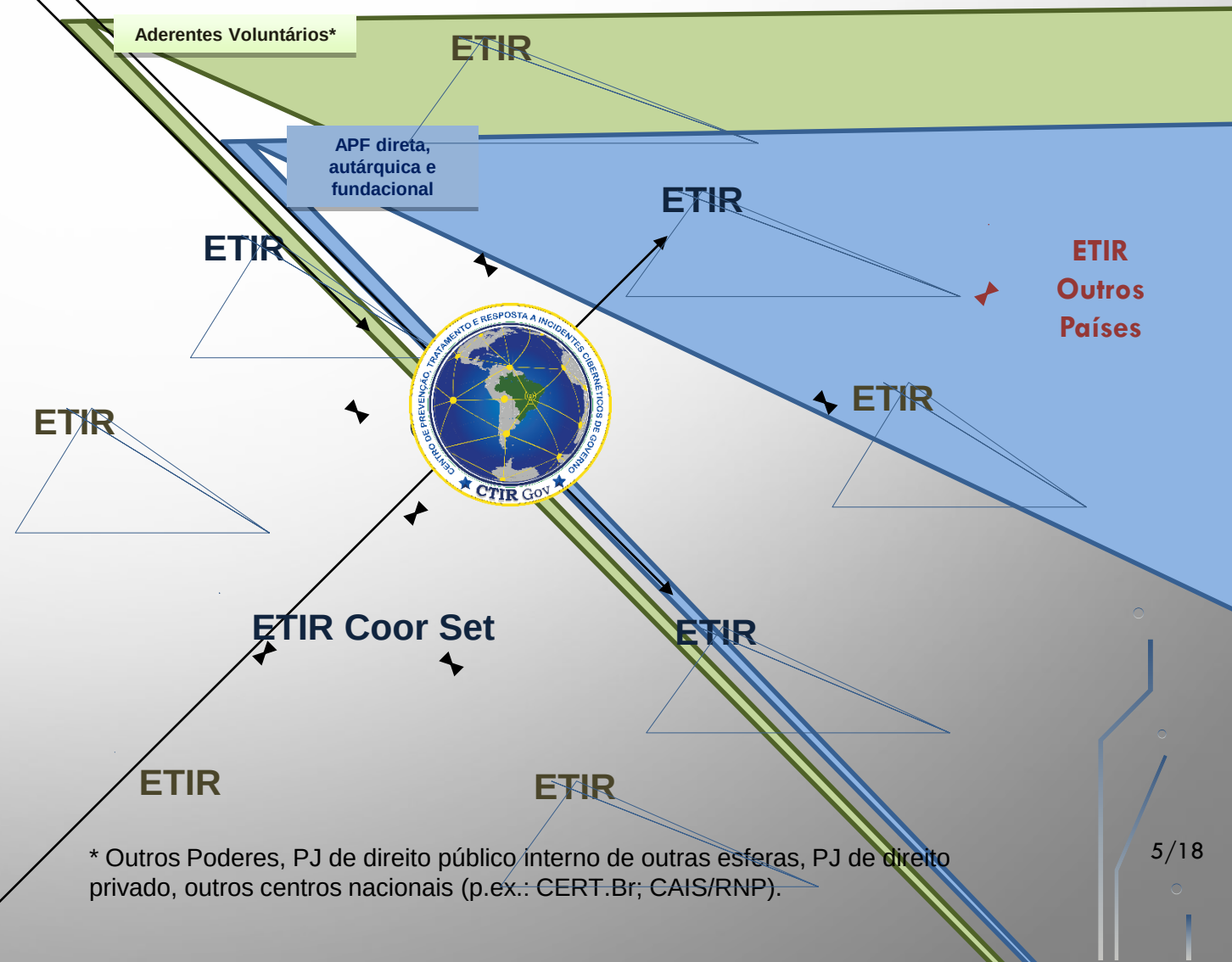
Visão geral da ReGIC

- **Rede de Gestão de Incidentes Cibernéticos**

  (Decreto nº 10.748, de 16/07/2021):

  - Composição
  - Conceitos
  - Coordenação Setorial
  - Competências

- Plano Nacional de Gestão de Incidentes Cibernéticos – PLANGIC



* Outros Poderes, PJ de direito público interno de outras esferas, PJ de direito privado, outros centros nacionais (p.ex.: CERT.Br; CAIS/RNP).

Finalidade e objetivos

Finalidade da ReGIC (art. 2º):

"... 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 resiliência em segurança cibernética de seus ativos de informação."

Objetivos da ReGIC (art. 3º):

- divulgar medidas de prevenção, tratamento e resposta a incidentes cibernéticos;
- compartilhar alertas sobre ameaças e vulnerabilidades cibernéticas;
- divulgar informações sobre ataques cibernéticos;
- promover a cooperação entre os seus participantes; e
- promover a celeridade na resposta a incidentes cibernéticos.

... novos planos

plano de gestão de incidentes cibernéticos para a administração pública federal (art. 4º, VI):

> *"... plano que **orienta as equipes dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional**, exceto das agências reguladoras, do Banco Central do Brasil e da Comissão Nacional de Energia Nuclear, sobre a coordenação de atividades referentes à prevenção, ao tratamento e à resposta a incidentes cibernéticos; e"*

planos setoriais de gestão de incidentes cibernéticos (art. 4º, VII):

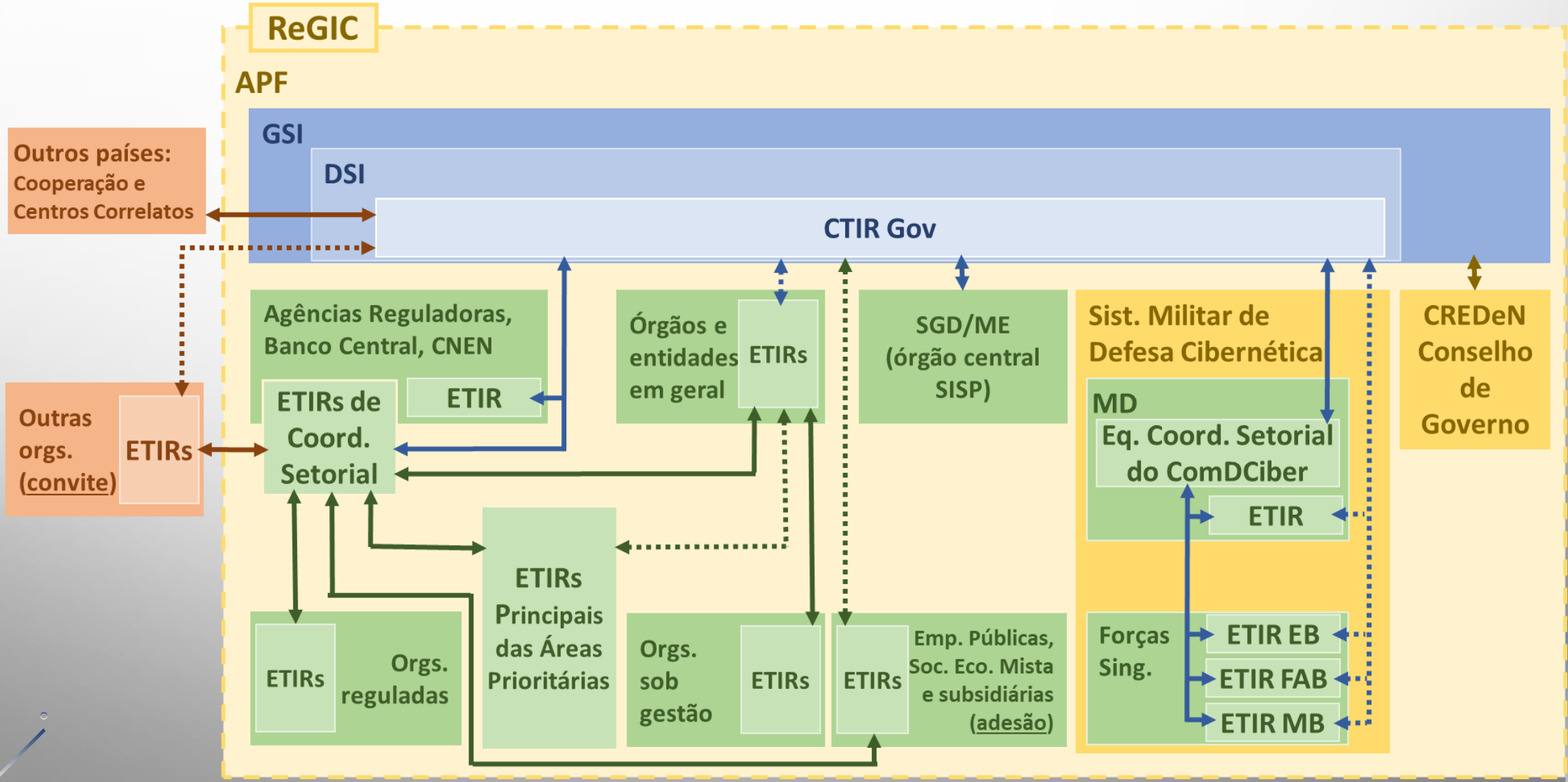
> *"... planos que **orientam as equipes nas agências reguladoras**, no **Banco Central do Brasil**, na **Comissão Nacional de Energia Nuclear** ou nas suas **entidades reguladas** sobre a coordenação de atividades referentes à prevenção, ao tratamento e à resposta a incidentes cibernéticos inerentes ao setor específico."*

Pessoas jurídicas convidadas

PJ convidadas (art. 8º):

- se reportarão à respectiva equipe de coordenação setorial ou, se inexistente, diretamente ao CTIR Gov (*caput*);
  - p.ex.: o BRB é sociedade de economia mista majoritariamente do GDF, sob regulação do Bacen, então, se convidado para a ReGIC, deverá se reportar à equipe instituída pelo Bacen ou, se inexistente, diretamente ao CTIR Gov;
- deverão reportar ao CTIR Gov (*caput*):
  - incidente cibernético que extrapole a sua capacidade de saná-lo; e
  - vulnerabilidade em ativos de informação que a sua ETIR julgue que possa causar incidente cibernético, em sua rede computacional ou em outras.
- a saída dessas PJ da ReGIC ocorrerá a pedido de seu dirigente máximo ou por decisão do GSI/PR, na hipótese de (art. 9º) :
  - ☒ descumprimento dos requisitos de que trata o art. 7º;
  - ☒ descumprimento do disposto no plano setorial; ou
  - ☒ conveniência administrativa.

Rede Federal de Gestão de Incidentes Cibernéticos (Decreto nº 10.748/2021)



Competências

(art. 12)

Órgãos e entidades da APF direta, autárquica e fundacional e órgãos reguladores:

- instituir e implementar as suas ETIRs, cfe. Dec. nº 9.637/2018 **e** normas do GSI/PR;
- apoiar suas ETIRs e ações de segurança da informação cfe. Dec. nº 9.637/2018, art. 15;
- identificar as equipes principais das áreas prioritárias sob a sua responsabilidade;
- comunicar imediatamente o CTIR Gov, por meio de suas ETIRs, sobre a existência de vulnerabilidades ou incidentes de segurança cibernética que impactem ou que possam impactar os serviços prestados ou contratados, cfe. Dec. nº 9.637/2018, art. 17;
- requerer diretamente às equipes principais, ou pela equipe de coordenação setorial, se instituída, as notificações sobre os **incidentes cibernéticos de maior impacto**;
- **notificar o CTIR Gov**, diretamente ou pela equipe de coordenação setorial, se instituída, quanto aos **incidentes cibernéticos de maior impacto**, com base nas informações obtidas das ETIRs das entidades sob a sua gestão;
- ações de capacitação e profissionalização de suas ETIRs, cfe. Dec. nº 9.637/2018, art. 15;
- manter atualizada a infraestrutura utilizada por suas ETIRs; e
- **sanar, com urgência, as vulnerabilidades cibernéticas**, em especial aquelas identificadas nos alertas e nas recomendações expedidos pelo CTIR Gov.

Incidentes cibernéticos de maior impacto: estabelecidos com base na classificação de severidade de seu processo de gestão de riscos de segurança da informação.

Competências

Agências reguladoras, Bacen e CNEN (art. 13) – parte 2 de 2:

- **incidentes cibernéticos de maior impacto**: estabelecidos com base na classificação de severidade de seu processo de gestão de riscos de segurança da informação (§1º);
- **plano setorial de gestão de incidentes cibernéticos**: CTIR Gov divulgará os elementos básicos e a periodicidade de atualização em seu sítio eletrônico (§2º);
- o disposto no art. 13 **aplica-se também a outros órgãos e entidades da APF direta, autárquica e fundacional com competência de regulação em área prioritária** que venha a ser estabelecida no PNSIC, no prazo de até 18 meses, contado da data de notificação pelo GSI/PR, para que o órgão ou a entidade implemente as ações necessárias (§3º).

Competências

Equipes de coordenação setorial (art. 14):

- elaborar o plano setorial de gestão de incidentes cibernéticos;
- coordenar as atividades e centralizar as notificações de incidentes recebidas das demais ETIRs das entidades sob a sua coordenação; e
- obedecer ao disposto nas normas de segurança da informação estabelecidas pelo GSI/PR que dispõem sobre ETIRs.

Prazos aos participantes da ReGIC

- as ações previstas para o funcionamento da ReGIC a cargo das agências reguladoras, Bacen e CNEN que incluam a instituição ou a designação das equipes de coordenação setorial deverão ser implementadas em 18 meses da publicação do Decreto (art. 16);

- os órgãos e as entidades da APF direta, autárquica e fundacional deverão implementar as ações previstas para o funcionamento da ReGIC em 1 ano da publicação do Decreto; e

- Decreto entra em vigor na data de sua publicação (art. 18).

Grato pela cooperação e parceria!

ULISSES Peixoto Pinto Neto
Assessor Técnico
Centro de Prevenção e Tratamento de Incidentes de Rede de Governo
Departamento de Segurança da Informação
(61) 3411-2728
contato@ctir.gov.br