

ISAC

SaúdePT

Termos de Referência

junho de 2023

ÍNDICE

TERMOS DE REFERÊNCIA DO ISAC PARA O SETOR DA SAÚDE PORTUGUÊS	3
EXPOSIÇÃO DE MOTIVOS E CONTEXTO	3
I. NORMAS GERAIS.....	4
§ 1º Objeto e âmbito.....	4
§ 2º Missão.....	4
§ 3º Objetivos.....	4
§ 4º Princípios.....	4
II. ORGANIZAÇÃO E FUNCIONAMENTO	5
§ 5º Composição	5
§ 6º Perda da qualidade de Membro ou Parceiro	5
§ 7º Integração no ISAC.....	5
§ 8º Representação dos Membros ou Parceiros.....	6
§ 9º Direitos e deveres	6
§ 10º Reuniões	6
§ 11º Partilha de Informação	7
§ 12º Alteração dos Termos.....	8
ANEXO A.....	9
ANEXO B.....	10
ANEXO C.....	11
ANEXO D	12

TERMOS DE REFERÊNCIA DO ISAC PARA O SETOR DA SAÚDE PORTUGUÊS

EXPOSIÇÃO DE MOTIVOS E CONTEXTO

A prestação de cuidados de saúde encontra-se progressivamente dependente das tecnologias de informação e de comunicação (TIC), o que a sujeita a específicas e complexas vulnerabilidades a ameaças que, pela sua natureza, permanentemente evoluem e mutam de formas não antecipáveis.

Qualquer perturbação no setor da Saúde, facilmente propicia impactos consideráveis na transversalidade da sociedade e economia de toda uma região ou país. A sua proteção suscita, por isso, compreensíveis preocupações a diferentes níveis e por diferentes atores que compõem o Sistema de Saúde, bem como pela sociedade em geral.

Os Centros de Análise e Partilha de Informação ou “ISAC” por referência à expressão na originária de língua inglesa) são parcerias para troca de informação e experiência sobre segurança cibernética e assentam no inequívoco pressuposto de que a partilha consistente e estruturada de informações e análise de incidentes, ameaças, tendências e boas práticas favorece a resiliência digital.

O desenvolvimento das atividades dos ISAC assentam sobretudo num princípio de confiança entre os seus elementos, como fator essencial para levar a cabo os desígnios a que se propõem.

As especificidades do setor da saúde e o impacto da sua atividade para a sociedade em geral, tornam particularmente relevante a criação de estruturas que contribuam para uma maior, segurança no ciberespaço e privacidade de dados neste setor.

A criação de um Centro de Análise e Partilha de Informação específico do setor da saúde resulta da necessidade de uma abordagem global e integrada por parte dos diferentes operadores deste setor, face aos desafios atuais no que respeita à segurança das redes e dos sistemas de informação.

Para um adequado funcionamento, é essencial que o ISAC se encontre suportado por regras claras e objetivamente definidas, que estabeleçam, designadamente, o propósito e o objetivo da sua atuação, as regras básicas para troca de informações e os procedimentos essenciais ou outras regras necessários para assegurar a partilha de informações.

Neste contexto, foram elaborados os presentes Termos de Referência com o propósito de regular a atividade do ISAC do setor da saúde, pressupondo-se a sua assinatura por parte de todos os elementos que o integram, como forma de manifestação expressa do compromisso assumido e do alinhamento com os seus objetivos.

I.NORMAS GERAIS

§ 1º Objeto e âmbito

1. Os Presentes Termos de Referência (TdR) têm por objeto regular a organização e funcionamento do Centro de Análise e Partilha de Informação do Setor da Saúde em Portugal (adiante ISAC ou ISAC SaúdePT).
2. O ISAC consiste num fórum de cooperação entre equipas de cibersegurança de organizações que operam no Setor da Saúde.
3. Os TdR aplicam-se a quem integre o ISAC, aceitando subscrever os mesmos.

§ 2º Missão

É missão do ISAC aumentar a resiliência do setor a incidentes cibernéticos, por via da consistente partilha de informação e experiência, assente num ambiente de confiança.

§ 3º Objetivos

São objetivos do ISAC:

- a) Criar laços de confiança entre os seus membros, a fim de promover um ambiente de colaboração e assistência mútua, com vista ao incremento da ciber-resiliência do setor;
- b) Estabelecer uma plataforma comum para partilha de conhecimento e de indicadores de cibersegurança, nomeadamente através da partilha de situações de ameaças, vulnerabilidades e incidentes;
- c) Analisar problemas e soluções relevantes para o setor;
- d) Promover referenciais e boas práticas para o setor.

§ 4º Princípios

1. O ISAC pauta-se pelos seguintes princípios:
 - a) Colaboração, através da participação ativa de todos os seus elementos;
 - b) Confidencialidade e sigilo, a fim de promover uma relação de confiança entre os seus elementos;
 - c) Compromisso de todos os seus elementos com a missão do ISAC e com objetivos estabelecidos;
 - d) Partilha, através da disponibilização de informação de qualidade, de forma consistente e organizada.
2. As opiniões, ideias, dúvidas ou propostas partilhadas por qualquer dos membros ou dos seus representantes no âmbito do ISAC devem ser exclusivamente interpretadas no

contexto do próprio ISAC e não prejudicam, projetam ou vinculam quaisquer posições externas.

3. A informação partilhada no ISAC pressupõe-se sensível e deve ser tratada como tal por todos os que o integrem.

II. ORGANIZAÇÃO E FUNCIONAMENTO

§ 5º Composição

1. Podem integrar o ISAC SaúdePT as entidades públicas, privadas e instituições do setor social que operem em Portugal e que pertençam ao setor.
2. O ISAC é composto pelo Promotor, Membros e Parceiros.
3. O Centro Nacional de Cibersegurança (CNCS) é, no âmbito das suas competências e no cumprimento da sua missão, promotor do ISAC, assegurando o apoio logístico e administrativo necessário ao funcionamento do mesmo, participando em todas as atividades que os Membros tenham por adequadas
4. Os Membros são as entidades do setor da saúde que aderem ao ISAC de acordo com os presentes TdR.
5. Os Parceiros são as entidades convidadas a integrar o ISAC, considerando os contributos específicos e especializados, no âmbito das respetivas áreas de atuação, para a prossecução dos objetivos deste.
6. Excluem-se do âmbito do ISAC as agências, entidades, órgãos de polícia criminal e outras autoridades que devam ser notificadas de incidentes ou outras ocorrências no contexto da cibersegurança.

§ 6º Perda da qualidade de Membro ou Parceiro

1. Qualquer Membro ou Parceiro pode, a todo o tempo, solicitar o cancelamento da sua participação no ISAC, mediante comunicação escrita dirigida ao Promotor.
2. Qualquer Membro ou Parceiro pode, a todo o tempo, ser excluído do ISAC, com fundamento em ter deixado de constituir uma mais-valia para o mesmo, quando pratique atos contrários aos objetivos e princípios do ISAC ou que sejam aptos a causar prejuízo ao ISAC ou a algum dos seus Membros.
3. A decisão de exclusão depende da unanimidade de votos dos demais Membros.
4. O cancelamento da participação ou exclusão de qualquer Membro ou Parceiro não o isenta de cumprir os deveres de confidencialidade e sigilo a que se tenham vinculado no âmbito do ISAC.

§ 7º Integração no ISAC

1. A integração no ISAC é feita após convite do Promotor, previamente consensualizado entre os seus Membros.

2. A integração como membro ou parceiro do ISAC deverá ser precedida do integral preenchimento e remessa ao secretariado, que é assegurado pelo Promotor, do documento que integra o ANEXO B.
3. Os candidatos a membro ou parceiro deverão constituir um valor acrescido para o ISAC, por referência à sua missão.
4. A integração no ISAC implica a aceitação integral e sem reservas dos TdR, através do preenchimento e assinatura de documento elaborado em conformidade com o modelo constante do ANEXO A.

§ 8º Representação dos Membros ou Parceiros

1. Os membros e os parceiros são representados por um elemento da sua entidade especialmente designado para o efeito, designado por representante principal.
2. Para além da designação do representante principal, cada entidade poderá, caso o entenda, indicar outros representantes, até um máximo de três.
3. Cada representante deve ter legitimidade e autonomia para partilhar as informações e, sempre que aplicável, participar nas deliberações necessárias à prossecução dos objetivos do ISAC.
4. Os membros e os parceiros podem requerer a todo o tempo a alteração dos seus representantes, devendo para esse efeito remeter o formulário constante do ANEXO C, devidamente preenchido.

§ 9º Direitos e deveres

1. Constituem direitos dos membros do ISAC:
 - a) Ser informados das reuniões do ISAC;
 - b) Participar nas atividades do ISAC;
 - c) Indicar ao Promotor assuntos a incluir nas reuniões do ISAC.
2. São deveres dos membros:
 - a) Constituir uma mais-valia para o ISAC, partilhando informação relevante e de qualidade;
 - b) Não comprometer a disponibilidade, confidencialidade ou integridade da informação partilhada no âmbito do ISAC;
 - c) Adotar a plataforma de comunicação do ISAC, que estiver em uso;
 - d) Abster-se de praticar atos contrários aos objetivos e princípios do ISAC, ou que sejam aptos a causar prejuízo ao ISAC ou a algum dos seus membros.

§ 10º Reuniões

1. O ISAC reúne, de forma presencial ou por meios telemáticos, pelo menos, quatro vezes ao ano, devendo uma dessas reuniões ser de carácter presencial.
2. As reuniões são presididas pelo Promotor, a quem compete estabelecer a ordem do dia, incluindo os assuntos que para essa finalidade lhe forem atempadamente propostos.
3. As reuniões são convocadas pelo Promotor, com uma antecedência mínima de 48 horas relativamente à sua realização, salvo motivos de urgência imperiosa.
4. O ISAC só pode, em regra, deliberar quando a maioria do número dos seus membros com direito a voto esteja fisicamente presente ou a participar através de meios telemáticos.
5. Cada membro tem direito a um voto nas deliberações sobre os assuntos que sejam submetidos ao ISAC, através do representante nomeado para o efeito.
6. As deliberações são tomadas por maioria de votos dos membros presentes à reunião, salvo nos casos em que, se exija maioria qualificada ou unanimidade.
7. As reuniões do ISAC decorrem de acordo com a regra “Chatham House”, pelo que a informação nelas partilhada deve salvaguardar o anonimato de dados pessoais, nomeadamente a identificação do seu autor.
8. As opiniões expressas pelos representantes dos membros ou parceiros durante as reuniões não serão tratadas como a posição formal da organização que representam.
9. Apenas os representantes nomeados podem assistir às reuniões presenciais ou por via telemática, sendo individualmente responsáveis por assegurar a confidencialidade e segurança da informação a que acedam no âmbito do ISAC.
10. Por convite dos representantes, podem participar nas reuniões e atividades do ISAC, sem direito a voto, outros elementos ou colaboradores dos Membros Representados.
11. O ISAC pode convidar a participar nas suas reuniões e atividades, entidades ou personalidades que possam ter uma intervenção relevante para as temáticas em apreciação, bem como solicitar contributos específicos no âmbito das respetivas áreas de atuação.
12. As participações do Promotor e dos Parceiros nas reuniões ou atividades do ISAC poderão ser definidas casuisticamente pelos Membros.

§ 11º Partilha de Informação

1. Todos os elementos do ISAC que integrem participem ou participem em atividades, em representação do Promotor, Membros, ou Parceiros devem aceitar e assinar o Acordo de Confidencialidade que integra o ANEXO D.
2. O ISAC utiliza o protocolo Traffic Light Protocol (TLP), versão 2.0, para determinar o nível de sensibilidade da informação partilhada, sendo responsabilidade dos Membros e Representantes o seu estrito respeito.
3. As quatro classificações por cores são, nos termos daquele protocolo, as seguintes:
 - a) **TLP:RED** = Informação não partilhável, destinada apenas aos presentes. Se apresentada na forma escrita, devem todos os suportes ser destruídos no fim da reunião. Os Representantes estão impedidos de discutir a informação fora da reunião.

- b) **TLP:AMBER+STRICT** = Informação suscetível de partilha apenas com Membros e Promotor.
 - c) **TLP:GREEN** = Informação suscetível de partilha com entidades externas ao ISAC que dela extraíam benefício. Ficam excluídas publicações de qualquer tipo na Internet.
 - d) **TLP:CLEAR** = Informação suscetível de partilha sob qualquer forma, sendo as únicas restrições eventuais direitos de autor.
- 4. É da responsabilidade do Promotor, Membros e Parceiros, a classificação de qualquer informação que, por qualquer meio, partilhem.
 - 5. A ausência de classificação determina que a informação em causa tenha a classificação TLP:AMBER+STRICT e a identidade de quem a partilhou TLP:RED.
 - 6. Todos os contactos, discussões e partilhas de informação no âmbito do ISAC devem exclusivamente ocorrer pelos meios e no âmbito da(s) plataforma(s) expressamente pré-determinadas pela unanimidade dos membros, carecendo a sua eventual substituição ou modificação da aprovação também por unanimidade.
 - 7. Os meios e plataformas referidos no número anterior devem ser usados estritamente para os expressos fins do ISAC.
 - 8. A publicação de informação partilhada no âmbito do ISAC carece do expresse consentimento de todos os membros.
 - 9. O ISAC não constitui um instrumento de queixa ou denúncia de natureza criminal ou de prestação de informação a autoridades.

§ 12º Alteração dos Termos

A alteração dos TdR só podem ocorrer por deliberação tomada por maioria qualificada, correspondente a 2/3 dos membros.

ANEXO A

ACEITAÇÃO DOS TERMOS DE REFERÊNCIA

REPRESENTANTE PRINCIPAL

NOME COMPLETO:

ENDEREÇO DE EMAIL:

CONTACTO TELEFÓNICO:

CARGO E/OU FUNÇÃO(ÕES) EFETIVAMENTE EXERCIDA(S) AO SERVIÇO DO MEMBRO:

OUTROS REPRESENTANTES

NOME COMPLETO:

ENDEREÇO DE EMAIL:

CONTACTO TELEFÓNICO:

CARGO E/OU FUNÇÃO(ÕES) EFETIVAMENTE EXERCIDA(S) AO SERVIÇO DO MEMBRO:

NOME COMPLETO:

ENDEREÇO DE EMAIL:

CONTACTO TELEFÓNICO:

CARGO E/OU FUNÇÃO(ÕES) EFETIVAMENTE EXERCIDA(S) AO SERVIÇO DO MEMBRO:

NOME COMPLETO:

ENDEREÇO DE EMAIL:

CONTACTO TELEFÓNICO:

CARGO E/OU FUNÇÃO(ÕES) EFETIVAMENTE EXERCIDA(S) AO SERVIÇO DO MEMBRO:

Declaro conhecer, compreender e aceitar todas as cláusulas dos Termos de Referência do ISAC SaúdePT, designadamente as regras relativas à partilha de informação, e expressamente reconheço a sensibilidade e confidencialidade da informação partilhada.

Data: _____

Assinatura(s)

ANEXO B

FORMULÁRIO DE ADESÃO

Nome da entidade

Objeto da(s) atividade(s)

Sede

Endereço(s) de email

Contacto telefónico

Valor acrescido oferecido pela entidade

Identificação do Representante Principal

1. Nome completo:

Cargo e funções efetivamente exercidas no candidato:

Data: ____/____/____

Assinatura

ANEXO C

PEDIDO DE ALTERAÇÃO DE REPRESENTANTE

Identificação do atual Representante do Membro a ser substituído

Nome completo:

Identificação do Representantes em substituição do atual

Nome completo:

Cargo e funções efetivamente exercidas na pessoa candidata:

Motivação para a pretendida substituição

ANEXO D

ACORDO DE SIGILO DA COMUNIDADE ISAC

É assumido entre Membros, Promotor e Parceiros o seguinte acordo de sigilo (“Acordo”):

1. Objecto

O presente Acordo tem por objeto garantir o sigilo e proteção da Informação que seja trocada ou divulgada entre representantes dos Membros, Promotor e Parceiros do ISAC SaúdePT (“Partes”).

2. Informação Sigilosa

- a. Considera-se, para efeitos do presente Acordo, "Informação Sigilosa" toda a informação transmitida no âmbito da atividade do ISAC, ou a que uma Parte tenha acesso ou acedido naquele contexto — independentemente do modo ou do suporte de comunicação — designadamente informação de natureza organizativa, técnica, comercial ou financeira, a relativa a produtos ou serviços, relações com clientes e fornecedores, bases de dados, técnicas e métodos de trabalho, logística, programas, aplicações e soluções relativas a tecnologias de informação, a sua configuração e comportamento, marketing, investigação e desenvolvimento de produtos, estratégias comerciais em curso e em perspectiva, informação relativa a direitos de propriedade intelectual, em especial direitos de autor e direitos conexos e afins de cada uma das Partes, designadamente ideias, conceitos, esquemas, protótipos, materiais e métodos de análise concepção e de preparação, documentação técnica e documentação de utilização que estejam ou possam estar na génese ou em relação com tais direito e quaisquer outras que as Partes classifiquem como sigilosa.
- b. Não é, para efeitos do presente Acordo, considerada Informação Sigilosa a que seja já conhecida por uma das Partes independentemente de divulgação por outra Parte ou do conhecimento da actividade desta nem informação que seja, ou se tenha tornado, do conhecimento público, salvo se tal decorrer do incumprimento do presente Acordo.

3. Exclusões

Exclui-se do presente Acordo qualquer informação que a Parte informante autorize expressamente a sua divulgação a terceiros.

4. Obrigação de Sigilo

- a. As Partes comprometem-se a manter a Informação Sigilosa em regime de sigilo e estrita confidencialidade, não copiar total ou parcialmente, alterar o seu conteúdo e/ou a comunicá-la a terceiros.
- b. As Partes obrigam-se a impedir, por todos os meios lícitos ao seu dispor, que a Informação Sigilosa seja divulgada a terceiros.
- c. As Partes obrigam-se a não comentar junto de terceiros qualquer aspecto da actividade das outras Partes, ou do seu relacionamento com ela, a menos que estejam em causa factos de conhecimento público.
- d. As Partes obrigam-se a transmitir às outras todas as informações pertinentes, ainda que se trate de Informação Sigilosa, que lhe sejam solicitadas com a finalidade de verificar o bom cumprimento do presente Acordo.
- e. Nenhuma das Partes poderá utilizar o nome das outras para fins publicitários, comerciais ou outros sem o prévio consentimento por escrito.

5. Cumprimento de Ordens Judiciais e Administrativas

- a. As Partes encontram-se autorizadas a divulgar Informação Sigilosa em cumprimento de decisão judicial ou administrativa não suscetível de recurso ou cujo recurso não possua efeito suspensivo na estrita medida necessária a assegurar o cumprimento de tal ordem.
- b. Nos casos previstos na alínea anterior, a Parte obrigada ao cumprimento da ordem judicial ou administrativa deve informar previamente as demais Partes e observar as recomendações compatíveis com a obrigação legal, e a fazer acompanhar tal divulgação da indicação de que se trata de Informação Sigilosa.
- c. As Partes obrigam-se, nos casos referidos nas alíneas anteriores, e sem prejuízo das obrigações decorrentes da lei, a concertarem posições e a desenvolverem esforços com vista a evitar ou limitar a revelação de Informação Sigilosa, nomeadamente pela prática conjunta das diligências adequadas à proteção dos respetivos interesses.

5. Responsabilidade

A violação das regras de sigilo previstas no presente Acordo constituirá incumprimento do mesmo suscetível de responsabilidade civil pelos danos e prejuízos causados às Partes e ao ISAC SaúdePT

6. Termo da obrigação de sigilo

- a. O presente Acordo vigora enquanto as Partes integrarem, na qualidade de representantes, o ISAC SaúdePT e por um período de cinco anos após cessação das demais obrigações que com aquele assumam.
- b. As Partes comprometem-se, durante o período de vigência e responsabilidade decorrente do presente Acordo, a restituir ou destruir, no prazo e conforme solicitado,

todos os elementos de Informação Sigilosa em seu poder, independentemente da forma que assumam e do suporte em que se encontrem vertidos.

7. Comunicações

As comunicações efectuadas entre as Partes para efeitos do presente Acordo serão realizadas por carta ou correio electrónico e por intermédio do secretariado do ISAC SaúdePT

8. Alterações

Qualquer alteração ao presente Acordo deverá revestir a forma de documento escrito, assinado por todas as Partes.

9. Competência

Para a resolução de quaisquer litígios emergentes do presente Acordo, designadamente quanto à sua interpretação, aplicação, validade, execução, cumprimento e termo, as partes atribuem competência exclusiva ao Tribunal da Comarca de Lisboa.

Feito em duplicado, ficando um exemplar, devidamente assinado, em poder de cada uma das partes

Lisboa, _____
