FLUIDEZ NAS COMUNICAÇÕES

ANACOM AUTORIDADE NACIONAL DE COMUNICAÇÕES

Segurança de Redes e Serviços de Comunicações Electrónicas: As alterações na regulação

IEEE COMMUNICATIONS SOCIETY Portugal Chapter

POSTIT

INSTITUTO SUPERIOR TÉCNICO

Palestras da ComSoc/POSTIT

Manuel Pedrosa de Barros
Direcção de Segurança nas Comunicações

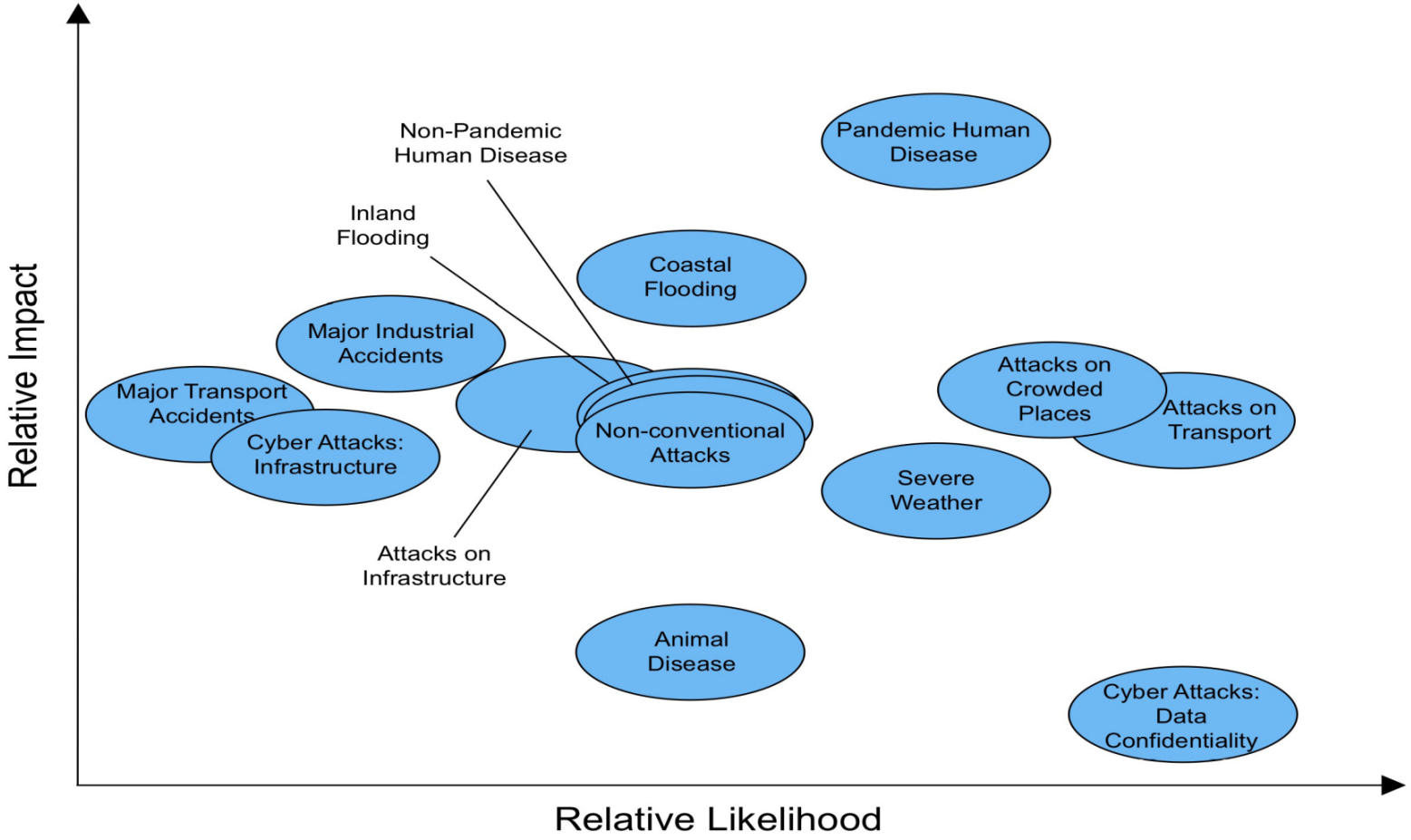
Julho 2011

Cenário de Ameaça

ANACOM

National Risk Register of Civil Emergencies: 2010 Edition

An illustration of the high consequence risks facing the United Kingdom



Cenário de Ameaça (exemplos)

ANACOM

- Quebra no **fornecimento de alimentação de energia** ou noutro fornecimento crítico para o funcionamento da rede ou do serviço;
- **Desastre natural** ou condição climatérica de extrema severidade;
- Quebra súbita do **nível de desempenho** de activos críticos da rede ou do serviço;
- Aumento súbito e extremo na procura dos serviços provocando **situação de sobrecarga**;
- **Ataque físico** a elementos da infra-estrutura da rede ou serviço;
- **Ataque cibernético** a activos da rede ou do serviço, nomeadamente aplicações e sistemas;
- **Situação de pandemia**.

Alterações publicadas a 2009.12.18

ANACOM

	Directiva Quadro	Directiva Serviço Universal	Directiva Privacidade	Directiva Acesso e Interligação	Directiva Autorização
Directiva 2009/140/CE	**XX**			x	**XX**
Directiva 2009/136/CE		**XX**	XX		

Directiva Autorização

A autorização geral para a oferta de redes ou serviços de comunicações electrónicas pode estar sujeita a condições no que diz respeito a condições de utilização :

- para as comunicações das autoridades públicas com o público em geral para o **avisar de ameaças iminentes** e **atenuar as consequências de grandes catástrofes**;
- durante **grandes catástrofes** ou **emergências nacionais**, para assegurar as comunicações entre os serviços de emergência e as autoridades.

Anexo

ANACOM

Directiva Serviço Universal

- Contratos entre OPS e consumidores
- Transparência e publicação de informações
- Disponibilidade dos serviços

Directiva Serviço Universal

O **contrato** especificará, de forma clara, exaustiva e facilmente acessível, no mínimo:

- Informações sobre eventuais procedimentos instaurados pela empresa para **medir e condicionar o tráfego** a fim de evitar esgotar a capacidade num segmento de rede, ou ultrapassá-la...;
- O tipo de medidas que a empresa poderá tomar na **sequência de incidentes** relativos à segurança ou à integridade ou para fazer frente a ameaças e a situações de vulnerabilidade.

Artigo 20.º

Disponibilidade dos serviços telefónicos acessíveis ao público

- Adopção de todas as medidas necessárias para assegurar a **máxima disponibilidade** possível em caso de ruptura catastrófica da rede ou em caso de força maior.
- Adopção de todas as medidas necessárias para assegurar o **acesso ininterrupto aos serviços de emergência**.

Artigo 23.º

Directiva Quadro

- **Novo capítulo sobre Segurança e Integridade de Redes e Serviços**
- Directiva Privacidade passa a directiva específica
- Sem prejuízo para os EM's da adopção de medidas de protecção dos interesses essenciais de segurança, de salvaguarda da ordem pública e da segurança pública, e de investigação, detecção e repressão de actos criminosos

Quadro – Capítulo III

ANACOM

- Os Operadores e Prestadores de Serviço:
  - Adopção de **MEDIDAS TÉCNICAS E ORGANIZACIONAIS**
  - (baseadas)
    - Análise e gestão do risco
    - Estado da técnica (evolutiva)
  - (objectivo)
    - Impedir e minimizar **impacto dos incidentes de segurança**
      - nos **utilizadores** e
      - nas **redes interligadas**

Artigo 13.ºA

Quadro – Capítulo III

ANACOM

- Os Operadores:
  - Adopção de **MEDIDAS DE GARANTIA DE INTEGRIDADE DAS REDES**
  - (objectivo)
    - Assegurar a **continuidade do fornecimento dos serviços** que utilizam essas redes

Artigo 13.ºA

Quadro – Capítulo III

ANACOM

- Os Operadores e Prestadores de Serviço
  - Fazem **Notificação à ARN** de qualquer
    - **Violação da segurança** ou
    - **Perda da integridade**

    com **impacto significativo n**o funcionamento das redes ou serviços.

Artigo 13.ºA

Quadro – Capítulo III

ANACOM

- A Autoridade Reguladora compete:
  - **Tratamento de cada notificação**
    - Informação a outras ARN's e à ENISA (se adequado)
    - Informação ao público em resultado de avaliação de interesse público
      - directamente ou
      - exige que o operador ou prestador o faça
  - **Relatório Anual**
    - sobre notificações e medidas tomadas
    - enviado à Comissão Europeia e à ENISA

Artigo 13.ºA

HARMONIZAÇÃO E NORMALIZAÇÃO

- **MEDIDAS DE EXECUÇÃO** aprovadas pela Comissão Europeia mediante parecer da ENISA
  - No caso das Notificações:
    - Circunstâncias, formato, procedimentos aplicáveis
- **Normas técnicas**
  - Europeias (CEN, CENELEC, ETSI, …) ou
  - Internacionais (ISO/IEC, UIT, IETF, …)

- **Requisitos adicionais** (1 e 2) aprovados pelos Estados Membros

Artigo 13.ºA

Quadro – Capítulo III

ANACOM

- A Autoridade Reguladora pode
  - Emitir **instruções vinculativas** (incl. prazos) aos OPS
  - Exigir **informações e documentação** para
    - Avaliar segurança e/ou integridade redes e serviços
  - Exigir **auditoria de segurança**
    - Organismo qualificado independente ou Autoridade nacional competente
    - Disponibilização resultados à Autoridade Reguladora
    - Custeada pelo Operador ou Prestador de Serviço
  - Investigar **casos de incumprimento** e os seus efeitos sobre a segurança e a integridade das redes

Artigo 13.ºB

Avaliação de Impacto / Decisão de notificação – parâmetros

ANACOM

1. Número de utilizadores afectados
2. Duração do incidente
3. Área geográfica afectada
4. Interligações afectadas
5. Casos especiais:
    a. Combinações dos parâmetros anteriores
    b. Utilizadores específicos
    c. Serviços específicos

a definir posteriormente

Elementos da Notificação

ANACOM

1. Identificação do operador ou prestador de serviço
2. Data/Hora da ocorrência / detecção
3. Breve descrição do incidente
4. Impacto
    a. Tipos de redes e de elementos afectados
    b. Serviços afectados (incluindo serviços de emergência)
    c. Número/proporção de utilizadores afectados
    d. Tempo de restauro (se conhecido)
    e. Região afectada (se conhecida)
5. Breve descrição das acções tomadas até ao momento
6. Nome e detalhes de contacto para seguimento

OFCOM

Situações de Emergência - Aspectos

ANACOM

- Melhoria da **preparação**
  - Estabelecimento de plataforma de conhecimento e de análise de risco
  - Desenvolvimento de planos de contingência e de restauro
  - Realização e participação em exercícios
  - Identificação das lições aprendidas com os exercícios e com casos reais
  - Desenvolvimento de sistema de auditorias
  - Registo de incidentes e das acções tomadas
- Estabelecimento de **comunicações prioritárias** para garantir comunicações vitais
- Promoção da **ajuda mútua** na resposta a emergências
- Identificação e caracterização de **interdependências** com relevo para as interligações nacionais e internacionais
- Reforço da integridade da **cadeia de fornecimento** e da resiliência da **cadeia de produção**

Situações de Emergência: Aspectos

ANACOM

- Melhoria dos **fluxos de informação**
  - Desenvolvimento de plataformas e procedimentos de partilha de informação sensível
  - Estabelecimento de sistema de notificações
  - Melhoria da informação ao utilizador
- Melhoria do **suporte à tomada de decisão**
  - Manutenção da informação de situação agregada
  - Desenvolvimento de conhecimento (histórico)

Objectivos

ANACOM

- Melhoria dos **níveis de disponibilidade** dos serviços prestados mediante:
  - Melhoria da robustez
  - Redução do impacto
    - Minimização do tempo de detecção
    - Eficácia da acção de resposta
    - Limitação da queda dos níveis de desempenho
  - Redução do tempo de recuperação
- Melhoria da **informação ao utilizador**
- Melhoria da **cooperação** nacional e internacional
- Promoção da coerência e articulação do **enquadramento legislativo**
- Análise do **impacto da implementação** das alterações ao quadro

FLUIDEZ NAS COMUNICAÇÕES

ANACOM AUTORIDADE NACIONAL DE COMUNICAÇÕES

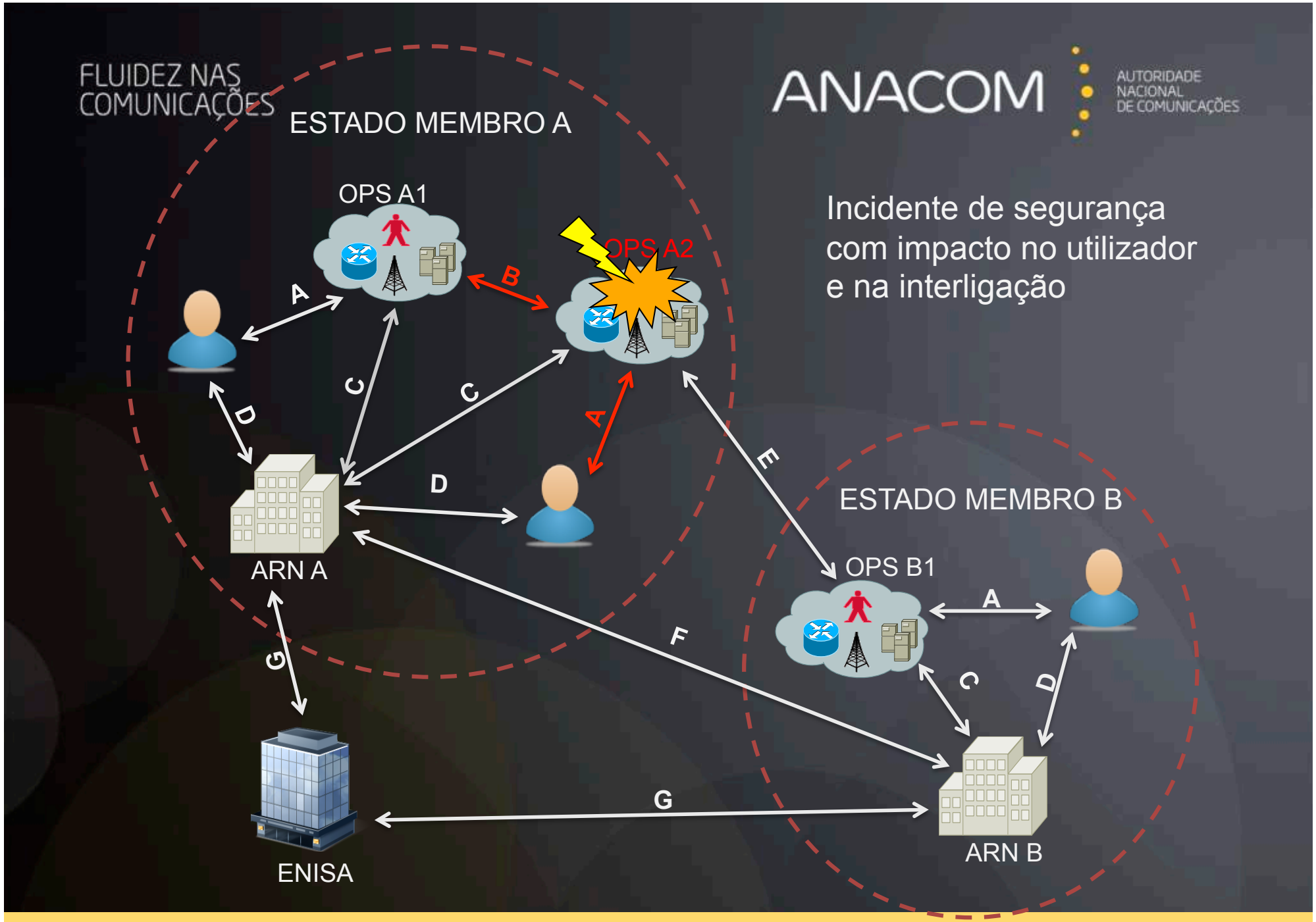
Fluxos de Informação associados a Incidente de Segurança

(visão em sequência)

Artigos 13.ºA e B

FLUIDEZ NAS COMUNICAÇÕES

ANACOM AUTORIDADE NACIONAL DE COMUNICAÇÕES

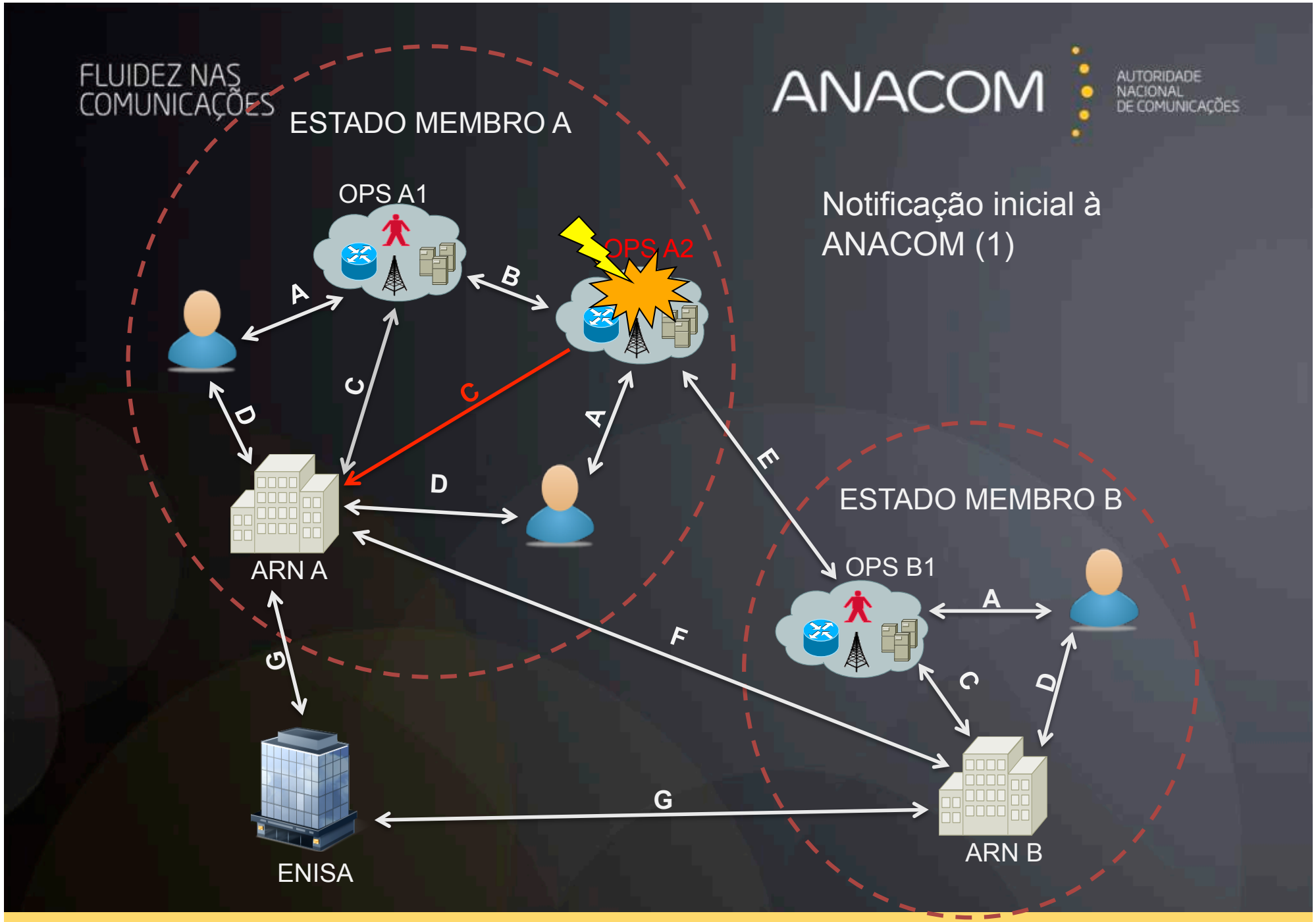


Incidente de segurança com impacto no utilizador e na interligação

FLUIDEZ NAS COMUNICAÇÕES

ANACOM AUTORIDADE NACIONAL DE COMUNICAÇÕES

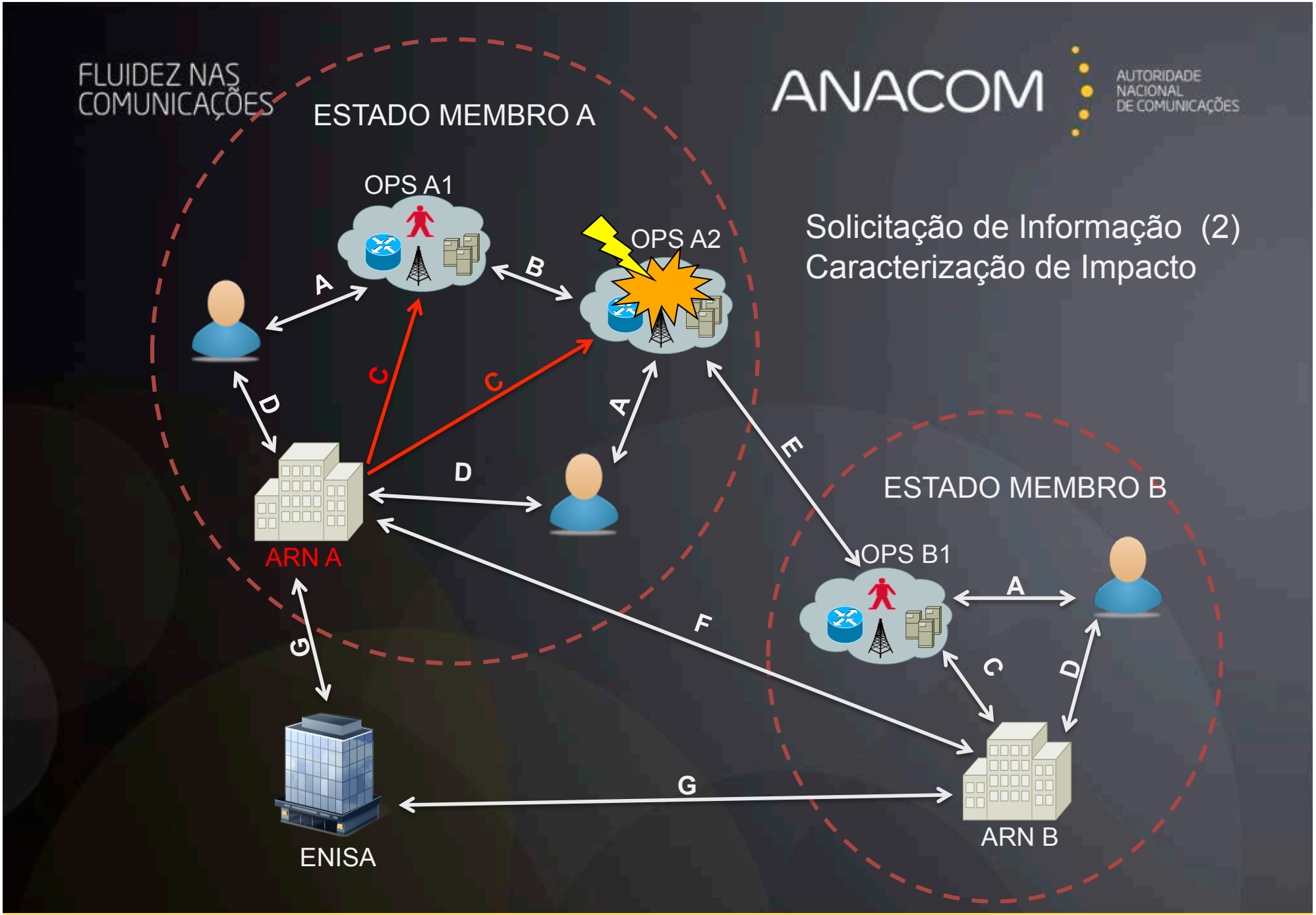
Notificação inicial à ANACOM (1)



FLUIDEZ NAS COMUNICAÇÕES

ANACOM AUTORIDADE NACIONAL DE COMUNICAÇÕES

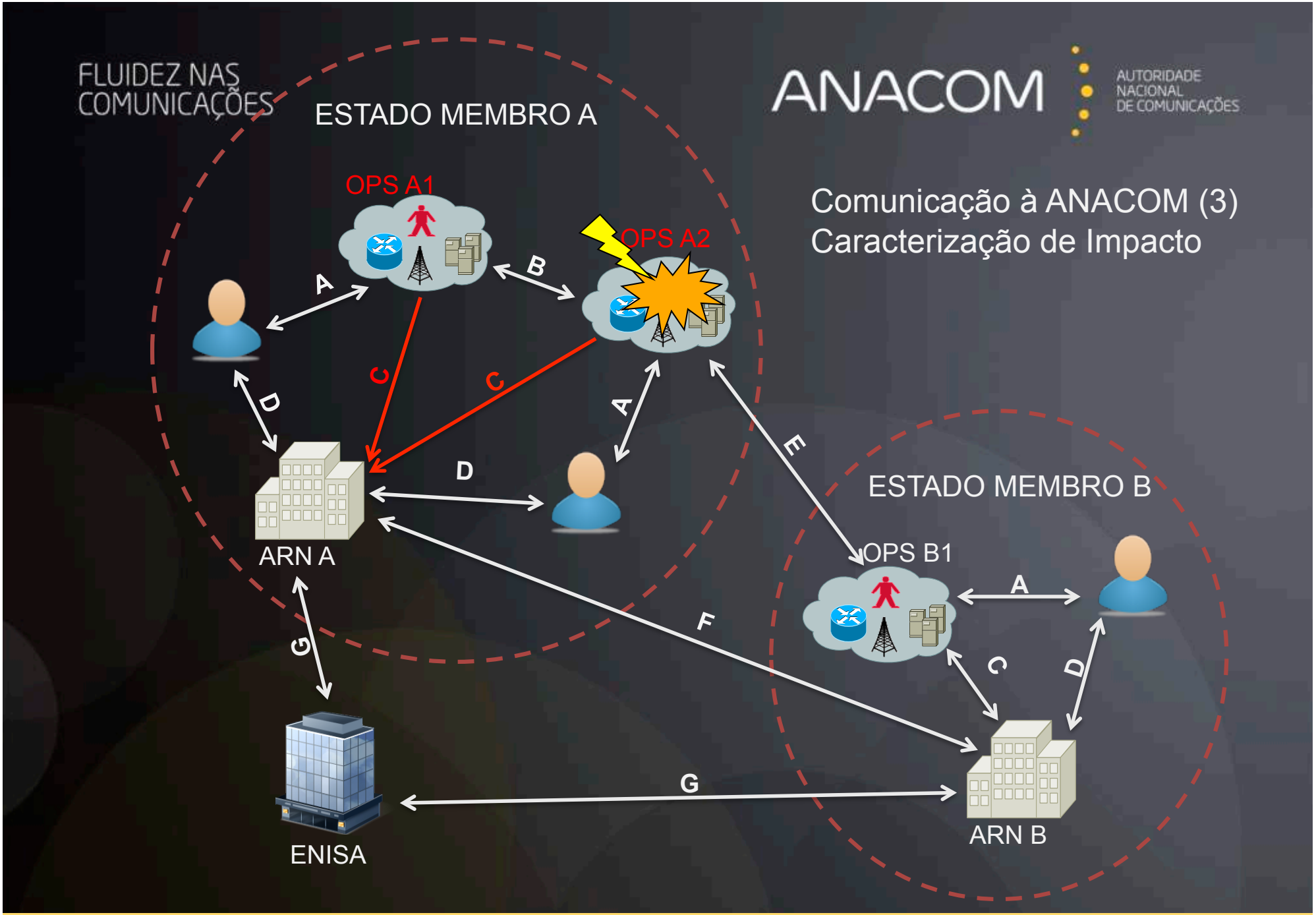
Solicitação de Informação (2)
Caracterização de Impacto



FLUIDEZ NAS COMUNICAÇÕES

ANACOM AUTORIDADE NACIONAL DE COMUNICAÇÕES

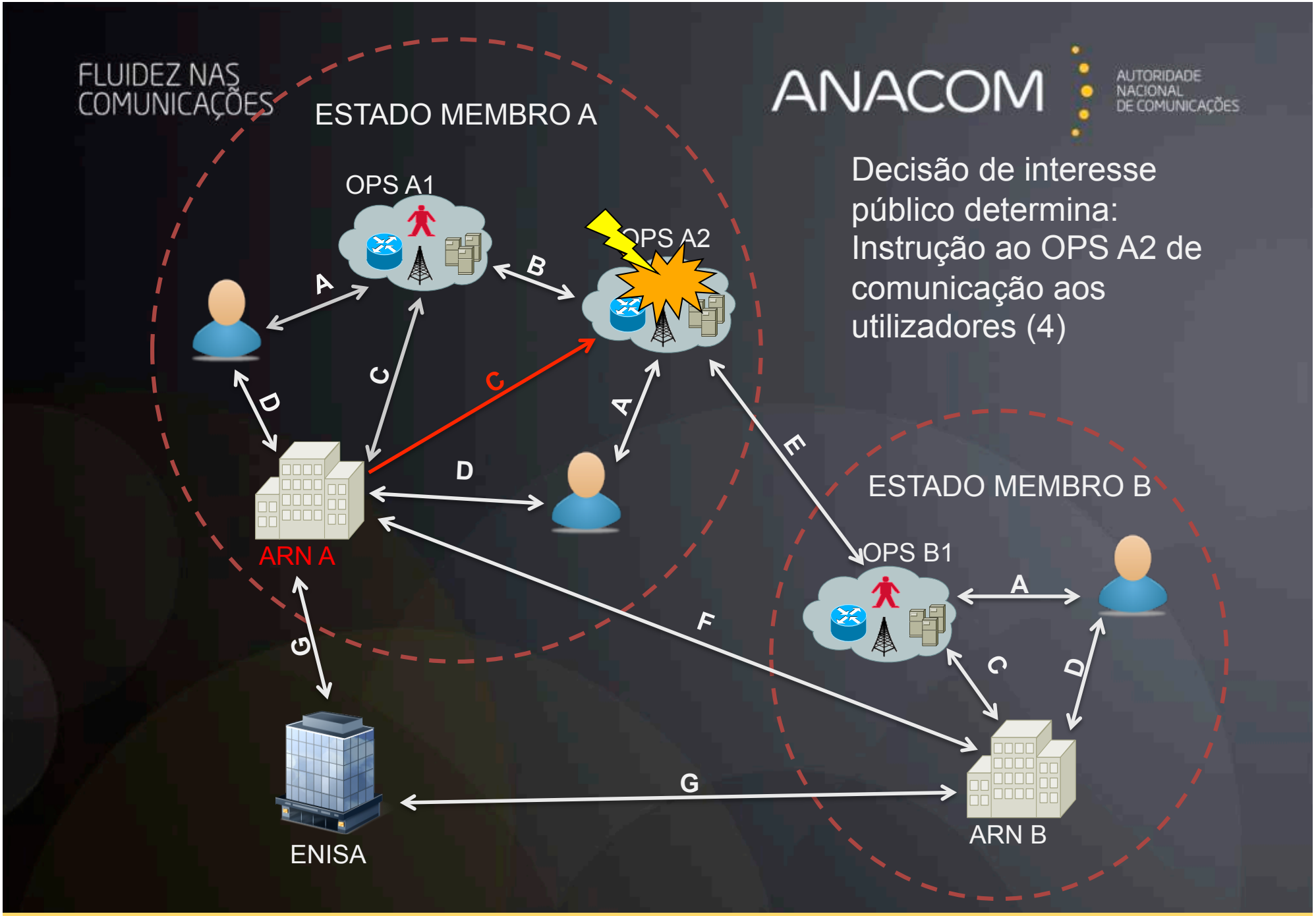
Comunicação à ANACOM (3)
Caracterização de Impacto



FLUIDEZ NAS COMUNICAÇÕES

ANACOM AUTORIDADE NACIONAL DE COMUNICAÇÕES

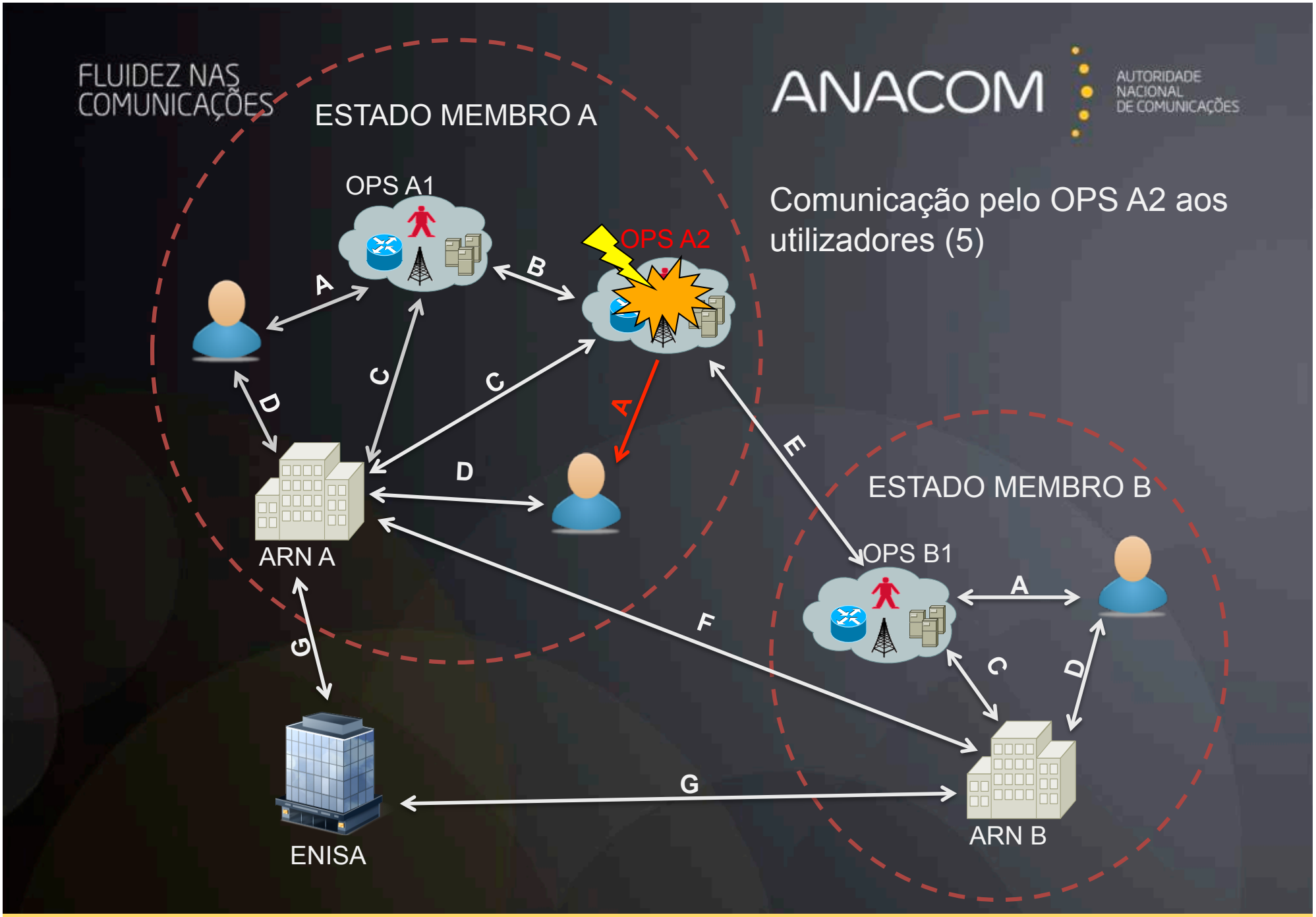
Decisão de interesse público determina: Instrução ao OPS A2 de comunicação aos utilizadores (4)



FLUIDEZ NAS COMUNICAÇÕES

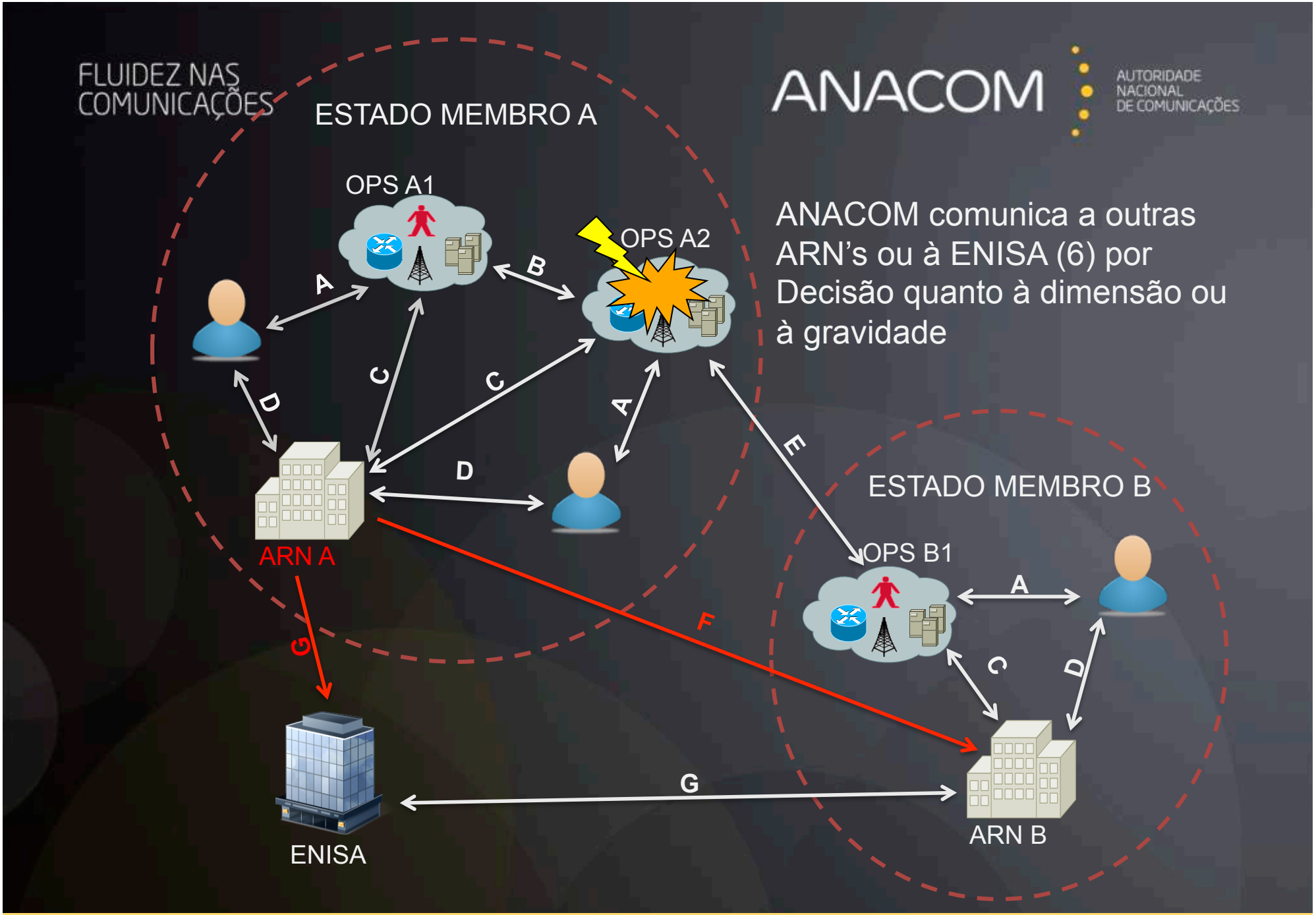
ANACOM AUTORIDADE NACIONAL DE COMUNICAÇÕES

Comunicação pelo OPS A2 aos utilizadores (5)



FLUIDEZ NAS COMUNICAÇÕES

ANACOM AUTORIDADE NACIONAL DE COMUNICAÇÕES

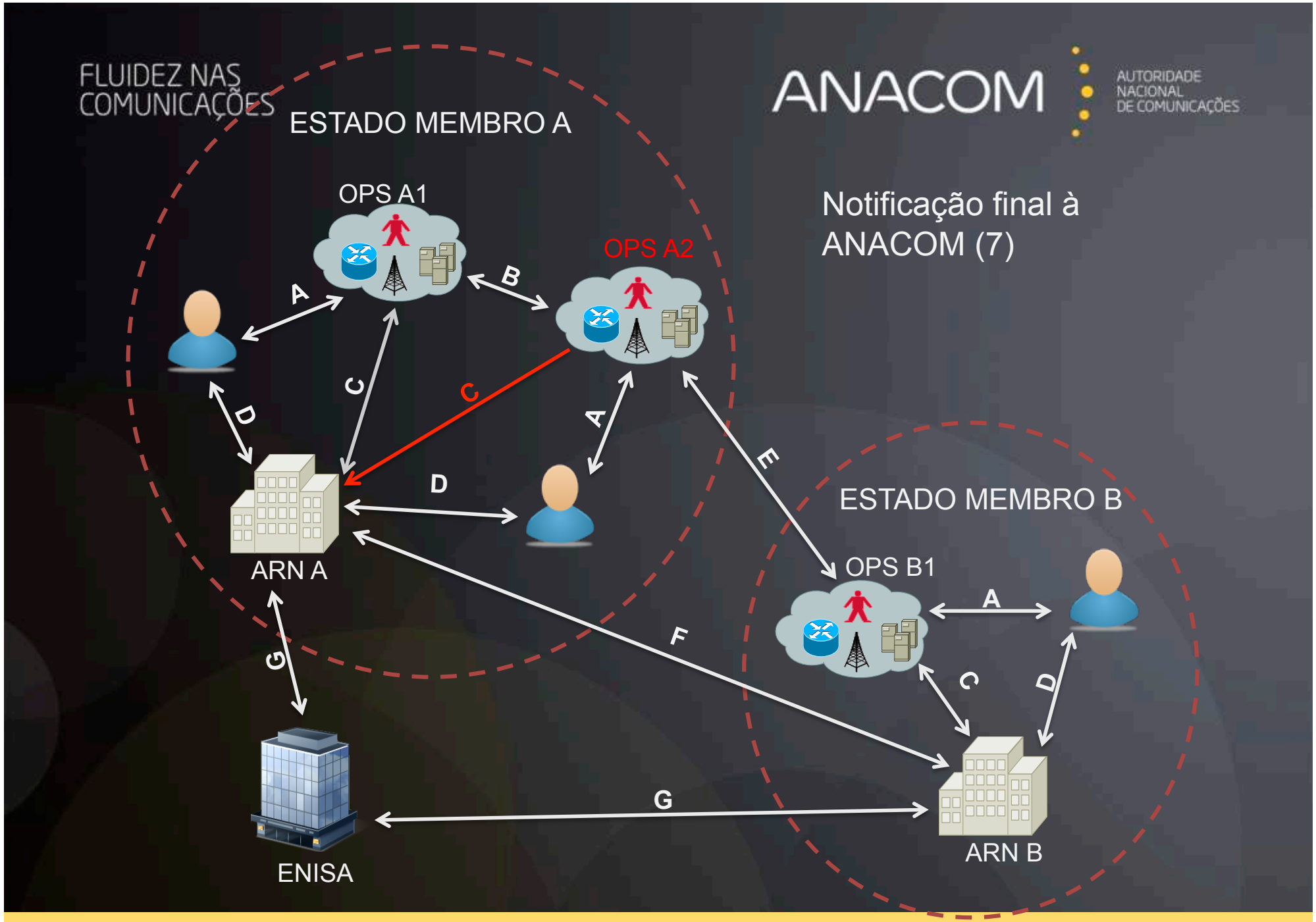


ANACOM comunica a outras ARN's ou à ENISA (6) por Decisão quanto à dimensão ou à gravidade

FLUIDEZ NAS COMUNICAÇÕES

ANACOM AUTORIDADE NACIONAL DE COMUNICAÇÕES

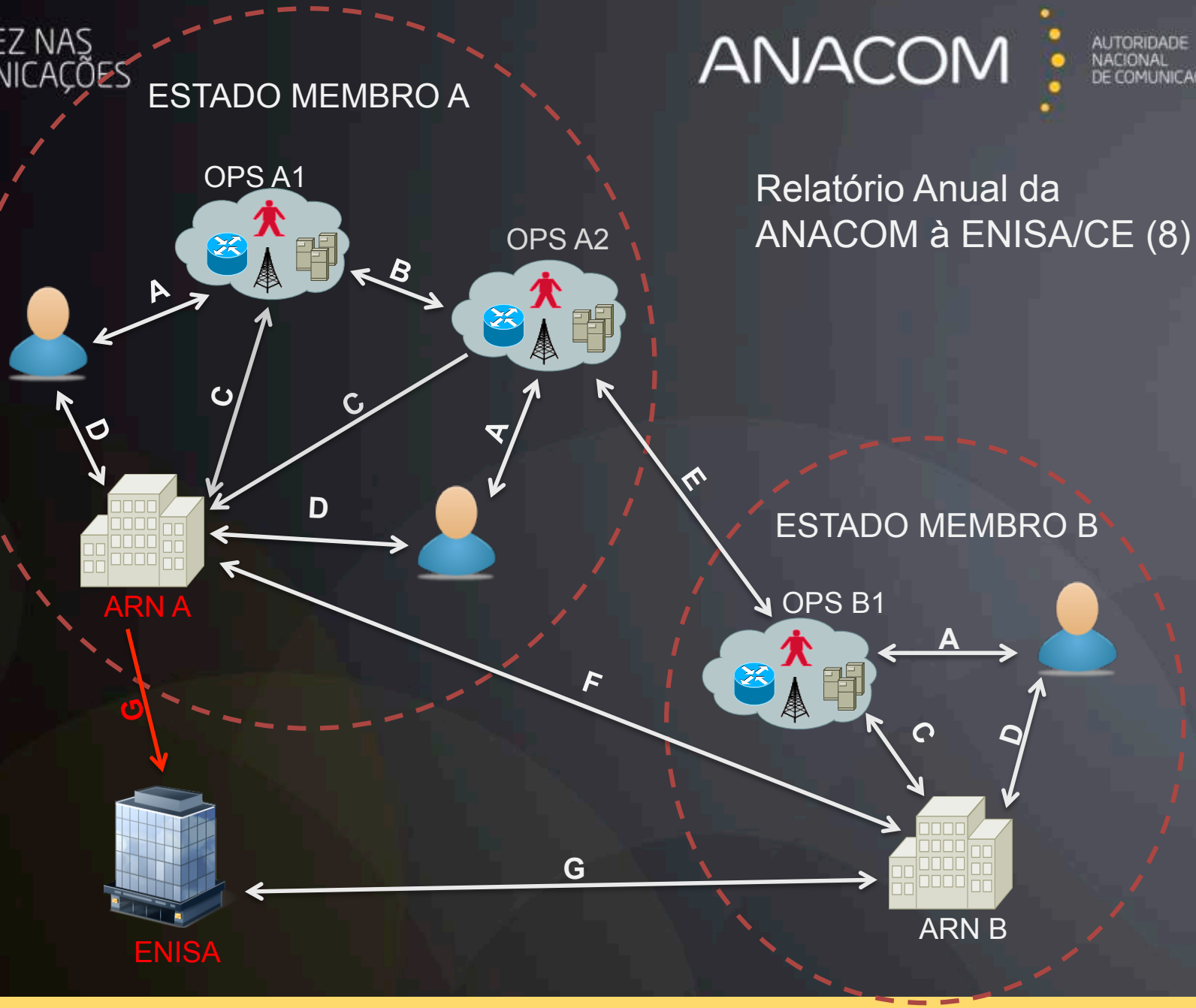
Notificação final à ANACOM (7)



FLUIDEZ NAS COMUNICAÇÕES

ANACOM AUTORIDADE NACIONAL DE COMUNICAÇÕES

Relatório Anual da ANACOM à ENISA/CE (8)



FLUIDEZ NAS COMUNICAÇÕES

ANACOM AUTORIDADE NACIONAL DE COMUNICAÇÕES

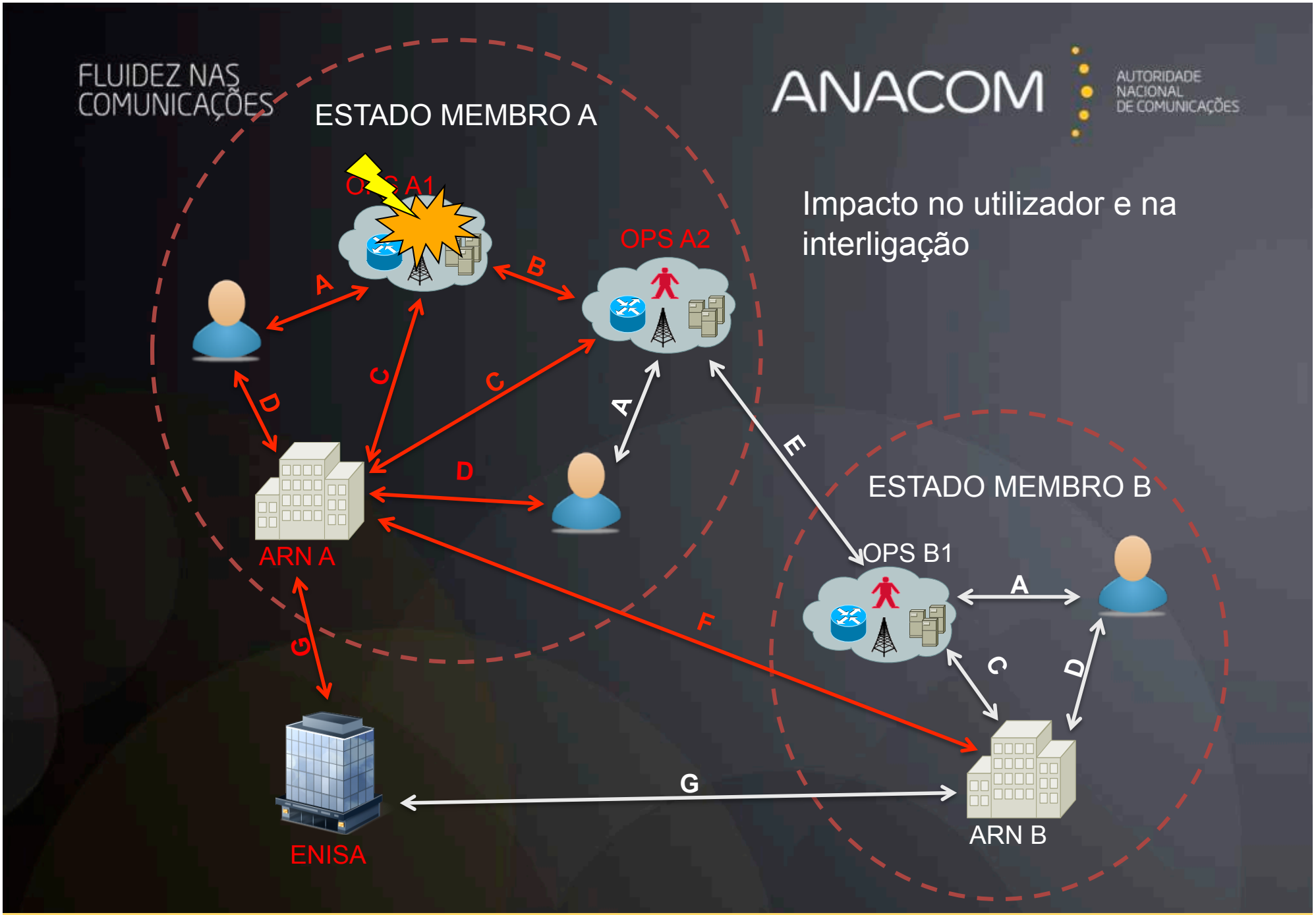
Fluxos de Informação associados a Incidente de Segurança

(visão agregada)

Artigos 13.ºA e B

FLUIDEZ NAS COMUNICAÇÕES

ANACOM AUTORIDADE NACIONAL DE COMUNICAÇÕES

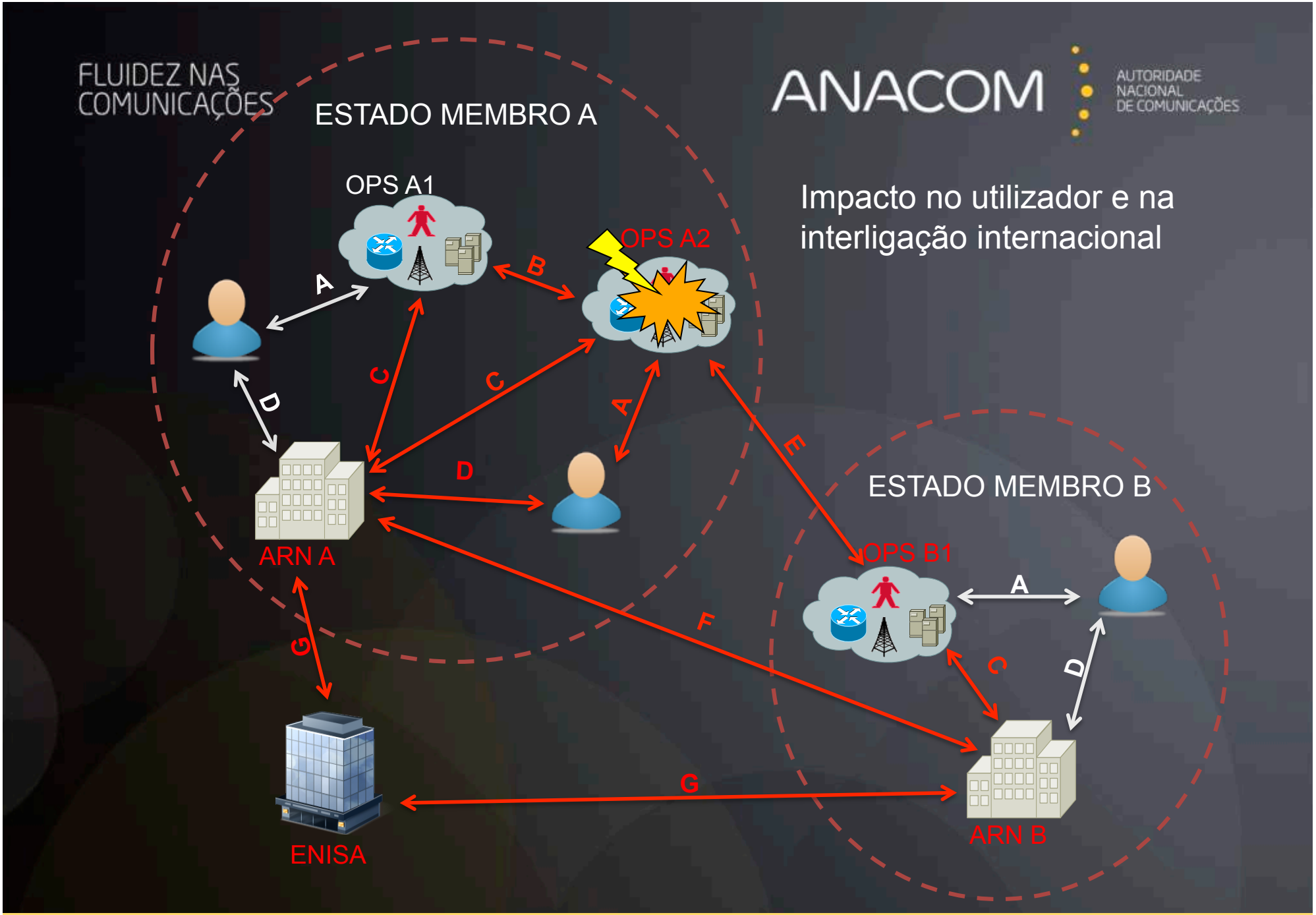


Impacto no utilizador e na interligação

FLUIDEZ NAS COMUNICAÇÕES

ANACOM

AUTORIDADE NACIONAL DE COMUNICAÇÕES



Impacto no utilizador e na interligação internacional

Implementação Harmonizada Art. 13.ºA

ANACOM

- **Metodologia**
  - Facilitação da ENISA
  - Envolvimento e participação das Autoridades Reguladoras/ Competentes
  - Envolvimento dos operadores e prestadores de serviço através das ARN's
- **Objectivos**
  - Análise e gestão de risco
    - Harmonização de metodologia
  - Medidas
    - Identificação de Boas Práticas de Medidas e de Requisitos Mínimos de Segurança
    - Caracterização de modelo de maturidade de segurança
    - Análise de impacto

Implementação Harmonizada Art. 13.ºA

ANACOM

- **Objectivos (cont.)**
  - Incidentes de segurança
    - Formato de notificação com elementos
    - Procedimentos de notificação
  - Impacto significativo
    - Caracterização de métricas / indicadores
    - Caracterização de limiar de notificação
- **Articulação**
  - Plano de Acção Europeu de Protecção às Infra-Estruturas Críticas
    - EP3R – GT Requisitos Mínimos de Segurança
  - Realização de exercícios nacionais e pan-europeus
  - Desenvolvimento de planos de continuidade e de contingência

Referências: directivas europeias

ANACOM

- **Directiva 2002/21/CE** do Parlamento Europeu e do Conselho, de 7 de Março, relativa a um quadro regulamentar comum para as redes e serviços de comunicações electrónicas (directiva - quadro);
- **Directiva 2002/22/CE** do Parlamento Europeu e do Conselho, de 7 de Março, relativa ao serviço universal e aos direitos dos utilizadores em matéria de redes e serviços de comunicações electrónicas (directiva serviço universal);
- **Directiva 2002/20/CE** do Parlamento Europeu e do Conselho, de 7 de Março, relativa à autorização de redes e serviços de comunicações electrónicas (directiva autorização);
- **Directiva 2009/136/CE** do Parlamento Europeu e do Conselho, de 25 de Novembro;
- **Directiva 2009/140/CE** do Parlamento Europeu e do Conselho, de 25 de Novembro.

Referências: normas

ANACOM

- **ISO/IEC 27001/2:2005** – IT - Security techniques -- Information security management systems – Requirements / Code of practice for information security management
- **ISO/IEC 27005:2011** – IT - Security techniques - Information security risk management
- **ITU-T Rec. X.1055 (11/2008)**: Risk management and risk profile guidelines for telecommunication organizations
- **ISO/IEC 24762:2008** - IT — Security techniques — Guidelines for information and communications technology disaster recovery services
- **ISO/IEC 27031:2011** - IT -- Security techniques -- Guidelines for information and communication technology readiness for business continuity

Referências: normas

- **ITU-T Rec. X.1056 (01/2009)** - Security incident management guidelines for telecommunications organizations
- **ITU-T Rec. X.1051 (02/2008)**, Telecommunication security – Information security management guidelines for telecommunications organizations based on ISO/IEC 27002
- **BS 25999 – 1/2** - Business Continuity Management
- **NICC ND 1643** - Minimum security standards for interconnecting communications providers

Referências: outros

- **OFCOM** – Ofcom guidance on security requirements in the revised Communications Act 2003. Implementing the revised EU Framework;
- **ENISA** – Inter-X: Resilience of the Internet Interconnection Ecosystem Report, April 2011;
- **NSTAC** - Report to the President on Communications Resiliency, April 19, 2011;
- **FCC 11-74**, PS Docket No. 11-82, May 13,2011 – Proposed extension of Part 4 of the Commission's Rule regarding to Interconnected Voice over Internet Protocol Service Providers and Broadband Internet Service Providers.

FLUIDEZ NAS COMUNICAÇÕES

ANACOM AUTORIDADE NACIONAL DE COMUNICAÇÕES

FIM

Segurança de Redes e Serviços de Comunicações Electrónicas: As alterações na regulação

IEEE COMMUNICATIONS SOCIETY Portugal Chapter

POSTIT

INSTITUTO SUPERIOR TÉCNICO

Palestras da ComSoc/POSTIT

Manuel Pedrosa de Barros
Direcção de Segurança nas Comunicações