MINISTÉRIO DA
DEFESA

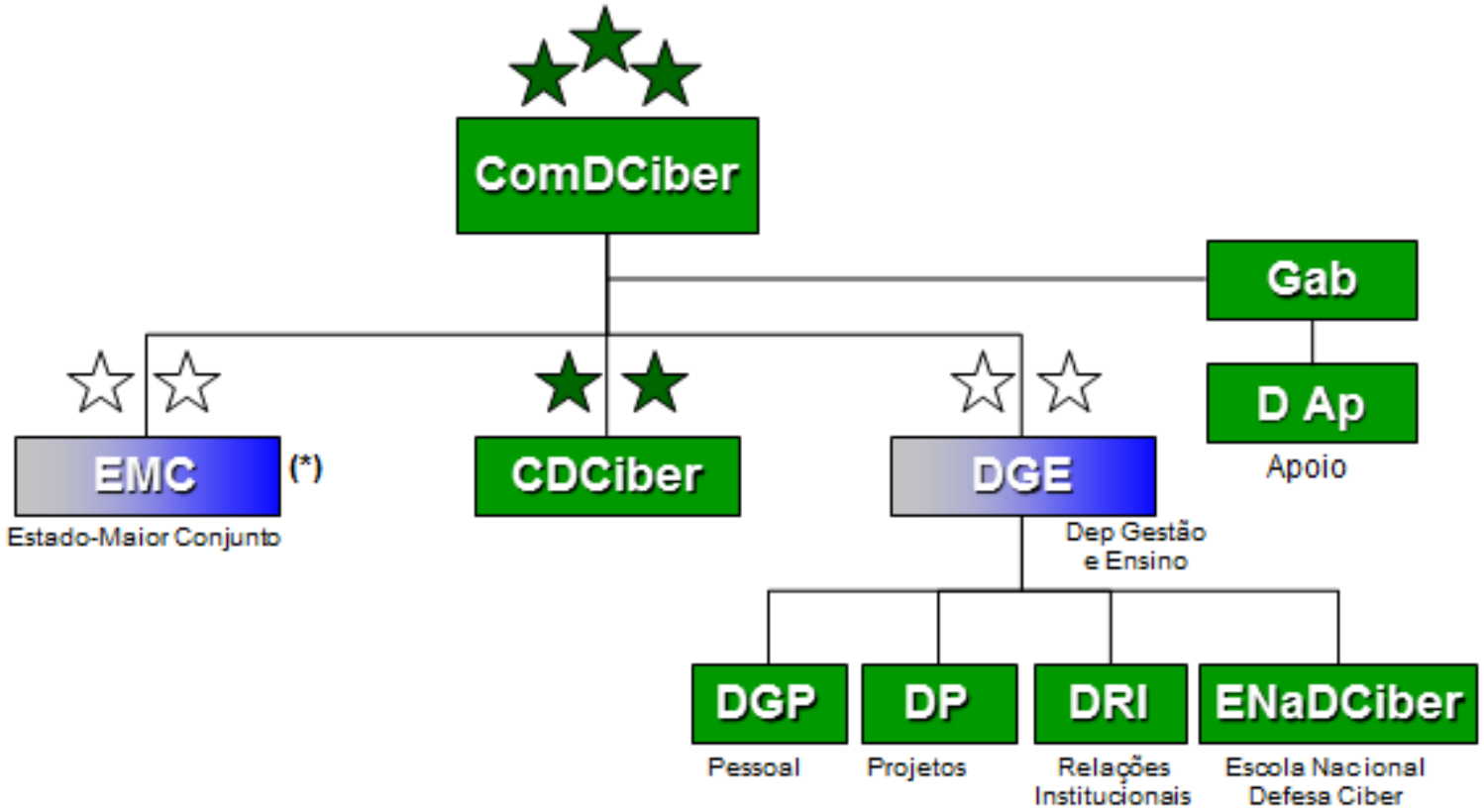
Estado-Maior Conjunto
das Forças Armadas

A Segurança e Defesa Cibernéticas nos Jogos Olímpicos e Paralímpicos Rio 2016

COM D CIBER

C D CIBER

COMANDO DE DEFESA CIBERNÉTICA



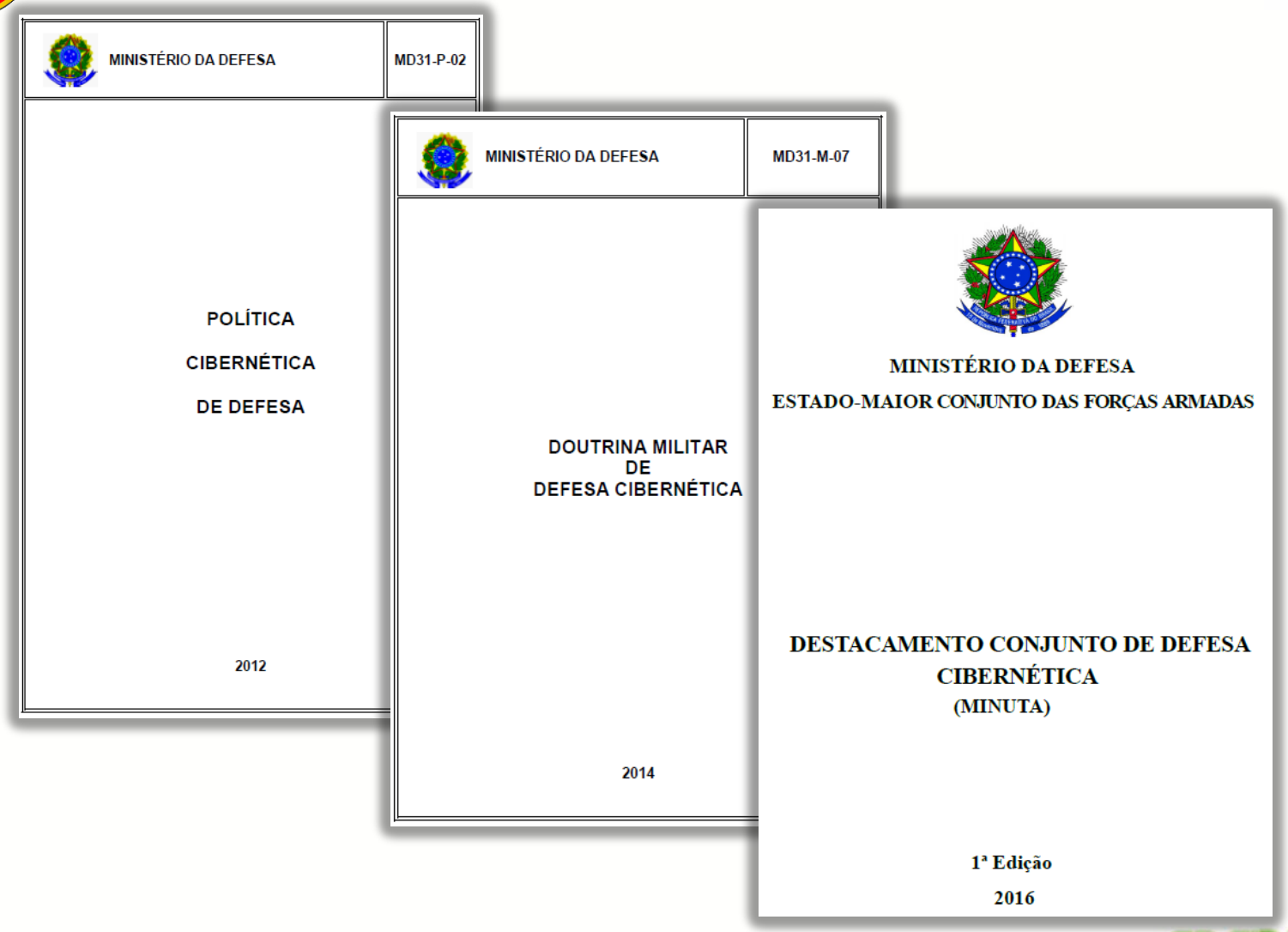
(*) a ser ocupado, em sistema de rodízio, entre a MB e a FAB.

Centro de Defesa Cibernética

CENTRO DE OPERAÇÕES CIBERNÉTICAS

Protege, Explora e Combate

CIBERNÉTICA E DEFESA NACIONAL



A SEGURANCA E DEFESA CIBERNÉTICAS NOS GRANDES EVENTOS

A SEGURANCA E DEFESA CIBERNÉTICAS NOS GRANDES EVENTOS

Rio 2016 Cyber Security Integration Meeting
24 de novembro de 2014
Rio de Janeiro, RJ

Cooperação:
CERT.br, CTIR Gov e CDCiber
A cooperação já era grande.
Ficou fortalecida após os grandes eventos.
Houve:
• Troca de informações
• Divisão de tarefas
CDCiber: atuação presencial nos CCDAs e CICCRs;
CTIR Gov: foco nos ataques às redes do Governo;
CERT.br: facilitar a comunicação e coordenação com outros atores,principalmente CSIRTs (nacionais e internacionais); monitoração de canais de IRC e Twitter; monitoração dos feeds de dados por qualquer atividade maliciosa saindo das redes mapeadas pelo CDCiber e pelo CTIR Gov.

A SEGURANCA E DEFESA CIBERNÉTICAS NOS GRANDES EVENTOS

Rio 2016 Cyber Security Integration Meeting
24 de novembro de 2014
Rio de Janeiro, RJ

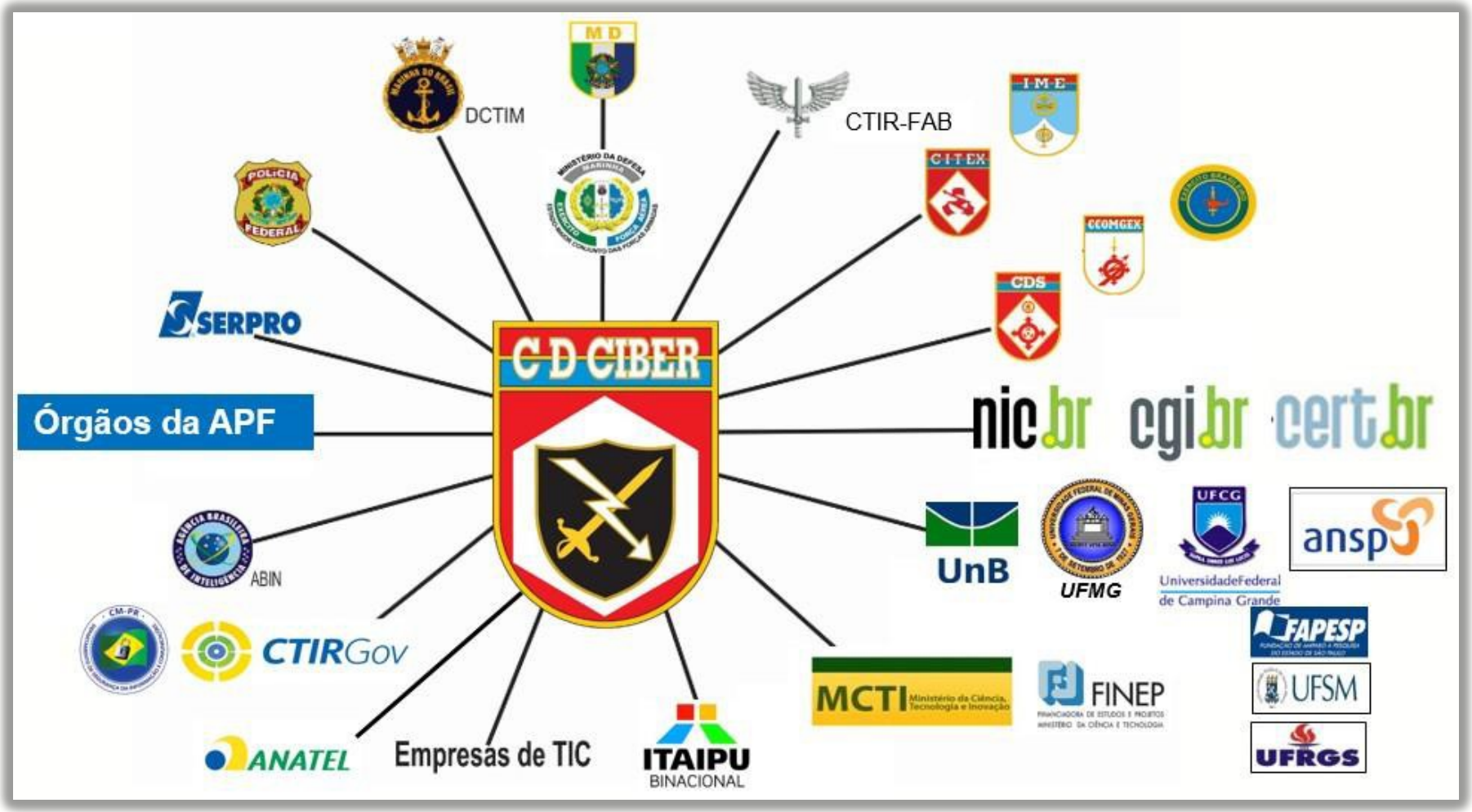
Reflexões para 2016

Cooperação

- Nenhum único grupo ou estrutura conseguirá fazer sozinho a segurança ou a resposta a incidentes;
- Pessoal preparado em todas as redes e áreas cooperação direta entre os diversos atores;
- Os times serão os mesmos de sempre, mas é necessário ter mais troca de informações e cooperação entre os grupos organizadores o pessoal técnico de todas as operadoras e provedores de serviços Internet e todos os CSIRTs formados no Brasil;

Ações necessitam iniciar já !

COORDENAÇÃO E INTEGRAÇÃO



CENÁRIO PROSPECTIVO PARA OS JO RIO 2016

Os ativos de informação podem sofrer ataques que modifiquem, destruam, exponham dados originais ou introduzam dados espúrios nos sistemas de TIC, comprometendo a disponibilidade, integridade, confidencialidade e autenticidade das informações contidas nesses sistemas.

JOGOS OLÍMPICOS RIO 2016

ASPECTOS DA MISSÃO RELACIONADOS À ATRIBUIÇÃO DE COORDENAR NO ÂMBITO DA SEGURANÇA CIBERNÉTICA

Na condição de Coordenador da Seg e Def Ciber planejar apoiar e colaborar com a Presidência da República para a Segurança das Infraestruturas Críticas Nacionais, devendo para tal:

- Identificar as Infraestruturas Críticas (IEC) para a realização dos JO;
- Levantar as vulnerabilidades e as ameaças cibernéticas das IEC identificadas e sua interdependência com outras IEC;
- Propor medidas necessárias à segurança cibernética das IEC.

JOGOS OLÍMPICOS RIO 2016

ASPECTOS DA MISSÃO RELACIONADOS À ATRIBUIÇÃO DE COORDENAR

Atuar como interface única entre o Comitê Rio 2016 e as instituições públicas e privadas no tocante ao processo de resposta a incidentes de segurança.

Parceiros

- SC2/EMCFA/MD
- DCTIM/MB
- CITEX/EB
- DTI/FAB
- SESGE
- CERT.br/CGI.br
- CM/PR
- CTIR.gov
- ABIN
- GRA/SERPRO
- SRCC/DPF
- ANATEL
- INFRAESTRUTURAS CRÍTICAS

JOGOS OLÍMPICOS RIO 2016

ASPECTOS DA MISSÃO RELACIONADOS À ATRIBUIÇÃO DE COORDENAR

Estabelecer parcerias com organizações e instituições que atuam em Seg e Def Ciber de modo a perceber, obter, registrar, processar e disseminar informações que permitam mitigar ou evitar **incidentes de Seg Ciber que ameacem a segurança do Evento**.

Definir a estratégia geral entre os parceiros para cumprimento da missão de Seg e Def Ciber .

Formalizar Protocolos de Procedimentos com cada parceiro, quando for o caso.

CAPACITAÇÃO TÉCNICA

Na Fase de Preparo, foram realizadas atividades de capacitação técnica nas ferramentas a serem empregadas pelos efetivos dos Destacamentos Central e Remotos dos diversos CDA, CGDA e CDS.

Capacitação		
Período (2016)	**Atividade**	**Efetivo (Civ e Mil)**
25 a 29 ABR	Curso de Tratamento de Incidentes de Rede do CERT.br	52
1º a 2 JUN e 28 JUN	Operação do Carbon Black	62
1º a 2 JUN e 4 a 8 JUL	Operação do Segurança Analítica	36
1º a 2 JUN	Operação do Splunk	28
1º a 2 JUN	Operação do RTIR	54
Total		**232**

REUNIÕES DE COORDENAÇÃO

Na Fase de Preparo foram realizadas reuniões de coordenação de grande importância para o estabelecimento de estratégias de atuação conjunta entre militares e civis de organizações parceiras.

Reunião de Coordenação da Seg e Def Ciber		
Data	**Atividade**	**Efetivo (Civ e Mil)**
6 ABR 16	Reunião de Coordenação	35
5 JUL 16		37
Total		**72**

JOGOS OLÍMPICOS RIO 2016

ASPECTOS DA MISSÃO RELACIONADOS À ATRIBUIÇÃO DE INTEGRAR

Identificar os principais ativos relacionados ao Evento, **realizando análise de riscos e levantamento de vulnerabilidades**, naqueles de interesse.

Montar uma estrutura que propicie CONSCIÊNCIA SITUACIONAL acerca dos incidentes e eventos de segurança relacionados aos ativos de interesse, permitindo um apoio a Decisão.

Acompanhar o espaço cibernético de interesse para avaliação do nível de risco dos sistemas envolvidos.

JOGOS OLÍMPICOS RIO 2016

BRASÍLIA

- **1 (um) Destacamento Conjunto de Defesa Cibernética Central.**

CIDADE-SEDE (Rio de Janeiro)

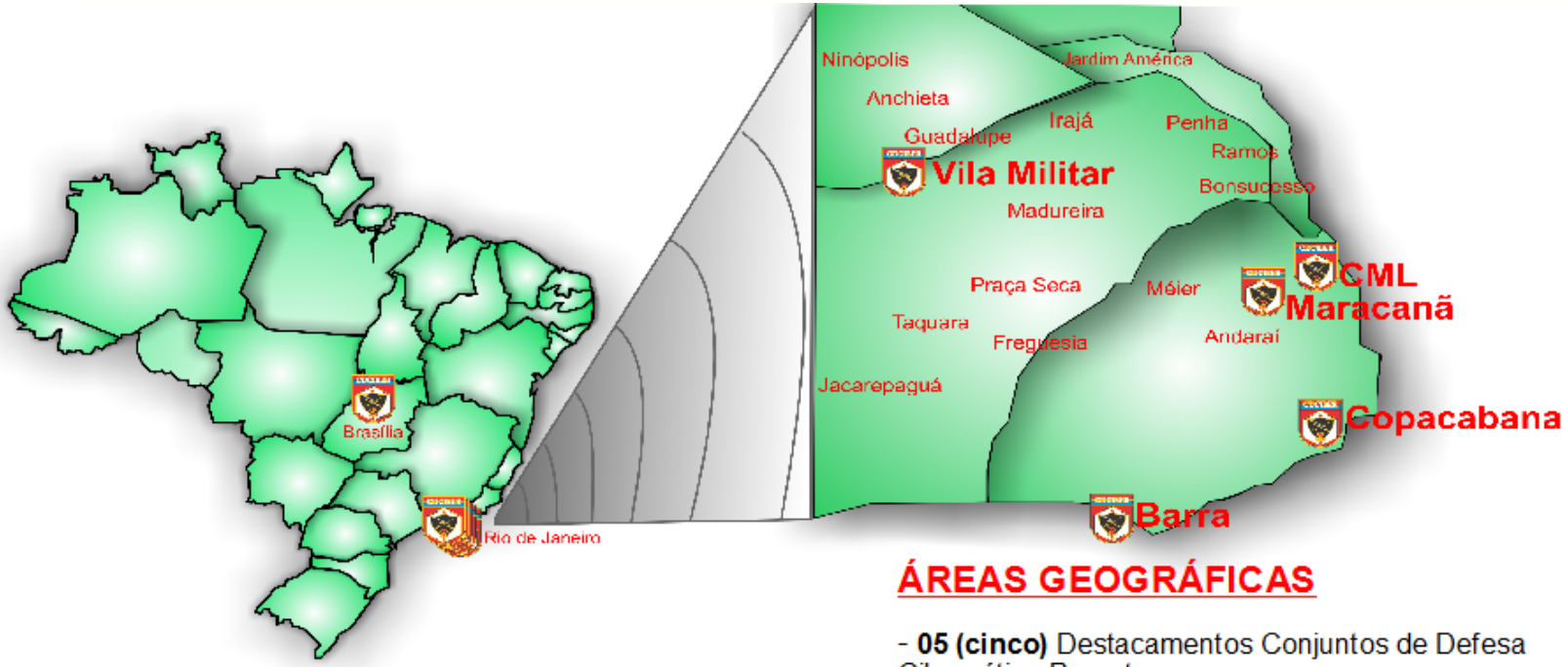
- **5 (cinco) Destacamentos Conjuntos de Defesa Cibernética Remotos (CGDA/CDS).**

CIDADES-SEDE Futebol

- **5 (cinco) Destacamentos Conjuntos de Defesa Cibernética Remotos (CDA).**

JOGOS OLÍMPICOS RIO 2016

DESDOBRAMENTO NO RIO DE JANEIRO



BRASÍLIA

- **01 (um)** Destacamento Conjunto de Defesa Cibernética Central.

ÁREAS GEOGRÁFICAS

- **05 (cinco)** Destacamentos Conjuntos de Defesa Cibernética Remotos.

- 01 CGDA (CML)

- 01 CDS Vila Militar

- 01 CDS Maracanã

- 01 CDS Copacabana

- 01 CDS Barra

Organização do CGDA para os JO Rio 2016

Log: Pessoal Pronto

10.2 Prontos					
Órgão	**Forças Armadas**	**Oficiais**	**Civis**	**Graduados/Praças**	**TOTAL**
CCSDCIBER	MB/EB/FAB	35	3	39	77
CGDA	MB/EB/FAB	14	-	23	37
CDA – MN	MB/EB/FAB	1	-	4	5
CDA – SP	MB/EB/FAB	1	-	4	5
CDA – SV	MB/EB/FAB	1	-	4	5
CDA – BH	MB/EB/FAB	2	-	3	5
CDA – BR	MB/EB/FAB	1	-	4	5
	TOTAL	**55**	**3**	**80**	**138**

CONCEITO OPERACIONAL

Destacamento Conjunto de Defesa Cibernética Central

Coordenação e Integração

CDCiber

Destacamento Conjunto de Defesa Cibernética Remoto

Proteção, Detecção e Reação

CGDA

Destacamento Conjunto de Defesa Cibernética Remoto

Proteção, Detecção e Reação

CDA/CDS

- **Correlacionador de Eventos**
- **Perícia Forense**
- **Monitoramento de Endpoint**
- **Gestão de Risco**
- **Gestão de Eventos**

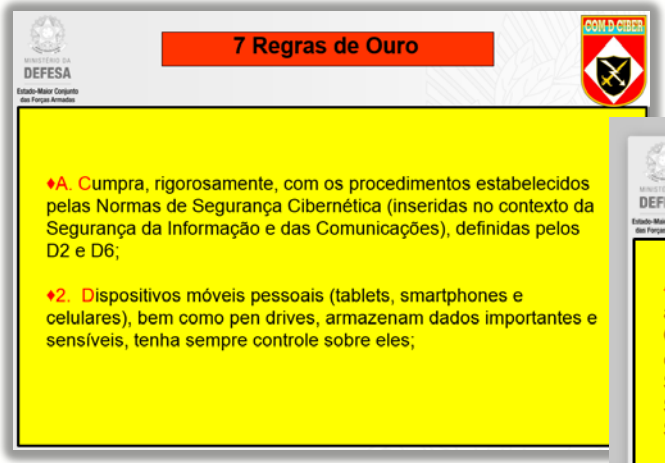
7 Regras de Ouro

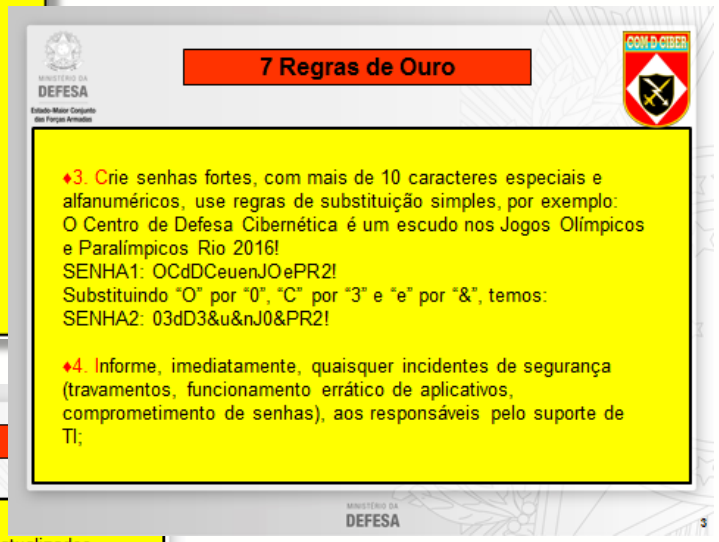
Jeh Johnson, U.S. Secretary of Homeland Security, observed:

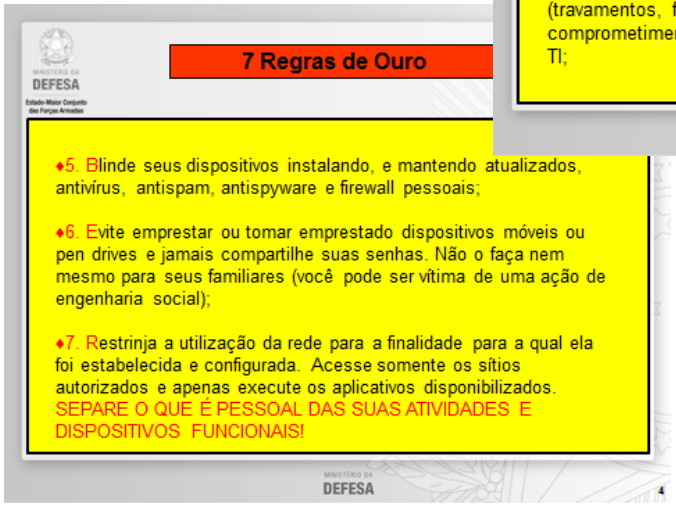
"What amazes me when I look into a lot of intrusions, including some really big ones by multiple different types of actors, ***it often starts with the most basic active spearphishing where somebody is allowed in the gate and penetrates a network simply because an employee clicked on something he or she shouldn't have.*** *And the most sophisticated actors count on penetrating a system in that way."*

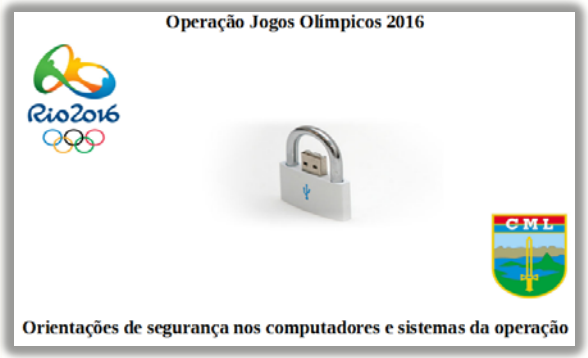
PREPARO

Procedimentos de conscientização para a SIC junto aos usuários e Adm de ativos de Info dos COp e Estrt Etta.

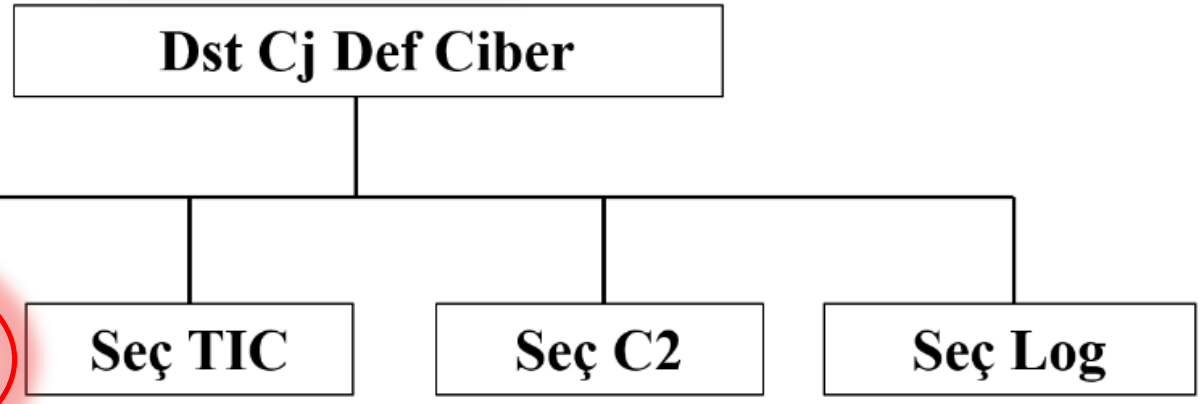









CDCIBER
CENTRO
DE
OPERAÇÕES
CIBERNÉTICAS


Dst Cj Def Ciber
C Op Ciber
Seç TIC
Seç C2
Seç Log
Seç Op
Seç Intlg

Detecção

- Monitoramento de *endpoint*
- Monitoramento da rede de dados interna
- Monitoramento de *sites*
- Oficiais de Ligação
- Dst Cj Def Ciber Rmto
- Abuse
- Dados de fontes abertas

MAIORES DESAFIOS

- Manter o importante legado intangível de coordenação e integração junto aos órgãos parceiros.

- Dar continuidade à cooperação para a proteção cibernética (civis e militares).

- Contribuir para a integração entre os CTIR das Forças Singulares.

- Aprimorar a capacidade de agregar informação aos incidentes críticos nas ligações com os CTIR.

MINISTÉRIO DA
DEFESA
Estado-Maior Conjunto
das Forças Armadas

Rio2016

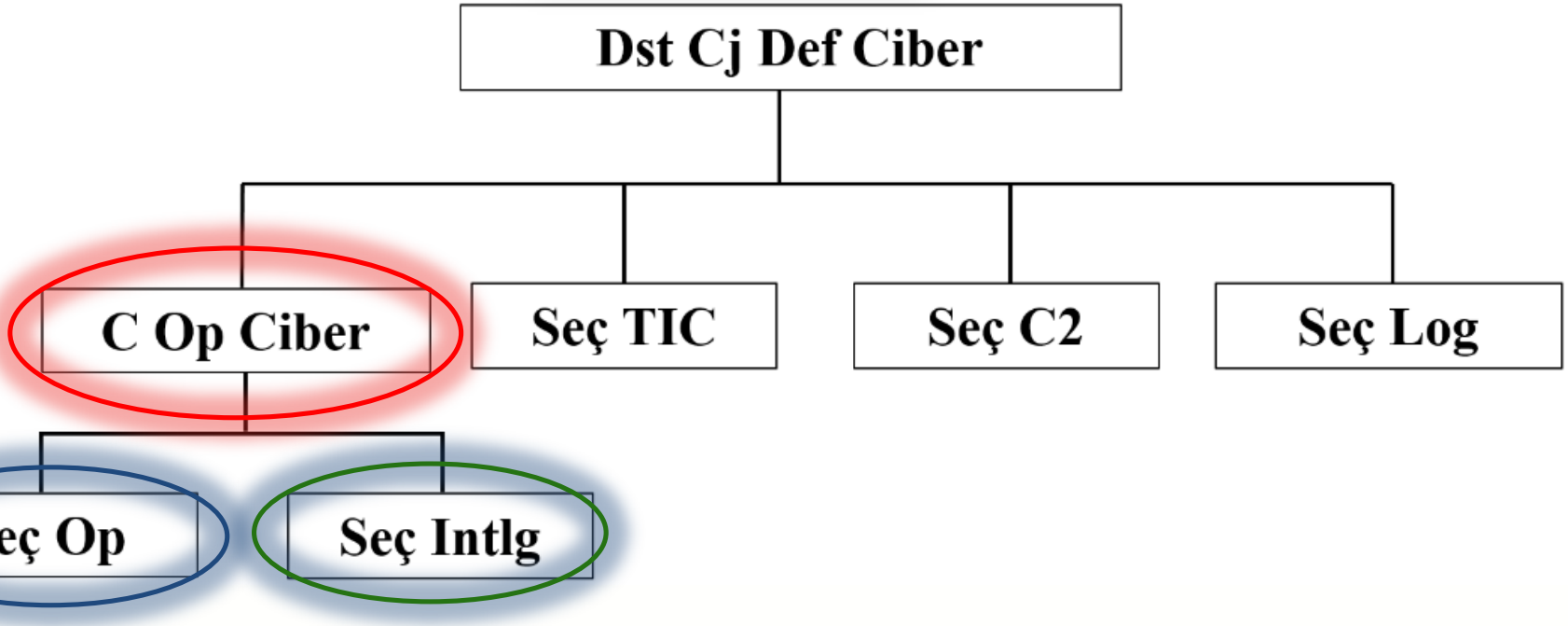
Rio2016
JOGOS PARALÍMPICOS

O Centro de Operações Cibernéticas

COM D CIBER

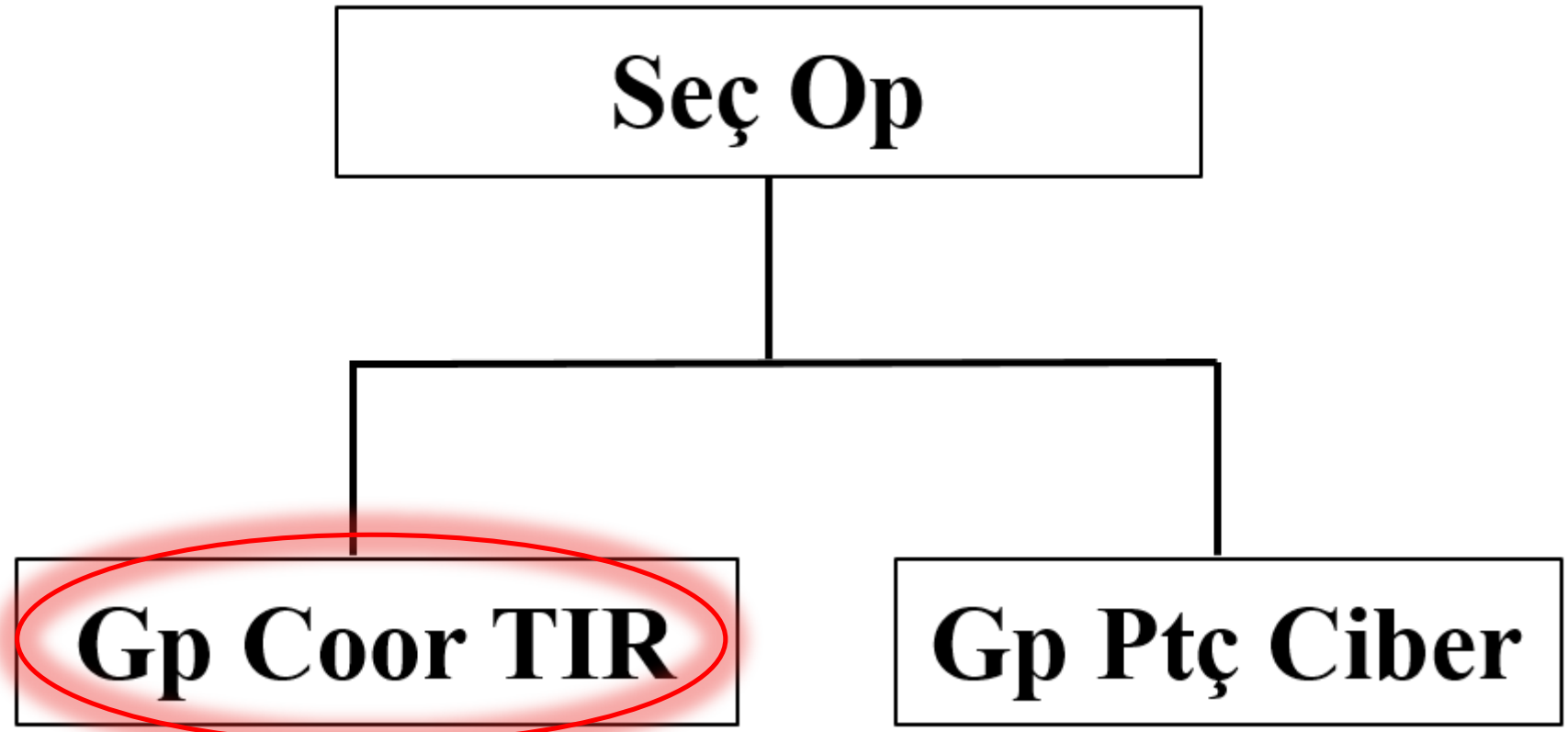
C D CIBER


CDCIBER
CENTRO
DE
OPERAÇÕES
CIBERNÉTICAS


Dst Cj Def Ciber
C Op Ciber
Seç TIC
Seç C2
Seç Log
Seç Op
Seç Intlg

Coordenação de TIR

Seção de Operações



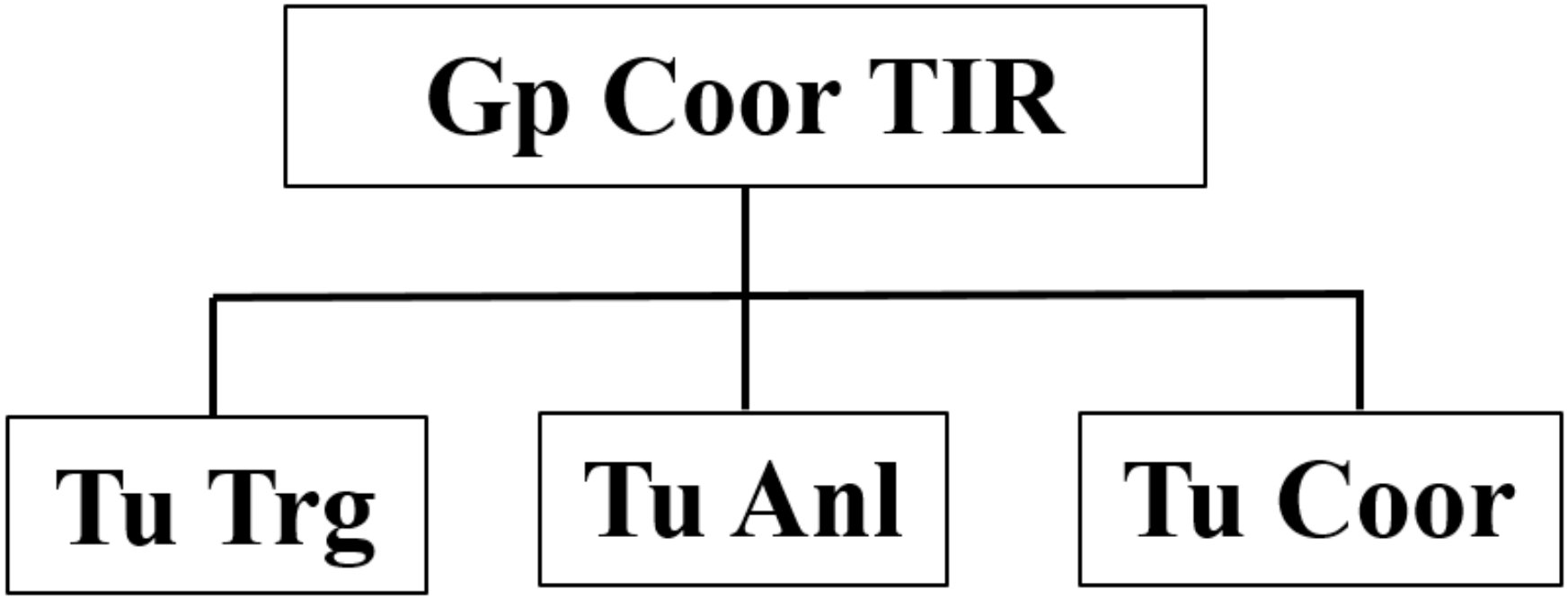
Grupo de Coordenação de Tratamento de Incidentes de Rede

Responsável pela coordenação do tratamento de incidentes de rede que envolvam a segurança e defesa cibernética, a fim de identificar as causas, consequências, assim como coletar evidências, sugerir possíveis soluções e encaminhar as notificações de incidentes ao CTIR ou ETIR responsável pelo ativo de informação para as providências necessárias.

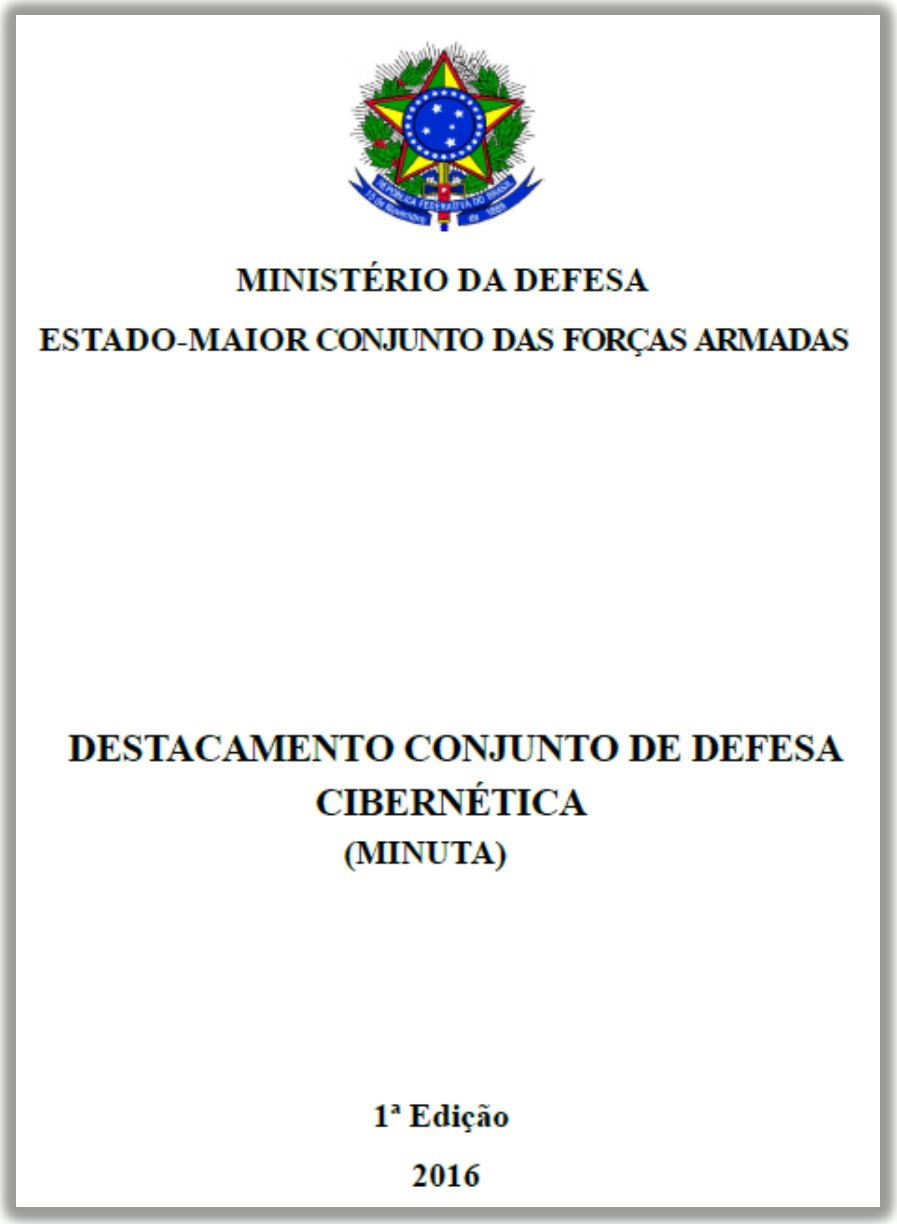
Detecção

- Monitoramento de *endpoint*
- Monitoramento da rede de dados da Defesa
- Monitoramento de *sites*
- Oficiais de Ligação
- Dst Cj Def Ciber Rmto
- Abuse
- Dados de fontes abertas

Tratamento de incidentes de rede



MAPEAMENTO DOS PROCESSOS



MINISTÉRIO DA DEFESA

ESTADO-MAIOR CONJUNTO DAS FORÇAS ARMADAS

DESTACAMENTO CONJUNTO DE DEFESA CIBERNÉTICA

(MINUTA)

1ª Edição

2016

MAPEAMENTO DOS PROCESSOS

SUMÁRIO

Turma de Coordenação

3.2.2.2.3 **Turma de Coordenação** é responsável pela revisão das análises dos incidentes em tratamento, bem como pela notificação aos responsáveis pelos ativos comprometidos, a fim de concluir o ciclo com a resposta ao tratamento de incidente. Em seu trabalho, deve considerar os impactos técnicos, gerenciais e legais, buscando compatibilizá-los com as políticas e procedimentos em vigor. Seu papel é de grande importância, de modo a permitir que o Cmt do Dst Cj Def Ciber possa ser assessorado para a tomar a decisão adequada frente aos incidentes recebidos.

3.2.2.2.3.1 **Composição** é composta pelo efetivo mínimo de 1 (um) Coordenador, o qual deverá ser oficial com experiência em Tratamento de Incidentes de Rede.

Turma de Coordenação

3.2.2.2.3.2 **Qualificação em**: gestão de pessoal, gestão de TI, mapeamento de processos, Tratamento de Incidentes de Rede (básico e avançado), administração de redes, sistemas operacionais e de banco de dados, bem como em segurança da informação.

3.2.2.2.3.3 **Competências**: deve possuir capacidade para gerenciar e coordenar equipes técnicas de forma eficiente e eficaz, priorizando os esforços de tratamento para a notificação dos incidentes mais críticos, de acordo com os parâmetros estabelecidos pelo Comando do Dst Cj Def Ciber.

Turma de Coordenação

3.2.2.2.3.4 **Procedimentos**

3.2.2.2.3.4.1 Verificar os *tickets* que já passaram pela análise, ordenando-os pela prioridade.

3.2.2.2.3.4.2 Selecionar incialmente os *tickets* prioritários para iniciar a verificação.

3.2.2.2.3.4.3 Clicar em "Histórico".

3.2.2.2.3.4.4. Avaliar os comentários do Analista e verificar as evidências coletadas.

3.2.2.2.3.4.5 Clicar em "Exibir" e, em seguida, na aba "Sumário".

3.2.2.2.3.4.6. Verificar a correção das informações constantes nos campos do "Sumário" e realizar a atualização, se for o caso.

3.2.2.2.3.4.7 Clicar em "Pessoas" e verificar se o destinatário correto está constando como requisitante.

Turma de Coordenação

3.2.2.2.3.4.8 Clicar em “Exibir” e copiar a notificação preparada pelo Analista.

3.2.2.2.3.4.9 Selecionar a ação “Notificar” no menu “Ações”.

3.2.2.2.3.4.10 Revisar o texto da notificação preparada pelo Analista na caixa de texto correspondente e realizar os ajustes necessários de acordo com o incidentes.

3.2.2.2.3.4.11 Alterar o estado do *ticket*, de acordo com o tratamento realizado no incidente.

3.2.2.2.3.4.12 Enviar a notificação.

MAIORES DESAFIOS

- Prosseguir nos trabalhos de melhoria das ferramentas de detecção.
- Manter a continuidade da cooperação para a proteção cibernética (civis e militares).
- Contribuir para a integração entre os CTIR das Forças Singulares.
- Aprimorar a capacidade de agregar informação aos incidentes críticos nas ligações com os CTIR.