ITAIPU BINACIONAL

Desafios dos Controles CIS e ISO/IEC 27001

11º Fórum Brasileiro de CSIRTs

20 anos cert.br

2023

31 de Julho

TLP:CLEAR

Aviso

Esta é uma apresentação baseada nas documentações existentes e experiencias vividas

Não represento, tampouco falo em nome da CIS, da ISO, do NIST; entre os outros órgãos nomeados nesta apresentação.

TLP:CLEAR

Objetivos

- Visão geral sobre ISO 27001
- Informações gerais sobre Controles CIS
- Aprendizados e Desafios do uso no dia-a-dia
- O que nos espera no futuro

Agenda

- **Itaipu e o Setor Elétrico**
- ISO/IEC 27001
- Controles CIS
- Implementação e Desafios
- Conclusões

Foto: Nilton Quoirin

TLP:CLEAR

Itaipu Binacional

Foto: Alexandre Marchetti


ITAIPU
BINACIONAL

TLP:CLEAR

Tratado de Itaipu (1973)

- **Criam em igualdade de direitos e obrigações entidade binacional ITAIPU**

  ITAIPU constituída por ELETROBRAS
  (sucedida pela ENBPar em 17.jun.22)
  e ANDE com igual participação no capital

- **Altas Partes outorgam concessão à ITAIPU para realizar o aproveitamento hidrelétrico**

Tratado, Anexos e Notas Reversais

BINACIONALIDADE

Empresa **una e indivisível** instalada 17 maio 1974

COGESTÃO

Igual número brasileiros e paraguaios **órgãos de gestão**

PARIDADE

Decisões **conjuntas e paritárias** (consenso)

TRATADO DE ITAIPU

- Aprovado Congressos BR e PY
- Promulgado 28 agosto 1973

ANEXOS

- Anexo A - Estatuto da ITAIPU
- Anexo B - Instalações
- Anexo C - Bases Financeiras

NOTAS REVERSAIS

- Notas entre MRE do BR e PY
- Assuntos específicos

TLP:CLEAR

Governança da ITAIPU

ITAIPU BINACIONAL

Conselho de Administração → 12+2 Representantes Altas Partes

- 6 Conselheiros nomeados pelo Governo do Brasil
- 6 Conselheiros nomeados pelo Governo do Paraguai

Diretoria Executiva → 12 Diretores

- Diretor-Geral Brasileiro
- Diretor-Geral Paraguaio

Diretores

- Diretores Técnicos
- Diretores Financeiros
- Diretores de Coordenação
- Diretores Administrativos
- Diretores Jurídicos

TLP:CLEAR

Operação Unidades Geradoras

ITAIPU BINACIONAL

TLP:CLEAR

Missão e Visão:
Energia e Sustentabilidade

ITAIPU BINACIONAL

MISSÃO: Gerar energia elétrica de qualidade com responsabilidade social e ambiental, contribuindo com o desenvolvimento sustentável no Brasil e no Paraguai

VISÃO: Ser uma Entidade binacional moderna, colaborativa e comprometida com a integração regional, reconhecida pela excelência na geração de energia limpa e renovável e pela sua contribuição ao desenvolvimento sustentável do Paraguai e do Brasil

TLP:CLEAR

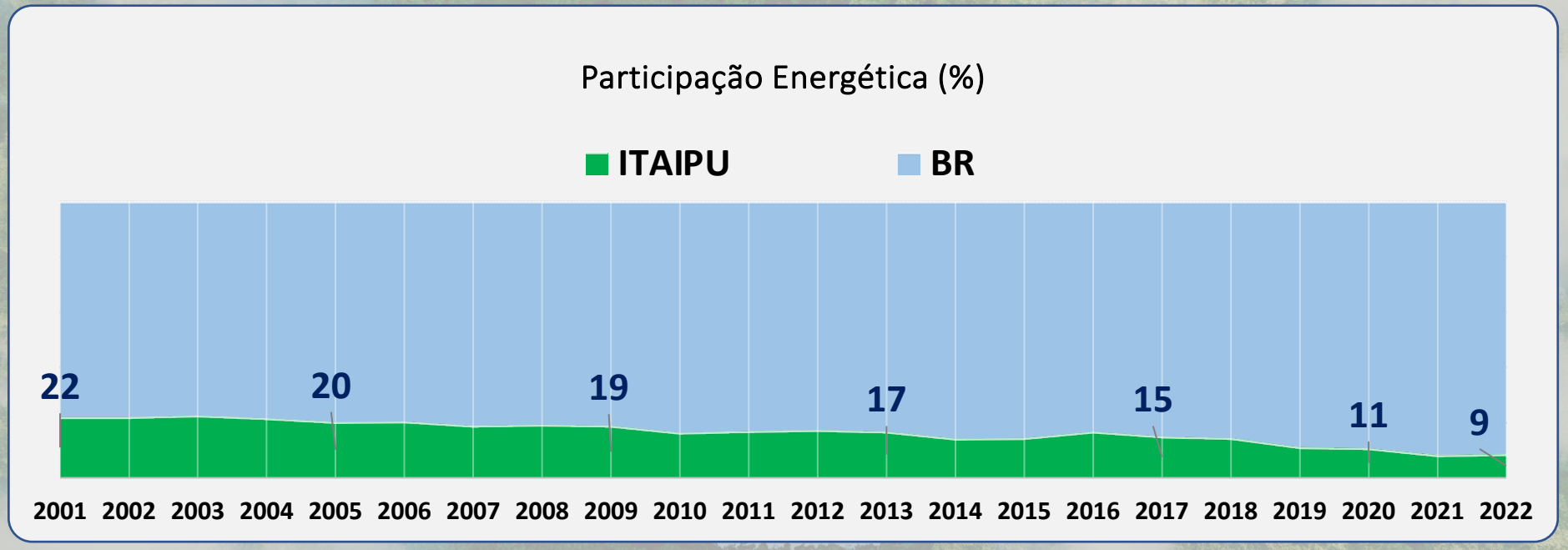
Relacionamento com Sistema Elétrico Brasileiro

TLP:CLEAR

Importância de ITAIPU: acumular energia despachável

A importância de Itaipu mudou, acompanhando a evolução do Setor Elétrico Brasileiro.

A **RELEVÂNCIA ENERGÉTICA** deu lugar à **SEGURANÇA OPERATIVA** para o Sistema Interligado Nacional!

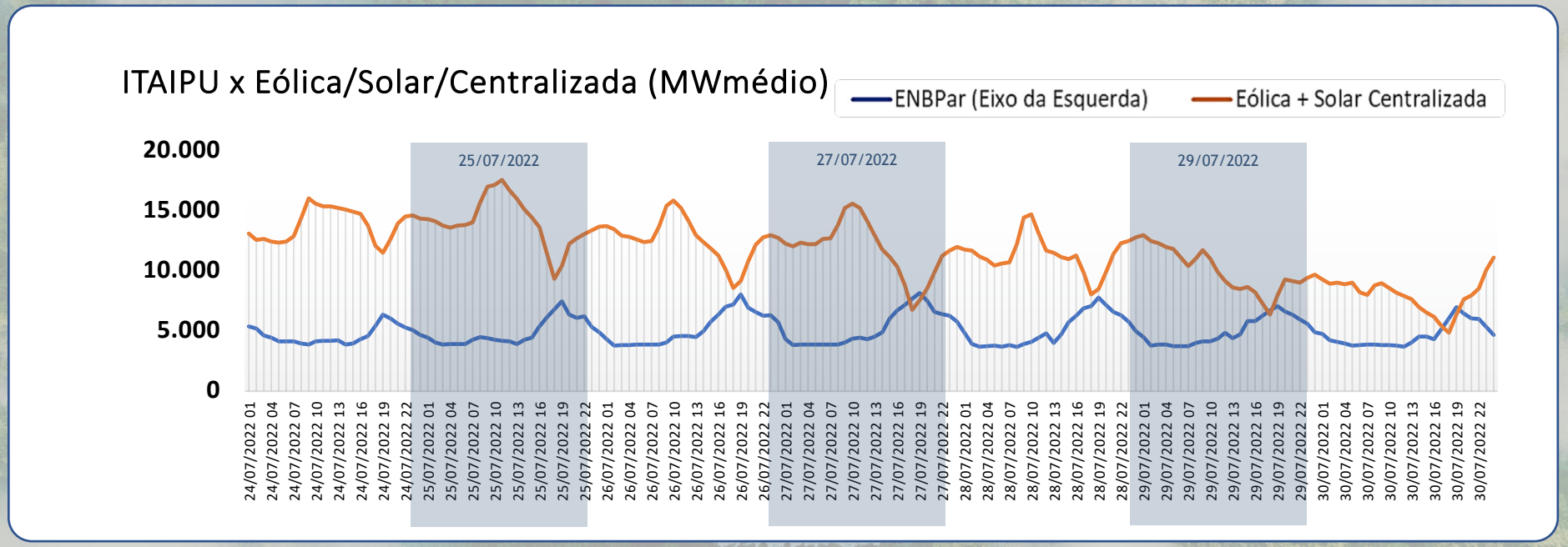


TLP:CLEAR

Importância de ITAIPU: acumular energia despachável

A importância de Itaipu mudou, acompanhando a evolução do Setor Elétrico Brasileiro.

A **RELEVÂNCIA ENERGÉTICA** deu lugar à **SEGURANÇA OPERATIVA** para o Sistema Interligado Nacional!

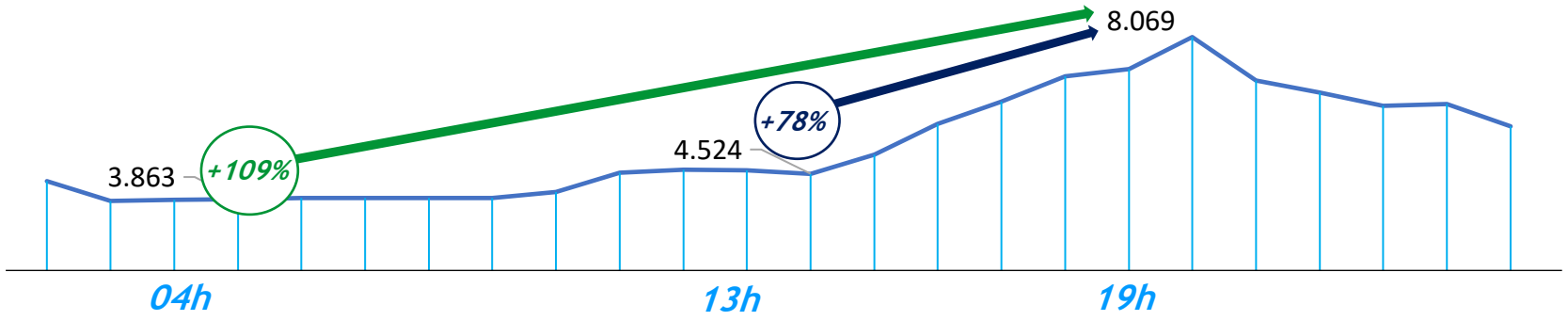


Importância de ITAIPU: acumular energia despachável

A importância de Itaipu mudou, acompanhando a evolução do Setor Elétrico Brasileiro.

A **RELEVÂNCIA ENERGÉTICA** deu lugar à **SEGURANÇA OPERATIVA** para o Sistema Interligado Nacional!

Intercâmbio Horário ITAIPU 26/07/2022 (MWmédio)



Agenda

- Itaipu e o Setor Elétrico
- **ISO/IEC 27001**
- Controles CIS
- Implementação e Desafios
- Conclusões

TLP:CLEAR

ISO/IEC 27001

Um dos padrões mais reconhecidos para implantação e operação de um sistema de gerenciamento de segurança da informação (SGSI)

TLP:CLEAR

NBR ISO/IEC 27001

NORMA
BRASILEIRA

ABNT NBR ISO/IEC 27001

Terceira edição
23.11.2022

Versão corrigida
31.03.2023

Segurança da informação, segurança cibernética e proteção à privacidade — Sistemas de gestão da segurança da informação — Requisitos

Information security, cybersecurity and privacy protection — Information security management systems — Requirements

TLP:CLEAR

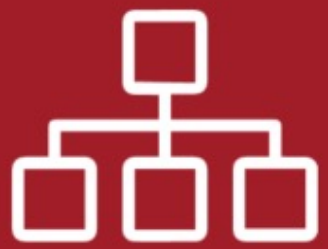
Benefícios

- Reduzir a vulnerabilidade a ataques
- Responder a evolução dos riscos de segurança
- Provê uma estrutura única e centralizado
- Focado em Riscos
- Dados digitais, em nuvem e em papel
- Economia de investimento com maior eficiência

TLP:CLEAR

NBR ISO/IEC 27001

ITAIPU BINACIONAL



Controles Organizacionais

Controles RH

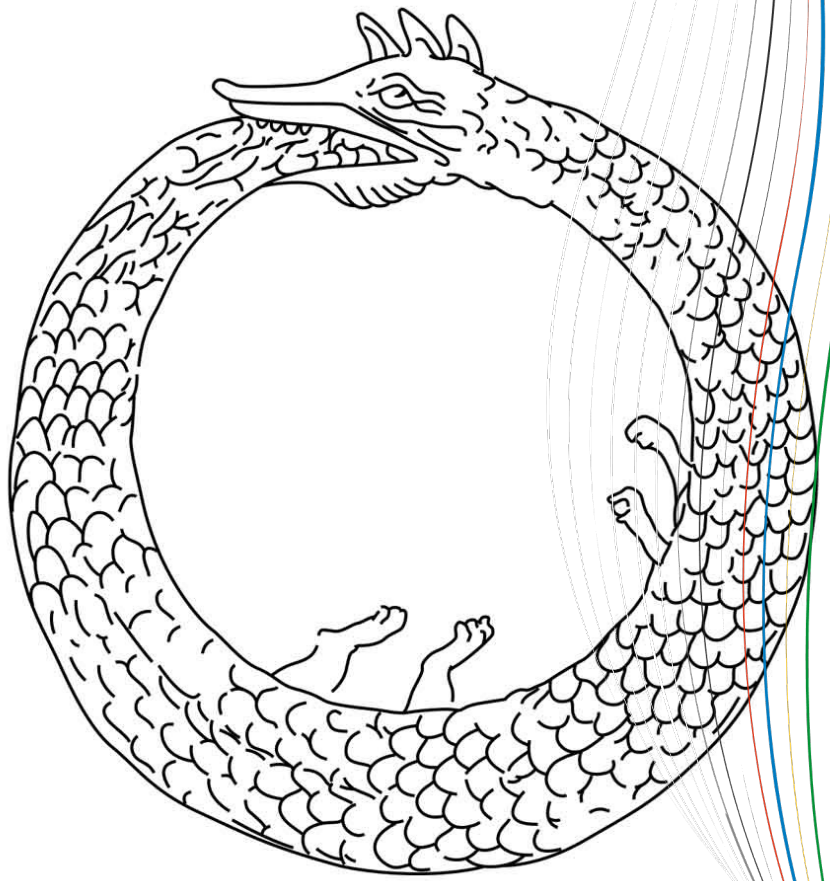
Controles Físicos

Controles Tecnológicos

TLP:CLEAR

7 passos

1. **Patrocínio** – comprometimento das partes
2. Classificar e priorizar os riscos
3. Mitigar os riscos
4. Estabelecer metas claras
5. Implementar os controles
6. Monitorar e ajustar
7. Concentrar nas melhorias do SGSI



TLP:CLEAR

NBR ISO/IEC 27001

TLP:CLEAR

NBR ISO/IEC 27001:2022

- Versão 2022 reduziu o número de controles em 21 (114 → 93):
  - Foram renomeados 23 controles para facilitar sua compreensão
  - 57 controles foram mesclados em 24, pois faziam parte de processos maiores
  - 1 controle foi dividido em 2 novos controles
  - 35 controles permaneceram iguais, apenas mudando a numeração
  - Foram introduzidos 11 novos controles no padrão

Fonte: advisera.com

TLP:CLEAR

NBR ISO/IEC 27001:2022

Fonte: advisera.com

TLP:CLEAR

PNPC - ABIN

Agenda

- Itaipu e o Setor Elétrico
- NBR ISO/IEC 27001
- **Controles CIS**
- Implementação e Desafios
- Conclusões

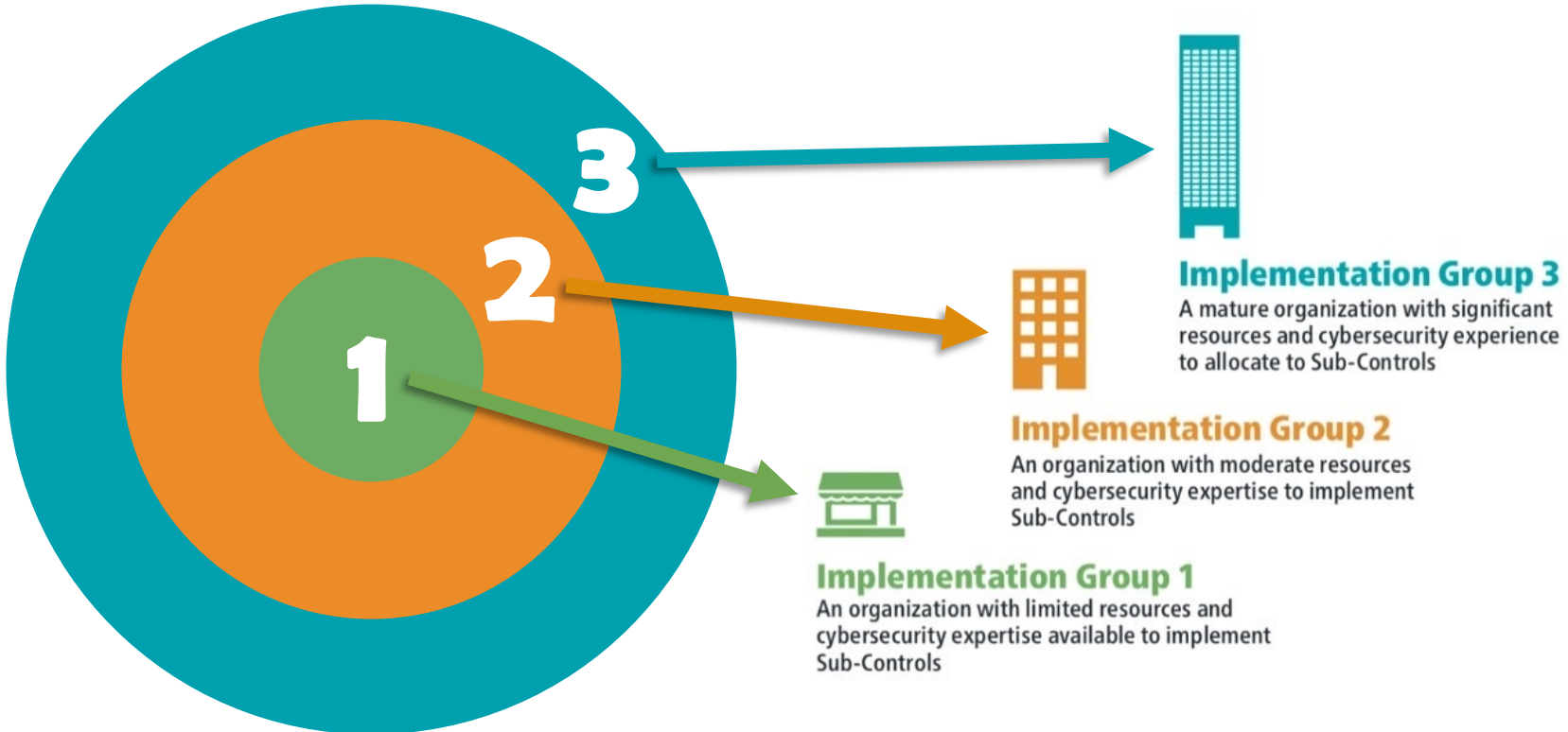
TLP:CLEAR

Controles CIS

- Capitaneados pelo *Center for Internet Security*;
- Identificar ataques cibernéticos importantes e traduzir em ações defensivas;
- Tem como base o framework de segurança do NIST
- Cada controle consiste:
  - **Visão Geral**: uma breve descrição da intenção do controle e sua utilidade como ação defensiva;
  - **Criticidade**: uma descrição da importância no bloqueio, mitigação ou identificação de ataques – e explicação sobre a exploração ou ausência do mesmo;
  - **Subcontroles**: tabela de ações específicas que as empresas

Grupos de Implementação de Controles (IGs)

- Categorias autoavaliadas para empresas
- Cada IG identifica um subconjunto dos Controles CIS que a comunidade avaliou amplamente para serem aplicáveis a uma empresa com um perfil de risco e recursos semelhantes para implementação.



TLP:CLEAR

Controles CIS

TLP:CLEAR

Controles CIS

Quadro 1: **Controles críticos de SegCiber preconizados pelo CIS**

1	**Inventário e controle de ativos corporativos**
2	**Inventário e controle de ativos de *software***
3	Proteção de dados
4	Configuração segura de ativos corporativos e *software*
5	Gestão de contas
6	Gestão de controles de acesso
7	**Gestão contínua de vulnerabilidades**
8	Gestão de registros (*logs*) de auditoria
9	Proteção de *e-mail* e navegador da web
10	Defesa contra *malware*
11	Recuperação de dados
12	Gestão de infraestrutura de rede
13	Monitoramento e defesa de rede
14	**Conscientização sobre segurança e treinamento de competências**
15	Gestão de provedores de serviço
16	Segurança de aplicações de *software*
17	**Gestão de respostas a incidentes**
18	Teste de invasão

Fonte: CIS Controls® Version 8 (tradução livre).

TLP:CLEAR

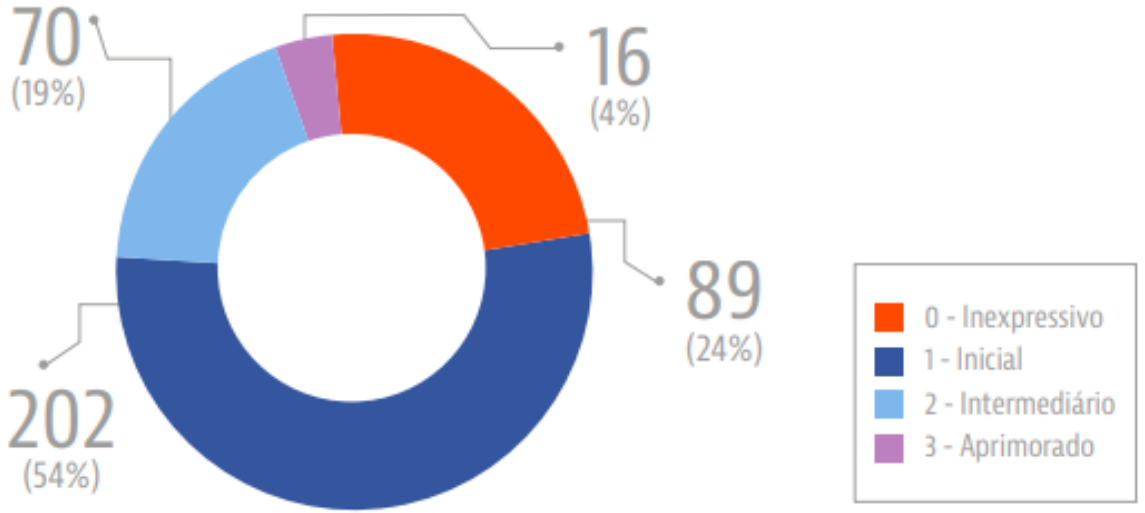
Controles CIS

- 1) Inventário e controle de ativos corporativos;
- 2) Inventário e controle de ativos de software;
- 7) Gestão contínua de vulnerabilidades;
- 14) Conscientização sobre segurança e treinamento de competências;
- 17) Gestão de respostas a incidentes.

TLP:CLEAR

Benchmark do TCU

"O TCU realizou, entre 03/08/2021 e 09/03/2022, o primeiro de sete ciclos previstos para o acompanhamento de controles críticos de segurança cibernética das organizações públicas federais. O panorama geral que se apresentou neste primeiro ciclo é preocupante, pois 24% das 377 organizações ainda se encontram no estágio Inexpressivo e 54%, no estágio Inicial, conforme apresentado no Gráfico 1:"



Fonte: Elaboração própria.

TLP:CLEAR

MINISTÉRIO DA GESTÃO E DA INOVAÇÃO EM SERVIÇOS PÚBLICOS

ITAIPU BINACIONAL

gov.br Ministério da Gestão e da Inovação em Serviços.. Órgãos do Governo Acesso à Informação Legislação Acessibilidade Entrar com o gov.br

Governo Digital

O que você procura?

Privacidade e Segurança > Programa de Privacidade e Segurança da Informação (PPSI)

Programa de Privacidade e Segurança da Informação (PPSI)

O que é o PPSI, quais são seus objetivos e quais são suas áreas de atuação?

Publicado em 16/06/2021 18h26 | Atualizado em 24/07/2023 22h29 Compartilhe:

O Programa

O **Programa de Privacidade e Segurança da Informação** (PPSI) caracteriza-se como um conjunto de projetos e processos de adequação nas áreas de privacidade e segurança da informação e tem como valores: a **maturidade**; a **resiliência**; a **efetividade**; a **colaboração** e a **inteligência**. No âmbito da Secretaria de Governo Digital, a Diretoria de Privacidade e Segurança da Informação é a unidade responsável pelo PPSI.

O Programa foi instituído por meio da PORTARIA SGD/MGI Nº 852, DE 28 DE MARÇO DE 2023 e implementa ações de Privacidade e Segurança da Informação no âmbito dos órgãos e entidades da administração pública federal direta, autárquica e fundacional, que possuem unidades que compõem o Sistema de Administração dos Recursos de Tecnologia da Informação (SISP), conforme art. 3º do DECRETO Nº 7.579, DE 11 DE OUTUBRO DE 2011.

TLP:CLEAR

Resolución MITIC N° 277

"SESQUICENTENARIO DE LA EPOPEYA NACIONAL: 1864 - 1870"

PODER EJECUTIVO
MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

RESOLUCIÓN MITIC Nº 277

PODER EJECUTIVO MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

POR LA CUAL SE ACTUALIZA LA GUÍA DE CONTROLES CRÍTICOS DE CIBERSEGURIDAD DEL MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN.----------

- 1 -

Asunción, 23 de junio de 2020

VISTO: La Resolución SENATICs N° 115/2018 de fecha 13 de agosto de 2018 "POR LA CUAL SE APRUEBA LA GUÍA DE CONTROLES CRITICOS DE CIBERSEGURIDAD".----------

El Memorándum DG N° 026/2020 de fecha 17 de enero de 2020, de la Dirección de Gabinete del Viceministerio de Tecnologías de la Información y Comunicación de la Institución, mediante el cual fuera solicitada la emisión de la Resolución Ministerial respectiva, a fin de actualizar la "Guía de Controles Críticos de Ciberseguridad" en las Instituciones del Estado, aprobada por Resolución

TLP:CLEAR

CERT-PY

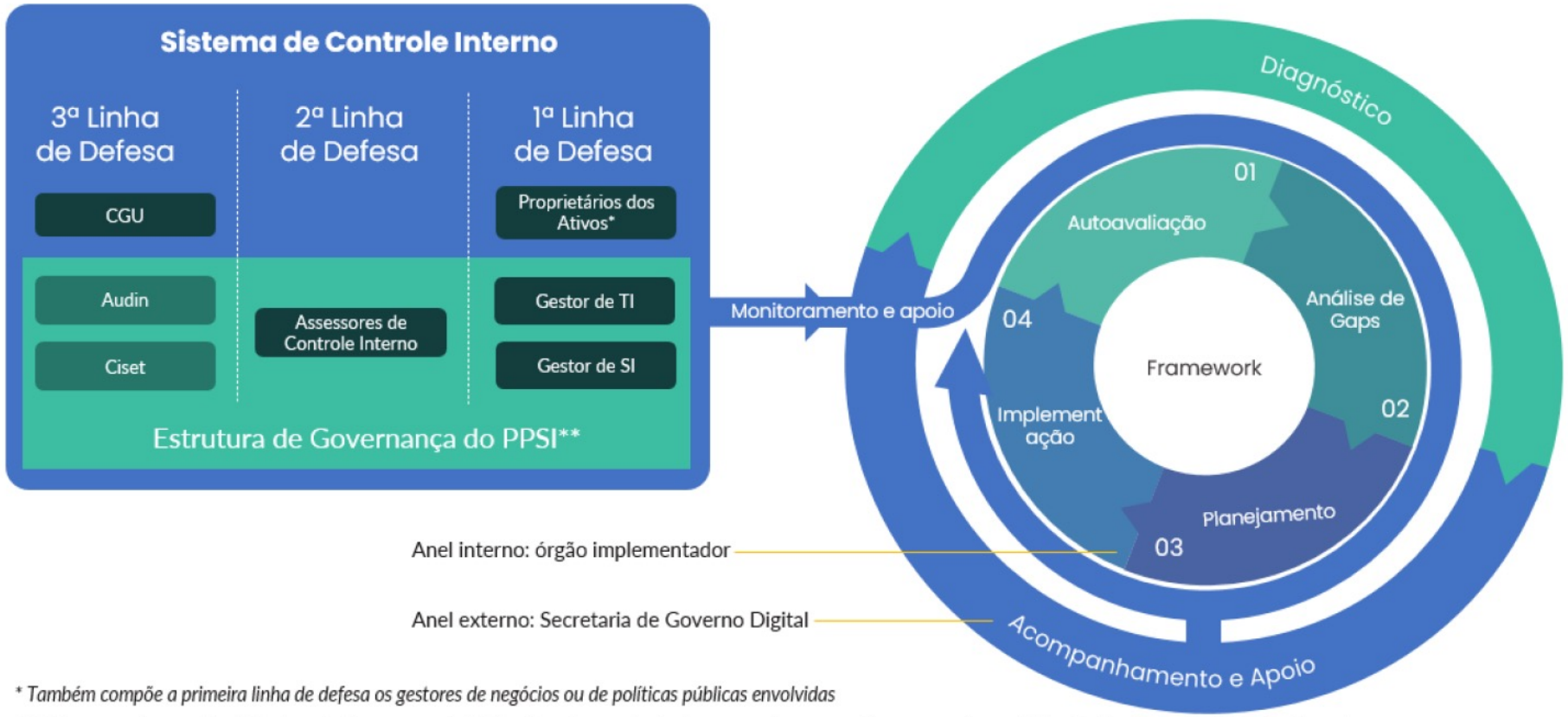
Agenda

- Itaipu e o Setor Elétrico
- NBR ISO/IEC 27001
- **Controles CIS**
- **Implementação e Desafios**
- Conclusões

TLP:CLEAR

Modelo alinhado

Figura 3: METODOLOGIA DE IMPLEMENTAÇÃO DO FRAMEWORK.



* *Também compõe a primeira linha de defesa os gestores de negócios ou de políticas públicas envolvidas*

** *O Encarregado compõe a Estrutura de Governança do PPSI e atuará com orientações e suporte nas questões que envolvem a Privacidade e Proteção de Dados Pessoais*

Agenda

- Itaipu e o Setor Elétrico
- NBR ISO/IEC 27001
- **Controles CIS**
- Implementação e Desafios
- **Conclusões**

TLP:CLEAR

Conclusões

- “Ótimo é inimigo do bom”
- Normas e melhores práticas ajudam a sensibilizar alta gerência
- Demonstre que o esforço diminui os riscos e trabalho futuro
- Controles CIS ajudam a priorizar as ações
- Cada escala de empresa, tem um respectivo desafio
- Não tem início/fim, é um exercício

TLP:CLEAR

Mais Informações

- GUIA DO FRAMEWORK DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO – Ministério da Gestão e da Inovação em Serviços Públicos
- Guia de Requisitos e Obrigações quanto a Privacidade e à Segurança da Informação - Ministério da Gestão e da Inovação em Serviços Públicos
- Cinco controles de segurança cibernética pra ontem – Tribunal de Contas da União
- PNPC – Boas Práticas – Agencia Brasileira de Inteligência
- Controles Críticos de Ciberseguridad – CERT-PY
- Resolución MITIC Nº 277 – Ministerio de Tecnologias de La Información y Comunicación
- RansomChats

TLP:CLEAR

Foto: Klaus Steding-Jessen

ITAIPU BINACIONAL

MINISTÉRIO DE MINAS E ENERGIA

MINISTÉRIO DAS RELAÇÕES EXTERIORES

GOVERNO FEDERAL BRASIL UNIÃO E RECONSTRUÇÃO

Endereço: Av. Sílvio Américo Sasdelli, 800
CEP: 85.866-900
Foz do Iguaçu, Paraná, Brasil

TELEFONE: 45 3520-5252

www.itaipu.gov.br

2023

31 de Julho