Análise dos dados – P1. Experiência

1. Dados das entrevistas

Variável dependente – Participante

P1.V1.1

P1.V1.1 – P1ULSNA#01	Sem dúvida. A PDS é também um exemplo que está a obrigar as pessoas a pensar de maneira diferente, apesar de ainda não estar suficientemente difundida, e o seu conceito interiorizado nos profissionais para que estes vejam a PDS como uma boa ferramenta de trabalho. A PDS é um excelente exemplo de partilha de dados. Faz sentido a partilha de dados quando os utentes "saltam" muito entre instituições de saúde. Se nos hospitais ou nos centros de saúde, principalmente nos hospitais, não houver um rigor na disponibilização de informação, porque existe muita gente que não disponibiliza informação em formato eletrónico, a qualidade da informação disponibilizada acaba por retrair os profissionais na sua utilização.
P1.V1.1 – P2ULSNA#02	Com toda a certeza, quanto mais projetos maior a experiência. É o caso da PDS, projeto nacional, e pequenas ligações a bases de dados do hospital de Évora, onde obtemos dados de exames feitos lá, que não conseguirmos fazer localmente. A própria troca de informação a nível de videoconferência, partilha de informação clinica, apesar de resumida entre especialistas.
P1.V1.1 – P2ULSNA#03	Completamente, eu acho que sim. Ou seja, aqui internamente, o início de atividade de um novo profissional com excelentes conhecimentos em informática, mas que não consegue associar estes conhecimentos à área da saúde, os conhecimentos práticos que tem não lhe irão servir de nada. Temos um projeto de interoperabilidade, que embora interno é abrangente, trata-se de uma plataforma que pesquisa dados em várias aplicações.
P1.V1.1 – P1USF#01	Está, acima de tudo dependente disso. Ou seja, quanto mais experiência os profissionais tiverem dentro deste domínio, mais garantido está o sucesso da proteção de dados. É necessária uma disponibilidade dos profissionais para a partilha de dados.
P1.V1.1 – P2USF#02	Acho que sim. Mesmo antigamente em que os sistemas funcionavam de forma isolada, já existia alguma preocupação com estas questões. A preocupação não era tanta como hoje. Não tínhamos que nos preocupar muito porque estava tudo dentro da nossa "ilha". Os níveis de acesso eram suficientes para controlar tudo. Agora não. Temos uma quantidade, é quase uma estrela a nível de rede, a tentar aceder aos dados e soluções, o que obriga a assegurar a proteção e segurança. As organizações estão muito cientes em relação a isto. Existe um contexto propício para que sejam consideradas as questões da proteção de dados a "sério".
P1.V1.1 – P1INEM#01	Pode depender muito. Se eu tiver uma má experiência de certeza que eu não quero abraçar outra iniciativa nos próximos tempos. Quando existir consciência do benefício, nunca financeiro mas em termos de confiança, que existe com a partilha de dados, vai ser mais fácil promover o seu desenvolvimento. Por exemplo o facto de obtermos os dados de identificação do cartão do utente através da PDS, para além de nos poupar imenso tempo no registo destes dados, permitiu-nos a nós internamente também termos uma fonte fidedigna, um histórico de informação – é possível saber se para um utente, já houve intervenções anteriores (…) o que em algumas situações pode fazer a diferença. Pode permitir por exemplo um suporte à decisão de transportar ou não o utente numa situação.

	Numa fase iniciar as pessoas são muito sépticas quanto às soluções de integração e recolha de dados, mas depois quando começam a aperceber-se dos benefícios, são os principais dinamizadores destas soluções.
P1.V1.1 – P2INEM#03	Neste momento e como está tudo muito vago, sim. Quanto mais experiência a equipa tiver dentro destas áreas, mais fácil se implementa políticas de proteção. Estão mais rotinados com aquilo que poderão ser os problemas a ser encontrados.
P1.V1.1 – P2INEM#04	Uma instituição que não tenha experiência em projetos de partilha de dados, de interoperabilidade dificilmente vai conseguir desenvolver políticas conjuntas de proteção de dados. Vai de encontro a outras questões que já falamos. Uma organização pela sua natureza, pela natureza daquilo que desenvolve, pode ainda não ter tido a oportunidade de observar um conjunto de preocupações e de problemas que outra organização poderá ter antecipado e estar na posse de um conjunto de soluções que pode partilhar com quem ainda está a iniciar este processo.
P1.V1.1 – P2INEM#09	Sim podemos afirmar que sim. Apesar de no nosso caso as regras são ditadas pela SPMS. O que não me coloca preocupações. Agora se o cenário fosse ao contrário, se fossemos nós a desenvolver o processo de partilha de dados, aqui sim ficava preocupado com a proteção dos dados, o que não quer dizer que não fosse necessário acertar estas questões com os destinatários dos dados.
P1.V1.1 – P2INEM#10	Sim a experiência aqui é fundamental. Em interoperabilidade em partilha de dados.
P1.V1.1 – P1HFF#01	Esta questão da privacidade dos dados a nível alargado depende também muito de uma estratégia conjunta para estas questões. Mas as coisas começam aqui. Não vai existir uma estratégia conjunta se o processo não nascer de cima. Quem tem que induzir e garantir esta estratégia, e manter este ciclo em funcionamento, dentro do ecossistema, são os responsáveis pela gestão. Voltamos ao princípio da responsabilidade – tem que haver iniciativa aos níveis de gestão, para depois se partir para uma estratégia. Se existir um protocolo que tem que mudar, ele tem que partir sempre de cima.
P1.V1.1 – P2HFF#02	Sim quanto mais experiência melhor – diminui o risco de haver problemas de privacidade. Quanto mais experiência se tiver em projetos de partilha de dados maior a probabilidade de sermos proactivos e não reacionários. Gradualmente é mais simples efetuar alterações, desenhar medidas. Temos alguns projetos com sucesso em interoperabilidade, em transcrições externas, resultados de laboratórios realizados externamente, o caso da PDS. Nestes projetos não houve uma preocupação em relação aos dados partilhados.
P1.V1.1 – P2HFF#03	No caso da saúde, ao contrário por exemplo da banca, em que dois bancos trabalham da mesma maneira em sistemas diferentes, e conseguem interagir, e conseguem garantir a privacidade dos dados. Existe depois um conjunto de reguladores que conseguem garantir a normalização. Na saúde isto não existe. A saúde neste ponto de vista está mais atrasada. Começou há menos tempo a fazer esse caminho. E portanto numa primeira fase eu não consigo ver como vamos aplicar modelos de privacidade à informação, se a informação não estiver ela própria bem categorizada. Mais uma vez é necessário um consenso sobre aquilo que é o processo clinico, que pode variar de hospital para hospital. O que é o processo clinico? Que informação é que contempla? E depois sim, posso qualificar todos os objetos com diferentes níveis de acesso, privacidade, de escrutínio, de auditoria. Sem isto, vai ser muito difícil. Se tivermos vários sistemas que interpretam da mesma maneira o processo clinico, então vai ser mais fácil a aplicação de políticas de proteção da privacidade. Ao nível dos hospitais o que nós fazemos ao nível da interoperabilidade é ainda muito imaturo. A experiência que há é mínima. Quando eu falo com académicos, com outros setores de atividade, assusto-me face ao ponto em que nós estamos. Deveria haver um maior investimento neste domínio. Mas seria necessário que todos os hospitais tivessem bem desenvolvido o seu processo clinico eletrónico. Não podemos ter os objetos em papel. Assim não há interoperabilidade possível. Tenho de garantir primeiro a base, que a informação está lá, e que está devidamente estruturada num repositório digital. Depois posso aplicar práticas de interoperabilidade. Os hospitais têm pouca experiência a este nível. A interoperabilidade também é um desafio recente. Só há poucos anos a que de facto os hospitais começaram a fazer que os sistemas falassem entre eles. Depois

	aplicar sobre esta base regras de segurança.
P1.V1.1 – P1SPMS#02	Têm vindo a crescer os projetos de interoperabilidade. A partilha de dados está cada vez mais massificada através da PDS. Mas temos outros cenários de interoperabilidade, iniciativas locais, que com a disponibilidade da SPMS, as instituições organizam-se implementam os seus cenários de ligação direta. Claro que depois surgem questões que escapam ao nosso controlo, e se não existir uma política de privacidade, podem surgir problemas. Estes projetos, estas iniciativas despertam nas pessoas uma atitude de preocupação em relação aos dados, em relação á troca de dados. Pode haver aqui uma dependência direta entre a experiência da partilha de dados e a proteção desses dados. Antes da PDS, tínhamos a ligação direta entre sistemas, para agendamento de consultas, por exemplo, para facilitar a vida ao utente. A partilha de dados clínicos entre hospitais e centros de saúde, está a evitar-se que isso aconteça diretamente. A informação que é partilhada tem por objetivo agilizar processos, e não propriamente passagem de informação clinica. Agora estamos a caminhar para um cenário único a nível nacional, em que a SPMS está a fornecer às instituições as ferramentas para elas trabalharem, em vez de termos várias soluções para um processo temos apenas uma solução. Um conjunto de integrações que existem a nível regional poderão ser descontinuadas porque nós já estamos a fornecer esta solução a um nível alargado. É esta a tendência, de caminharmos para um sistema único, com base na interoperabilidade, e esta tendência está a despertar nas pessoas uma maior atenção nas questões de proteção de dados. Assim como as pessoas estão mais desconfiadas pelo facto de haver um maior controlo sobre a informação. Preocupa-os que possam estar a ser vigiadas por uma entidade superior.
P1.V1.1 – P2SPMS#03	Era o desejável. Mas na minha o meio tecnológico da partilha de dados passou a existir, não que com isso também tenha aumentado a preocupação em relação á proteção de dados.
P1.V1.1 – P2SPMS#04	Gradualmente, temos cada vez mais situações de partilha de dados e de serviços, e como consequência, uma maior atenção e consciência em relação às questões da proteção de dados.
P1.V1.1 – P1HES#01	Existe uma relação e que transmite confiança. Claro que não é só isto, mas claro que transmite segurança.
P1.V1.1 – P2HES#02	É um fator que surge com a experiência, com o conhecimento. Ao nível local as aplicações informáticas que temos já fazem um pouco a partilha de dados, comunicam entre si. Temos que analisar quem trabalha com este tipo de aplicações e o conhecimento desses profissionais. Falo do conhecimento deste tipo de questões. Noto que existem muitos profissionais com grandes dificuldades ao nível a informática. São bons profissionais na área da saúde, mas não conseguiram evoluir para a era do digital. Temos profissionais com algumas limitações, o que limita a implementação de algumas medidas. Responsáveis dos sistemas de informação e técnicos ao nível local, a partir do momento em que começam a desenvolver soluções de partilha de dados com outras instituições, começam a olhar para estas questões [da privacidade dos dados] de uma outra maneira. Eu próprio sinto isto. Quando temos que enviar dados para o ministério da saúde, questionamos a forma como os dados são enviados, quais as garantias técnicas de segurança destes dados. Não chega confiar nas pessoas, é necessário saber como é que as coisas funcionam.
P1.V1.1 – P2HES#03	Sim é mais fácil para alguém que já tenha experiência em gestão da informação, que saiba com o que é que está a trabalhar, que tipo de informação se trata, a sua criticidade, desenhar medida de proteção. A experiência que nós temos de partilha de dados com outras instituições ainda é pouca. O aumento destas situações vai sem dúvida despertar questões sobre a proteção de dados. A nossa experiência em interoperabilidade de bases de dados ainda está numa fase inicial.

P1.V2.1

P1.V2.1 – P1ULSNA#01	Matéria de segurança decididamente sim, e privacidade e proteção de dados também. Estas três vertentes estão muito interligadas.
P1.V2.1 – P2ULSNA#02	Conhecimento dos sistemas TI, o ambiente dos profissionais, as tendências de trabalho dos profissionais, conhecimento das entidades externas com quem se colabora, conhecer os serviços, onde estão os dados críticos.
P1.V2.1 – P2ULSNA#03	No tratamento de dados. Preservar os dados primários, neste caso os utentes. Saber construir uma hierarquização de dados (classificação), níveis. É muito importante esta classificação para depois conhecer melhor o que se está a partilhar.
P1.V2.1 – P1USF#01	Experiência tecnológica é muito importante. Conhecimentos ao nível da segurança. Os conhecimentos ao nível da privacidade dependem das tecnologias utilizadas. Estou com alguma dificuldade em responder dado o meu perfil técnico, de ligação entre os responsáveis pelos sistemas e os utilizadores das aplicações.
P1.V2.1 – P2USF#02	Assumindo que quando se refere ao responsável pelos sistemas de informação se está a referir ao coordenador da instituição, é necessário que este saiba os requisitos legais e como devem ser aplicados, não é necessário um conhecimento como as aplicar tecnicamente. É necessário que na organização, nos diferentes peris técnicos, dentro do IT disponível, que seja capaz de fazer cumprir estas imposições, implementar estes requisitos.
P1.V2.1 – P1INEM#01	Dever-se-ia exigir. Temos uma grande lacuna de técnicos nesta área. A área de proteção de dados é uma área onde em termos estratégicos é necessário investir no futuro. É importante e exigível que no futuro os responsáveis pelos sistemas de informação ou outro tipo de técnicos venham a ganhar experiência em matéria de proteção de dados. Até porque, como é o nosso caso, estamos a avançar para a certificação da qualidade da organização em vários departamentos, o que nos obriga a ter conhecimentos básicos. A equipa de IT vai ser certificada na ISO 9000 a nível de processos. E queremos aproveitar esta experiência para avançarmos para a certificação da ISO 27000, em segurança da informação. A proteção de dados é assim um caminho a seguir.
P1.V2.1 – P2INEM#03	Não esquecer que a proteção de dados está ligada à segurança. Se eu não tiver segurança não consigo garantir a confidencialidade dos dados. São essenciais canais seguros. Tenho que ter garantias que quem utiliza os dados é a pessoa certa, os dados não foram adulterados. Dai ter vantagens que que tenha conhecimentos de segurança, principalmente durante o desenvolvimento de soluções (...). Por outro lado é necessário um conhecimento dos conceitos de privacidade, que ainda estão muito vagos. Se até determinada altura as pessoas não tinham uma cultura de segurança, passaram a ter uma cultura de segurança, e a implementar soluções de segurança, hoje em dia estamos no dados e temos que começar a ter uma cultura muito virada para os dados (...).
P1.V2.1 – P2INEM#04	Quanto aos responsáveis pelos sistemas de informação é essencial que estes deixem de olhar para cada sistema como uma caixa fechada, e troquem experiências com outros de outras organizações. São as pessoas ideais para desencadear estes processos [proteção de dados]. Tecnologicamente conhecem os sistemas como ninguém. Conhecem os processos e conseguem dinamizar colaboração com alguma facilidade, mas falta-lhes um conhecimento mais aprofundado em matérias de proteção de dados. Não querendo fazer um juízo do nosso universo!
P1.V2.1 – P2INEM#09	É necessário experiência em vários sectores. Mas preponderante é a gestão de sistemas e de informação [bases de dados], segurança de sistemas e infraestruturas. É necessário, cada vez mais apostar na proteção de dados, por variadíssimas razões, seja pelas coisas mais insignificantes, seja pelas que afetam mais as pessoas, os seus dados devem ser bem protegidos.
P1.V2.1 – P2INEM#10	Garantidamente tem que ter conhecimentos em segurança. Experiência em segurança. Ao nível da proteção de dados acaba por se aplicar a mesma regra. O que se estuda não é suficiente, é necessário experiência. É importante dialogar com outras pessoas, estabelecer pontes com outras organizações. Um individuo que consiga perceber aquilo que é o seu sistema, quais são as lacunas

	e benefícios existentes, para quando se está a dar autorização para a utilização dos nossos dados, estes possam ser utilizados de uma forma segura. Isto não é um problema de uma instituição mas do conjunto.
P1.V2.1 – P1HFF#01	Penso que a experiência que é necessária começa numa questão muito simples: é necessário que a organização queira, ou seja basta que ao nível da administração alguém queira. Não é ser obrigado a fazer. É necessário que as pessoas sejam sensibilizadas. Têm de perceber as vantagens e no limite têm que ser penalizadas se não cumprirem. O ideal é os responsáveis perceberem desta necessidade, e serem eles próprios os indutores da mudança internamente. Ou seja, este compreende, absorve, divulga por todas a instituição, e estabelece o compromisso. E esta preocupação funciona como uma bola de neve, acaba por envolver várias pessoas, como o gabinete de risco clinico e não-clinico, alguém da tecnologia, pode criar-se um gabinete para o *chief security information officcer*, ou alguém com esta responsabilidade. Ou seja, um grupo de trabalho dedicado. Depois disto temos um modelo que pode partir para os sistemas de informação. O *privacy information officer* é sem dúvida o caminho a seguir no futuro.
P1.V2.1 – P2HFF#02	É exigível que os responsáveis dos sistemas de informação de alguma forma comecem a ter competências na área de proteção e dados e não apenas naquilo que é segurança de infraestruturas e informação.
P1.V2.1 – P2HFF#03	Podemos falar de competências, conhecimentos e motivações. O posicionamento preferencial para estas questões é dentro do *IT Governace*. Profissionais que possam estar preparados, para que de alguma forma, vejam a globalidade do sistema e consigam desenhar medidas que sejam eficientes para a proteção de dados. Existem questões em saúde em que o nosso não domínio clinico pode fazer com que nos escape coisas importantes. Temos que trabalhar em colaboração com os profissionais de saúde na tomada de decisão. Há sempre uma decisão técnica, mas há um procedimento e há um contexto, e o contexto aqui é clinico. Portanto, onde é que faz sentido intervir? Sem o clinico nós não conseguimos ser assertivos. É claro que a visão da floresta (*IT Governance*) é fundamental, assim como um conhecimento da legislação, e uma preocupação em relação a estes assuntos. Tipicamente um informático, um tecnólogo, não está virado para estas questões. Está focado na resolução do problema. São poucos os que constroem soluções a pensar que estas vão ser interoperáveis. Que a informação vai "verter". E quando eu construo uma ligação entre dois sistemas, como acontece hoje, tem que haver alguma preocupação a este nível. Isto não acontece. Têm de ser outras pessoas a introduzir estas questões (proteção da privacidade dos dados). Pessoas que têm a visão do projeto do sistema de informação, e que sejam capazes de induzirem esse trabalho.
P1.V2.1 – P1SPMS#02	Para estes profissionais esta questão da privacidade tem que ser clara. Ter uma estratégia para a segurança e para a proteção de dados. Difundir esta informação pelas instituições. As pessoas dão sempre prioridade à segurança das infraestruturas, mas a tendência e com o avançar da era da informação, é que as pessoas comecem a dar o mesmo valor ou até cada vez mais a proteção da informação. Ainda não estamos preparados para tal. Estes responsáveis devem ser preparados e consciencializados para a questão da privacidade e mais focados na questão dos dados. Temos a segurança toda implementada, mas temos que começar a olha para a informação. Nós não temos a noção da criticidade da informação que está a ser disponibilizada. Na PDS nós estamos a definir informação clinica relevante para ser partilhada. Há muita outra informação nos processos clínicos, que não está a ser partilhada. Nós estamos a tentar resumir numa "vista" informação clinica útil e que deve ser partilhada. Quanto ao pormenor dos dados, só mesmo nos processos locais. Nós não queremos substituir os processos clínicos. Não queremos centralizar tudo num único processo clinico eletrónico.
P1.V2.1 – P2SPMS#03	Pelo menos um conhecimento sobre a legislação. A maior parte dos responsáveis não se preocupa com esta questão. Conhecer as normas na área da segurança, elas já existem há alguns anos. Perceber quais os princípios que devem estar na base de proteção de dados. Ajudaria se existissem princípios generalizados. Isto extravasa um pouco o ministério da saúde e está relacionado com

	a função pública em geral. Em alguns países isto é feito de uma forma central, em que todos são tutelados por um conjunto de princípios. Na administração pública todas as instituições têm que ser tuteladas pelos mesmos princípios. A saúde terá depois a sua parte setorial mais específica. Ter conhecimento e competências neste nível de informação seria muito útil. Os sistemas de informação quando são construídos tentam abarcar toda a informação possível, e eventualmente é abordada muito mais informação do que aquela que vai ser necessária. A partilhada informação tem contribuído para que isto tenha vindo a decrescer, o que é positivo. Mas ainda assim, este facto acontece bastante. É necessário olhar para os sistemas mais numa visão estratégica e não apenas tecnológica.
P1.V2.1 – P2SPMS#04	Conhecer tudo em termos de legislação, normas e segurança de dados. Também ter conhecimento de boas práticas, verificar o que já existe noutros sistemas, ver o que já foi feito, e transpor para o seu sistema.
P1.V2.1 – P1HES#01	Atualmente o grande desafio é conseguirmos fazer aquilo que nos compete com as equipas pequenas que temos. Este tipo de coisas muitas vezes é relegado para 2º plano, porque passamos os nossos dias a "apagar fogos". Justifica-se ter nas organizações profissionais totalmente dedicados a estas matérias. Cada vez mais deveríamos apostar em profissionais especializados, principalmente se tivermos em conta a criticidade que a informação representa neste momento, a forma como esta informação está a ser gerada, distribuída, pelo país fora, não tenho dúvidas nenhumas. Atualmente com os recursos existentes, não conseguimos, é impossível.
P1.V2.1 – P2HES#02	Eu acho que grande parte dos responsáveis ainda não tem conhecimentos ao nível da proteção de dados. E é urgente este conhecimento. Alguém dentro da equipa [de sistemas de informação] deve dar este suporte. A experiencia em segurança pode ter aqui algumas vantagens, podendo ser numa primeira fase ser suficiente, mas depois tem que ser mais desenvolvida. A área da privacidade é um mundo à parte da segurança. Tem que ser uma pessoa com um grande domínio tecnológico, um grande domínio organizacional e também jurídico. As pessoas sem segurança têm uma grande falta de conhecimentos de legislação. [...]
P1.V2.1 – P2HES#03	Um líder tem que saber um pouco de tudo. Não propriamente ser especializado em tudo. Só desta forma consegue perceber qual o trabalho que está a ser feito. Em termos de dados é essencial que conheça quais é que são os dados mais críticos, como é que são partilhados. [...] O conhecimento existente em termos de proteção de dados é pouco, pelo que é necessário que desenvolva conhecimentos neste domínio. Ainda é uma lacuna muito grande, apesar de se falar muito em proteção de dados. É necessário conhecer o que é que implica [a proteção de dados], evoluir na proteção de dados. Basta ter uma experiência que correu bem, e as pessoas aprendem muito com esta experiência. Ficamos a saber quais os requisitos mínimos que temos que contemplar. A próxima experiência já corre melhor. Também é importante aprender com os erros dos outros, o que implica a colaboração. Haver encontros entre as instituições ficados nestas questões é importante. [...] Não apenas para a segurança.

P1.V2.2

P1.V2.2 – P1ULSNA#01	Irá contribuir positivamente para a melhoria da implementação de medidas adequadas à legislação, sem dúvida.
P1.V2.2 – P1USF#01	Pode ter um efeito prático bastante importante. Ao nível dos responsáveis pelos sistemas seria importante este conhecimento, dado que na maioria das vezes a sua maior preocupação é desenvolver as aplicações e colocá-las disponíveis. Apesar de todo este

	desenvolvimento ter por base a legislação existente, a proteção de dados sairia beneficiada.
P1.V2.2 – P2USF#02	Sem dúvida alguma. Veja o seguinte exemplo. Saiu recentemente legislação sobre o funcionamento dos cookies nos sites. Se ninguém na organização souber desta lei, ficamos sujeitos a multas pesadas. Estas questões são muito importantes, dado que as multas podem ser elevadas. Legalmente tem que haver alguém em permanência com conhecimento em legislação, e pedir a alguém a sua aplicação. O não conhecimento da lei não é resposta para coisa nenhuma. Temos que conhecer, saber o que existe e aplicar. Alguma legislação é de fácil aplicação.
P1.V2.2 – P1INEM#01	Seriam mais sensíveis, em momentos como os de criar utilizadores, atribuir permissões. Acima de tudo restringiam mais o acesso aos dados. Este conhecimento passa muito pela sensibilidade de cada um para estas questões.
P1.V2.2 – P2INEM#03	Sim teria um efeito benéfico. Se eu souber um pouco mais sobre aquilo que eu preciso de ter em atenção, sobre o que preciso de desenvolver, de certeza que vai influenciar tudo aquilo que eu vou fazer. Se estamos a tratar de dados confidenciais, é necessário trata-los o mais seguro possível e de acordo com aquilo que é exigível.
P1.V2.2 – P2INEM#04	Deveria haver um maior conhecimento destas matérias. As pessoas que fazem a ponte com outros sectores, nomeadamente as administrações, deveriam ter um maior conhecimento nestas matérias. Ao nível dos programadores estas questões são importantes, mas têm que ser planeadas antes – estes problemas têm que ser levantados antes. De facto as questões legais passam-nos [como programadores] um bocadinho ao lado. Existe uma maior preocupação em relação às questões técnicas. Apesar de ser importante o desenvolvimento de uma maior sensibilidade para estas questões.
P1.V2.2 – P2INEM#09	Numa fase inicial é uma ajuda importante. Não podemos consultar a legislação apenas quando temos dúvidas. É o caso das dúvidas na utilização da conta de correio eletrónico de serviço. Ao não existirem regras específicas sobre as boas práticas para a sua utilização surgem muitas dúvidas sobre a confidencialidade da informação, o que é considerado dado pessoal ou de serviço? Quem é o proprietário? É uma discussão que ainda não teve uma resposta conclusiva. Isto demonstra alguma dificuldade em lidar com as questões de proteção de dados. Um maior conhecimento da legislação poderia ajudar.
P1.V2.2 – P2INEM#10	Sim, pelo menos as pessoas pensavam melhor antes de disponibilizar um conjunto de dados. Despertava a consciência e a preparação, para questionarem o porquê da utilização dos dados. Deveria haver uma maior preocupação em disponibilizar a legislação sobre proteção de dados.
P1.V2.2 – P1HFF#01	Devia haver uma preocupação maior em relação áquilo que são regulamentos e legislação de proteção de dados. Cada país adota as suas normas e existe uma grande desregulação a nível europeu. Um maior conhecimento nesta área é sem dúvida fundamental. É necessário um maior reforço neste conhecimento.
P1.V2.2 – P2HFF#02	Despertava logo alguns profissionais. Como não existe esta preocupação constante acabamos por não dar atenção a esta questão. É o caso da norma ISO27001, em que basta folhear o documento para encontrar itens a implementar.
P1.V2.2 – P2HFF#03	Sem dúvida que é importante um conhecimento a este nível. Existe um conhecimento generalizado sobre o problema, mas depois não existe um conhecimento especializado, detalhado. O relatório de 2004 da CNPD detetou grandes problemas. Eu pergunto, o que é que terá mudado entre 2004 e 2014? A tecnologia evoluiu imenso nestes anos, mas os processos nas organizações levam mais tempo. A questão complicou-se pois grande parte da informação está acessível do exterior dos sistemas de informação. e dantes não estava. E portanto o problema só se complicou. Aumentou exponencialmente. Hoje duplicamos e reutilizamos a

	informação a uma velocidade maior. Dois aspetos: (1) a informação sai para o exterior dos sistemas e perdemos o controlo e o rasto; (2) nós agora podemos ir a um repositório tirar informação que antes não existia. Nós conseguimos dar muito mais informação porque estamos cada vez mais a concentrá-la e estrutura-la. Eu tenho muita dificuldade em saber o que devo exigir em termos de propriedade, segurança, responsabilidade. Saber aplicar a legislação é complicado.
P1.V2.2 – P1SPMS#02	Seria muito útil, sem dúvida. Não é uma preocupação constante das pessoas em perceber as alterações a este nível. É como uma cultura, que faça com que as pessoas sempre que pegam nesta temática leiam a legislação, uma vez que temos que estar informados sobre a legislação que sai sobre proteção de dados. Esta prática deveria ser fomentada nas organizações. É um hábito que pouca gente tem.
P1.V2.2 – P2SPMS#03	Só o simples conhecimento da legislação, dos regulamentos, teria um impacto positivo. Anteriormente o exame de admissão a um cargo da função pública, obrigava a um conhecimento detalhado da legislação de proteção de dados. Tínhamos que fazer prova em como a conhecíamos. Hoje todas as pessoas contratadas desconhecem esta legislação. Tivemos recentemente um workshop e quando se questionou as pessoas sobre o conhecimento integral da legislação, se já tinha lido pelo menos uma vez a lei de proteção e dados, verificou-se que são poucos os casos que responderam que sim. As pessoas têm de perceber a lei, pois só assim é que conseguem avaliar depois. Podem agir com conhecimento.
P1.V2.2 – P2SPMS#04	O feito prático seria muito positivo. As pessoas não têm este hábito.
P1.V2.2 – P1HES#01	Seria um catalisador de algumas medidas imediatas.
P1.V2.2 – P2HES#02	Uma maior consciencialização das pessoas, sem dúvida nenhuma. Neste momento as pessoas não sabem das consequências de uma má utilização dos dados. As pessoas não sabem das penalizações em que incorrem. E nesta situação facilitam. Daí que um conhecimento maior em legislação, diminuía o facilitismo. *É o caso do conceito de identidade digital, em que as pessoas pensam apenas que serve para abrir uma sessão num computador. […]*
P1.V2.2 – P2HES#03	Existe muito pouco conhecimento sobre a legislação de proteção de dados, em todos os profissionais. Só com um conhecimento sobre o que implica a legislação de proteção de dados desencadearia um conjunto de medidas. O nosso grande escudo de proteção acaba por ser o "medo". Mas não há como inverter o caminho da evolução dos sistemas. E o caminho é partilhar. Se houvesse mais informação em todos os intervenientes, em termos de legislação, dados, técnicos, acho que era mais fácil evoluir.

P1.V3.1

P1.V3.1 – P1ULSNA#01	Sem dúvida especialistas em segurança, área de redes. Especialistas em proteção de dados, acabam por abranger todas as áreas transversais que levam à proteção de dados. Poderemos caminhar neste sentido, mas neste momento ainda não o estamos a fazer. Os responsáveis pelos sistemas de informação, dada a sua sensibilidade e perceção podem realizar esta tarefa numa faze inicial,

	apesar de não dominarem a questão. É fundamental o envolvimento da parte jurídica, dado o conhecimento sobre consequências legais, o que certamente vai despertar a atenção para este tipo de questões. Apesar de localmente ainda não se justificar a presença contínua de profissionais especializados em proteção de dados, para o contexto da colaboração justifica-se a existência de uma equipa a trabalhar estas questões.
P1.V3.1 – P2ULSNA#02	Uma equipa tripartida, administração, área clinica, e TI. Apesar da dificuldade de conseguir profissionais com conhecimentos em proteção dos dados, seria uma mais-valia ter alguém focado nos dados. Não sei até que pondo é necessário ao nível da ULSNA alguém que se dedique inteiramente a esta área. Para o todo da colaboração, no ministério da saúde, deveria haver uma equipa que colaborasse com as equipas de TI dos hospitais mais para as questões de proteção dos dados.
P1.V3.1 – P2ULSNA#03	É sempre bom existir recursos humanos com o máximo de conhecimentos. De facto é necessário, um técnico na ULSNA com conhecimentos em proteção de dados, nem que sejam conhecimentos básicos. Sem dúvida que a administração, sistemas de informação e a parte jurídica devem estar relacionados com estas questões. Uma estrutura dedicada a estas questões, não sei se será de todo justificável dentro destas instituições.
P1.V3.1 – P4ULSNA#06	Os profissionais ligados aos sistemas de informação, médicos e também enfermeiros, e incluía também juristas. Penso que são as pessoas fundamentais neste domínio. Apesar de concordar com a introdução de um profissional como "delegado de dados", o meu receio é que as instituições tenham que o fazer por imposição e não por iniciativa própria. Este trabalho em parte já é feito pelo gabinete jurídico, apesar da sua limitação nestas questões. Profissionais com conhecimentos em gestão, sistemas de informação e legislação, poderiam ser o perfil ideal para tratar estas questões. Sim justifica-se. A SPMS poderia ter um papel muito importante. Ao nível das organizações, havendo interesse e consciência de que isto é uma mais-valia para a organização, e através de um gabinete não autónomo, inserido num outro serviço, por exemplo os sistemas de auditoria ou gabinete do utente, fica facilitada esta partilha de experiência com outros serviços e com a SPMS.
P1.V3.1 – P1USF#01	Sim deveriam existir recursos humanos dedicados á privacidade. Ao nível da ARS por exemplo deveria existir um profissional para estas questões. Enquanto ao nível de uma USF pode não se justificar um profissional dedicado em exclusividade a estas questões, ao nível de um hospital já se justifica.
P1.V3.1 – P2USF#02	Não acho que seja rigorosamente necessário recursos humanos exclusivamente dedicados a estas questões. Acho que uma equipa multidisciplinar que tenha uma visão transversal, que tenha elementos de redes, elementos de sistemas, juristas, consegue fazer isto. Ao nível do ministério, aqui sim justifica-se profissionais em privacidade, dedicado a criar normas transversais para todo o ministério da saúde. Será de certeza útil para as organizações. Agora ao nível mais local, ARS e hospitais, tem que existir alguém que tenha uma maior preparação, que tenha uma facilidade nestas questões. Uma equipa pluridisciplinar faz sentido.
P1.V3.1 – P3USF#03	Concordo com a necessidade de existirem profissionais dedicados a estas matérias, a tempo inteiro, nomeadamente ao nível da ARS.
P1.V3.1 – P3USF#04	Se me tivesse feito esta pergunta há um mês atrás, a minha resposta seria que não se justificam recursos humanos dedicados às questões da privacidade, e isto porque já temos tantas preocupações mais prioritárias. Depois de termos estado a conversar sobre estas questões, a minha opinião já fica inclinada para o outro lado, é importante apostar-se nestes profissionais. No nosso dia-a-dia ainda não estamos muito conscientes para estes problemas, para o seu impacto. A pessoa ou está sensibilizada, sabe um pouco sobre isto, ou é algo que a pessoa esquece. O princípio ético, que nos diz muito respeito, tem que ser transportado para as ferramentas informáticas. (…)
P1.V3.1 – P3USF#06	Tenho colaborado nesta área. E acho que é muito importante quem está no terreno. Já tenho dito isto a algumas pessoas – eu só

	sou uma mais-valia enquanto eu estiver no terreno. O meu contributo é enquanto utilizadora. Agora haver no ACES uma pessoa exclusivamente dedicada a estas questões, a colocar medidas no terreno, a auditar, seria uma mais-valia. Nesta área não temos nada em auditoria. Esta necessidade vai começar a sentir-se mais, com o surgir de novas tecnologias e ferramentas, será muito natural que surjam estes profissionais.
P1.V3.1 – P4USF#05	Sim, acho que sim, é importante existirem recursos humanos dedicados a esta matéria. Não se justifica uma pessoa na USF totalmente dedicada, mas dentro das ARS sim. Quem desenvolve estes sistemas devem ter recursos que estejam dentro da área da privacidade. Até para fazer auditorias aos sistemas e verificar se está a haver fugas de dados.
P1.V3.1 – P1INEM#01	No caso do INEM não existe uma indicação formal sobre o responsável pelos processos de tratamento de dados. Talvez não seja necessário uma pessoa a tempo inteiro dedicada a estas questões. Pelo menos justifica-se a existência de um grupo de trabalho que de vez em quando faça e defina estes assuntos. Ao nível do ministério da saúde já se justifica a existência de uma equipa permanente. O que poderia criar condições para certificar, auditar, ajudar as instituições, desenvolver diretrizes. Ganhava-se uma economia de escala. Compensava ter uma equipa permanente para o desenvolvimento conjunto. Poderia salvaguardar as questões da privacidade na PDS. Justifica-se uma estrutura de suporte ao contexto alargado de partilha de dados.
P1.V3.1 – P2INEM#03	É uma questão complicada. Não sei dedicadas simplesmente a estas questões, ou se não seria uma mais-valia se tivesses mais que esta responsabilidade. É algo que ainda necessita de ser mais explorado, sem sombra de dúvidas, é algo que tem que ser mais definido, mais do que está neste momento. É necessário resolver a indefinição que existe neste momento. Mas faz sentido juntar algo mais, do que ter uma pessoas dedicada só a isto. Juntar todos os outros aspetos que levam à privacidade, como a segurança. Tem que ser um individuo multidisciplinar, por um lado um tecnólogo e por outro tem que ser também um individuo com competências em gestão, fazer auditorias regulares, as análises de conformidade que falamos. Mas para o universo que é a rede da saúde, uma estrutura enorme, em que seria incomportável, ter alguém a fazer várias coisas. Aqui sim, faz sentido ter uma equipa de apoio, de topo, que desenvolva projetos comuns.
P1.V3.1 – P2INEM#04	Penso que sempre se justificou a existência de profissionais especializados, não só em proteção de dados, como na segurança dos dados. Para á área da saúde justifica-se uma equipa permanente a desenvolver estas questões.
P1.V3.1 – P2INEM#09	Sim considero necessário haver recursos humanos dedicados a estas questões. Faz todo o sentido aqui no INEM haver um profissional especialista, que não vai estar ligado a outras funções (nem de desenvolvimento, nem de administração de sistemas), e que seja uma pessoa que consiga falar com todos, que reúna informação e analise os problemas existentes. Seria uma ponte para estas questões. Em simultâneo deve haver um staff mais alargado que cobrisse todo o ministério da saúde.
P1.V3.1 – P2INEM#10	Acho que se justifica haver recursos humanos dedicados à questão da proteção de dados. É algo que é importante, que é sério, logo justifica ter recursos humanos dedicados. Para o âmbito mais alargado, e se pensarmos naquilo que temos vindo a falar, no sentido de fazer as reavaliações, é necessário uma equipa permanente [...].
P1.V3.1 – P3INEM#05	Eu penso que sim, justifica-se numa organização como a nossa a presença de profissionais especializados em proteção de dados, com esta função. Todas estas questões poderiam ser analisadas de maneira diferente, para que não aconteça nada com grande impacto. É necessário um maior desenvolvimento de direitos e deveres dos profissionais em relação aos dados, à semelhança do que acontece com a assistência médica. Seria um passo muito importante. Imagine um profissional que é convocado para ir a tribunal, e pergunta-se? O profissional pode ter acesso ao verbete clinico, pode apresentar esta informação?
P1.V3.1 – P3INEM#06	Acho que se justifica profissionais dedicados a estas questões, e cada vez mais vão ser importantes, pois cada vez mais vai haver

	maior partilha, e com os sistemas de informação a evoluíram a uma velocidade muito grande, há cada vez mais dados a serem recolhidos em nos apercebermos, e a serem partilhados, convertidos, e é importante haver profissionais com conhecimento nesta área e que a consiga normalizar.
P1.V3.1 – P3INEM#07	Se queremos fazer uma análise de impacto ambiental de uma ponte, necessitamos de especialistas. O mesmo se passa com as ferramentas informáticas, é necessário especialistas em análise de impacto sobre a privacidade. Faz todo o sentido a presença nas organizações de profissionais especializados em privacidade, que acompanhassem o dia-a-dia das instituições, fazendo auditorias, melhorias continuas.
P1.V3.1 – P4INEM#08	Eu acho que, mais do que profissionais especializados, deveria de haver um verdadeiro sistema para controlo sobre estas matérias. Acho que estes profissionais não têm obrigatoriamente de estar dentro das organizações. Faz sentido no âmbito da saúde, que exista alguém, sem ser a CNPD, um gabinete de controlo para a proteção de dados. Agora a organização tem que ter acesso a um conhecimento técnico, que obriga a uma especialização, a fazer uma diferenciação. Se existir no ministério da saúde um organismo que tem como função, auditar os sistemas de informação, analisar o risco, e implementar ferramentas que garantam a proteção de dados, será ótimo.
P1.V3.1 – P1HFF#01	É importante a participação de um gabinete de gestão de risco, e se pensarmos ao nível do *IT Governance*, um *chief security information officer*. Para isto acontecer, é necessário o aval do conselho de administração. A partir daqui a gestão da informação é a parte mais importante. Contudo, tudo isto depende da grande maturidade do responsável por um gabinete a este nível que consiga dialogar com todos os outros departamentos. Depois faz todo o sentido que exista uma instituição que consiga ligar todas as organizações em relação a estas questões. O foco não pode ser a tecnologia. É necessário ir além da segurança. Poderia ser montada uma governação da informação, já não falo no IT, com peritos em várias áreas. Isto é muito mais conceptual ao nível da gestão da informação, do que questões técnicas.
P1.V3.1 – P2HFF#02	Localmente é necessário haver um auditor em privacidade e segurança, que não existe - um profissional com competências em privacidade, especializado nestas matérias. Justificava-se ao nível da SPMS haver profissionais dedicados a tempo inteiro a estas questões. Haver um recurso que vai circulando pelos hospitais. Que pode realizar auditorias, em vez de serem realizadas por empresas externas. Desenhar soluções de uma forma centralizada, de modo a poupar recursos, harmonizar soluções, uniformizar os processos de privacidade e segurança. O caminho é centralizar e caminhar para a certificação. Esta estrutura poderia revolucionar as organizações.
P1.V3.1 – P2HFF#03	Os exemplos bons que eu conheço, de desenvolvimentos de coisas deste género, passam por haver equipas a nível nacional, dedicados exclusivamente durante um prazo. Durante este prazo fazer *reporting* semanal ou mensal para todas as instituições do ponto ou nível em que cada uma está, com transparência para os pares, ou seja, eu sei o ponto em que estou e vejo onde é que estão os outros. Isto é indutor de um movimento completamente diferente, porque existe uma transparência e obriga a um *benchmarking* constante. Depois em cada instituição existe um elo de ligação com esta responsabilidade. Vamos chegar um dia a um *privacy information officer*. Já temos um monitorizador clinico, ou seja, um responsável pela monitorização da utilização da informação clinica, que já dá parecer regularmente sobre a qualidade, economia e eficiência em termos clínicos. Ainda não temos é depois toda a parte do acesso à informação – ainda não chegamos aí. Mas para chegar claramente vai ter que haver um responsável pela privacidade da informação, assim como temos um responsável pelo risco clinico, um responsável pela segurança. De facto a segurança da informação clinica está muito aquém da segurança da informação económica. Isto quando comparo as preocupações que o meu banco tem no aceso à minha conta, à informação da minha conta, com as preocupações que nós temos no acesso a informação clinica.
P1.V3.1 – P3HFF#04	Dentro das organizações deveria existir uma comissão estruturada. Nós temos a comissão de ética, informatização, auditoria,

	qualidade e segurança do doente, onde está implícito os dados. Deveria haver recursos humanos a tempo inteiro afetos a estas questões e a promover o seu desenvolvimento dentro das organizações. Facilita também aquilo que é a colaboração com outras organizações. Acima de tudo têm de ser profissionais multidisciplinares, agregadores, com várias perspetivas do problema.
P1.V3.1 – P4HFF#05	Nos dias de hoje existir uma comissão multidisciplinar. É importante que dentro das organizações comecem a surgir pessoas com uma maior especialidade nestas matérias. Para o domínio da saúde, a globalidade destas questões, depende da existência de uma entidade que tenha esta preocupação, caso contrário acabamos por ter apenas situações pontuais de desenvolvimento. A certificação é o melhor caminho. Vai ser necessário haver algumas diretrizes neste sentido. Dar algum tempo às organizações para interiorizarem os conceitos e partirem para a prática.
P1.V3.1 – P1SPMS#02	Justifica-se nas organizações pessoas dedicadas às questões da privacidade. De certa forma todas as equipas têm que ter alguém com conhecimentos neste domínio. A própria cultura deve influenciar que todos os processos tenham lá a componente da privacidade bem assente. No entanto, a meu ver, as organizações têm de ter alguém responsável para perceber se os processos estão a ser implementados corretamente. Verificar se está a ser dada a devida atenção a essa componente. E aí precisamos de recursos afetados a 100%. É no fundo aquilo que já falamos, a análise de conformidade e evoluir. Temos que ter alguém preocupado com a evolução, com as novas orientações, estar sempre a par do que está as ser publicado, e implementar na organização. Em termos futuros são profissionais que vão desempenhar um papel importantíssimo nas organizações. A nível nacional poderia ser criado um grupo para coordenar este desenvolvimento. Tal como temos grupos de trabalho focados na telemedicina, também podemos ter um grupo de trabalho focado na privacidade dos dados a nível nacional. A SPMS poderia incentivar essa reunião de pessoas e "alimentar" este grupo, com depois todas as pessoas a realizar o seu trabalho nas organizações. Antes de mais as pessoas têm de ser informadas e alertadas sobre todas estas questões da privacidade. Têm que ter noção desta necessidade e desta responsabilidade. E aí as instituições poder ter condições para destacar alguém para se preocupar com estas questões. Isto vai surgir. É necessário como que uma "revolução silenciosa". Por exemplo, ao nível de uma DGS esta questão é crítica, dada a quantidade de sistemas que a DGS produz.
P1.V3.1 – P2SPMS#03	Eu acho que todos os projetos deveriam ter uma análise externa de perceber realmente qual o impacto que têm do ponto de vista da privacidade. E ser considerada a privacidade logo no desenho das soluções. Não pode ser depois, em que os sistemas já estão montados e que vão começar a partilhar dados que nós nos vamos preocupar com a privacidade. Nós temos de nos preocupar antes. Este facto justifica que comece a haver dentro das instituições perfis profissionais em privacidade. É necessário pessoas a olhar para os dados e que percebem como implementar estas questões. Poderia dar-se um salto qualitativo nesta matéria. No fundo faz falta nas organizações, uma pessoa com responsabilidade sobre a gestão da privacidade e que faça a ponte com a CNPD. Não pode ser o responsável dos sistemas de informação a assumir mais uma competência. É necessário desenvolver nas organizações uma nova linha de pensamento, assim como é necessário entregar um modelo de arquitetura, um modelo de negócios. Num projeto de um novo sistema ser entregue também uma análise de risco, que não é feito, em relação à informação, e uma análise do impacto sobre a privacidade. Quem acaba por fazer a análise de impacto sobre a privacidade é a CNPD, que muitas vezes chumba projetos. Para o domínio alargado da partilha de dados, para o SNS, faria todo o sentido haver uma equipa que coordena-se esta questão. A tentativa que tem sido materializada através da comissão de informação clinica (CAIC), criada a nível da secretaria de estado, que entretanto foi transposta para a SPMS, que passou a ser comissão e acompanhamento de informação clinica. Um dos grupos é o da segurança. Se este grupo continua-se ao nível da secretaria de estado poderia ser um grupo efetivo e poderia ter um papel importante ao nível da privacidade dos dados. Ao nível da SPMS significa que já não temos hierarquia como as entidades.

	O objetivo deste grupo é definir um denominador comum. Ou seja, no mínimo o que é que todos temos que ter. E depois dar um apoio às entidades para conseguirem chegar a este mínimo. Quem conseguir ir mais longe, tanto melhor. Mas um mínimo a nível nacional, já seria muito positivo. É necessário, começar por criar pontos de contacto dentro das organizações, figuras formais que pudessem transpor estas iniciativas e que as promovessem dentro das organizações.
P1.V3.1 – P2SPMS#04	Começa a justificar-se que existam nas instituições pessoas dedicadas a estas questões. Isto e pessoas especializadas em legislação. Muitas vezes sai legislação e temos muita dificuldade em a interpretar. É uma terminologia mais jurídica. Para o âmbito nacional, faz sentido, haver uma equipa responsável, que fomente este desenvolvimento, caso contrário vamos ter apenas situações pontuais de desenvolvimento.
P1.V3.1 – P1HES#01	Haver dentro das instituições profissionais especializados em proteção de dados. Que possa por exemplo abranger aquilo que é a análise de risco. Seria um elemento extremamente importante para conseguirmos implementar localmente estas questões. Para o domínio mais alargado de partilha de dados, a SPMS como regulador, tem que olhar para esta questão. Justifica-se haver uma estrutura organizativa que suporte, que de alguma forma olhe para estas questões como um todo, e que promova uma maior colaboração entre especialistas, com base num conjunto de objetivos para a privacidade dos dados.
P1.V3.1 – P2HES#02	É fundamental haver profissionais especializados em proteção e privacidade dos dados nas instituições. Deverá haver pessoas especializadas em quase todas as áreas, porque nestas questões da informática cada vez mais é necessário um conhecimento especializado e não generalizado. É uma área que exige muito trabalho, muita dedicação. Se nos dedicarmos a muitas áreas em simultâneo, poderemos não ser capazes de aprofundar o conhecimento. Para a questão da privacidade dos dados, não tem que ser necessariamente um tecnólogo. Tem que ser uma equipa multidisciplinar, composta por pessoas da segurança informática, em conjunto com outros profissionais. Justifica-se que exista uma equipa multidisciplinar a nível nacional, que pudesse reunir e trocar informação, composta por elementos das principais instituições do ministério. À semelhança de algumas iniciativas semelhantes na área clinica. Não tem que necessariamente ser uma equipa centralizada em Lisboa. Tem que ser criada com base na colaboração entre as principais instituições, na partilha de experiências, de recursos, na otimização de processos.
P1.V3.1 – P2HES#03	É importante haver um profissional, ou mais do que um, para a proteção de dados. Não lhe consigo dizer se é necessário uma dedicação total a esta questão. Alguém que depois consiga fazer a ponte com a área tecnológica. O ideal era haver uma equipa de suporte ao nível a SPMS. Uma equipa que consiga estar algum tempo nas instituições e dar alguma preparação às pessoas localmente. Poderia nascer na RIS.
P1.V3.1 – P3HES#05	É necessário profissionais especializados em privacidade. Mas antes de isso precisamos do dia-a-dia. De equipas maiores de apoio. Ainda temos grandes dificuldades no apoio tecnológico. Mas temos que pensar seriamente nesta questão dos dados. Mas não podemos pedir às pessoas este patamar de exigência, sem os patamares inferiores. Ter uma solução tecnológica, ou plataforma, que abrange grande parte dos serviços, facilita imenso.
P1.V3.1 – P4HES#06	Há três anos atrás já se justificava a presença de profissionais especializados em proteção de dados nas instituições. Isto antes de implementar sistemas de partilha de dados. O problema que está criado, não foi criado pelas instituições. As instituições, de um modo geral, ao implementarem os seus sistemas tiveram esses cuidados [com a proteção de dados].

P1.V4.1

P1.V4.1 – P1ULSNA#01	Sessões de sensibilização, casos de estudo, projetos de investigação que permitam refletir sobre a privacidade. Apesar da importância dos meios formais, dado o seu rigor e a presença de profissionais especializados, os meios informais que permitam a partilha de conhecimento e experiências podem contribuir muito positivamente.
P1.V4.1 – P2ULSNA#02	Eventos internos não públicos, mostrar a determinados grupos as facilidades e riscos de acesso a determinadas informações sobre os utentes. Criar grupos de trabalho de forma a mostrar como devemos utilizar a informação que guardamos. A ideia que a RIS é uma rede segura, pode ser um erro.
P1.V4.1 – P2ULSNA#03	Colóquios ou congressos que permitam a troca de experiências, ajudaria os vários profissionais das instituições para esta questão. Devem acontecer de uma forma contínua, pelo menos, numa fase iniciar. É necessário sensibilizar as instituições. Formação contínua para todos os profissionais, dada a necessidade de evolução nestas questões.
P1.V4.1 – P4ULSNA#06	Todo o tipo de eventos não só de natureza formativa, porque existe ainda existe uma cultura a implementar. Utilizando uma linguagem mais médica, há génese a incutir nas pessoas e de adesão livre as organizações devem traçar objetivos para a participação obrigatória das pessoas. Até para fazer o trabalho dos profissionais que se desmobilizam, tem toda a pertinência qualquer tipo de evento, sejam seminários formativos de natureza obrigatória ou não, promover reuniões conjuntas entre organizações, aferir o nível de desenvolvimento de uma organização e fazer a aprendizagem com outras organizações. Se o exemplo não poder vir de dentro então que possa vir de fora.
P1.V4.1 – P1USF#01	Essencialmente através de ações de formação que permitam debater este tipo de segurança. Apesar da dificuldade de abranger um grupo numeroso de interessados.
P1.V4.1 – P2USF#02	Com uma equipa com conhecimentos especializados ao nível da proteção de dados podem ser promovidos alguns Workshops uteis. Algo que vá além das deliberações da CNPD.
P1.V4.1 – P3USF#03	A este nível não temos tido eventos dedicados à privacidade. Seria importante em futuros congressos incluir esta questão. De uma forma informal, mais pratica, através de manuais das aplicações, através da internet. Do lado do utente ainda há um longo caminho a percorrer em relação á sua preocupação sobre os seus dados. Ainda não estão sensibilizados para esta questão e confiam “cegamente” nos nossos serviços. Nunca questionam a utilização dos seus dados (…). Cada vez mais os utentes estão atentos aos seus direitos sobre os dados.
P1.V4.1 – P3USF#04	Formações acima de tudo. Acima de tudo as pessoas têm que estar informadas. Desde que a informação chegue canais informais também podem ajudar, como a internet, email, distribuição de cartazes, portal do utente e do profissional. Não quero diminuir o impacto destes meios, mas se a pessoas à partida não estiver sensibilizada, o que vai acontecer é que esta vai receber um email e vai coloca-lo no lixo. Portanto, não nego que não seja melhor fazer isso do que fazer nada. Esta questão tem que ser vista como um todo. Tenho algumas dúvidas sobre a valorização que cada um vai dar aos meios utilizados. A reação mais corrente dos médicos, é “depois vejo”. Voltamos à ideia inicial, com uma maior cultura em privacidade, o resultado vai surgir.
P1.V4.1 – P3USF#06	Os eventos dos embaixadores da PDS são um exemplo importante. Junto dos utentes é importante desenvolver estes conceitos – fazer-lhes chegar essa informação a casa.
P1.V4.1 – P4USF#05	Reuniões e formação que permita discutir com as pessoas e técnicos como é que se pode melhorar, identificar as dificuldades, de modo a haver uma interação entre todos. As próprias estruturas organizativas têm que ser mais ágeis nesta matéria e é necessário que tenham consciência dos problemas existentes. O ACES é o mecanismo excelente para desenvolver estas coisas ao nível local.
P1.V4.1 – P1INEM#01	Deve abranger várias áreas, que não apenas as equipas de IT. Desenvolver eventos focados no perfil profissional. Não impor soluções, é necessário envolver as pessoas, sensibilizá-las para a proteção de dados.

P1.V4.1 – P2INEM#03	É necessário sensibilizar as pessoas para estas questões. Se existirem regras e *standards* definidos, promover ações de formação sobre estes standards. Não havendo, mas existindo a necessidade de proteção, e havendo pessoas que percebam bem estes conceitos, deveriam fazer algum tipo de ação de formação que consiga dar a entender melhor esta problemática. Mesmo meios informais, por divulgação, fazer chegar informação às pessoas, apesar de não ser o meio mais eficaz. Mas para as pessoas que necessitam de se dedicar a estes assunto, de fazer com que o meu trabalho seja sensível a esta informação é preferível que exista alguma formação, algum *workshop*.
P1.V4.1 – P2INEM#04	Formação, qualquer que seja o modelo. A presença de profissionais especializados nas organizações seria fundamental, para que estas questões fossem abordadas com maior responsabilidade. Isto é uma área de tal forma exigente que tem que ser agarrada por profissionais com experiência e com disponibilidade.
P1.V4.1 – P2INEM#09	Havendo pessoas nas organizações, podemos chamar-lhe grupo de trabalho multidisciplinar, que desenvolvam iniciativas como ações de formação, ações de sensibilização. Até mesmo o desenvolvimento de folhetos informativos, que divulguem esta informação. Atenção ao excesso de informação. A coisa tem que ser tratada para que não sature as pessoas.
P1.V4.1 – P2INEM#10	Eu vejo isto em vários níveis. Ao nível do público em geral, através dos meios de comunicação social, sensibilizar para aquilo que são os seus direitos, como devem disponibilizar os seus dados. Ao nível dos profissionais de saúde, sensibiliza-los para o facto de lidarem com informação sensível, e que não devem facilitar. Através de profissionais dedicados que podem estar permanentemente no terreno. Explicar às pessoas as precauções a ter, e o porquê da proteção. Seria uma forma muito eficaz de promover uma cultura de privacidade.
P1.V4.1 – P3INEM#05	Dependendo que quem é o consumidor final, adequar formação específica às pessoas responsáveis pelo desenvolvimento das tecnologias. Alertar informáticos, gestores responsáveis pela estratégia, para o risco, para as situações de risco. É necessário uma sensibilização das pessoas mas focalizada, uma vez que quem é esta envolvido na conceção é diferente do consumidor final. O consumidor final que vai apenas utilizar o equipamento, tem de perceber que dados podem ser expostos, de maneira a proteger-se.
P1.V4.1 – P3INEM#06	As pessoas têm de saber porque recolhem os dados. É o principal princípio. Formação específica e devidamente orientada é uma das soluções a implementar. É um tema de que nós não falamos, que não abordamos. É raro haver ações de formação e de sensibilização sobre estes aspetos.
P1.V4.1 – P3INEM#07	Formação e divulgação de quais são os deveres e direitos dos profissionais de saúde. Informação sobre quando devemos disponibilizar e partilhar os nossos dados - cultura do lado do utente.
P1.V4.1 – P4INEM#08	Se não houver uma linha, se não se criar uma linha política, estratégica, uma análise de necessidades. Não podemos correr o risco de estar a fazer formação sobre coisas que as pessoas já dominam, ou estarem-nos a escapar questões básicas. Tenho que perceber o que é um programa de gestão do risco. O que são processos e gestão de processos. Há requisitos de base que podem ter que ser compridos, o que significa que avançar para isto sem uma análise de necessidades é um risco. Seminários, formação específica, são tudo ações que têm que decorrer, é necessário segmentar as pessoas, os organismos, o tipo de dados, o tipo de utilizador, para direcionar a cada um plano de comunicação que permita uma preparação global nestas matérias. Não há aqui um canal único. A questão é simplificar. É necessário pegar naquilo que já se pratica melhor. Já nos chegam regularmente empresas habilitadas em certificação da segurança. Se a este nível já existem standards que permitem a certificação também podem existir ao nível da proteção de dados. Não é descabido existir no âmbito daquilo que é a saúde, uma área de diferenciação, algum organismo, pode ser a SPMS, uma vez que tem competências na área dos sistemas de informação, que promova este desenvolvimento. Ser consultora das instituições neste domínio.
P1.V4.1 – P1HFF#01	Promover encontros com especialistas não académicos, com experiência. Internamente já estou a promover estas questões –

	políticas de segurança, de privacidade. Necessito de gabinete de segurança para a implementação. Em conjunto estou a realizar uma análise de riso.
P1.V4.1 – P2HFF#02	Haver por exemplos eventos sobre segurança e privacidade. Temos tido alguns eventos sobre a PDS, mas não são focados na privacidade e na segurança. Tentar preparar um grupo para criação de certificação para os sistemas de informação. Por exemplo apostar em *IT Governance* a sério. Desenvolver algumas ações de formação para responsáveis de sistemas de informação, mesmo até informalmente cartazes, emails a alertar para estas questões, informar como se deve proceder em situações de utilização de dados. Por exemplo a revista eSaude ter um capítulo orientado para estas questões. Haver alguma preocupação nas publicações periódicas sobre estas matérias.
P1.V4.1 – P2HFF#03	O que cativa sempre as pessoas é ter alguns casos práticos, quer a nível nacional como internacional. Poder sensibilizar através da mais-valia, ou porque houve problemas e os profissionais foram sancionados, ou porque existem casos práticos de problemas. Se isto culminar sempre na segurança do doente, temos a adesão dos profissionais. As pessoas não têm esta preocupação. É necessário um processo de evangelização muito grande. Por exemplo, um aspeto essencial e obrigatório nos hospitais, e em que eu não vejo nenhum tipo de garantia de que assim é, é o facto de estarmos todos abrangidos pelo sigilo profissional da saúde. De um modo geral, direta ou indiretamente todos temos acesso à informação clinica. Parte-se do princípio que todos sabem que há a obrigação de sigilo, mas isto não passa de uma ilusão teórica, porque eu nunca fui sensibilizado sobre isto. Posso-lhe dizer que nas várias empresas privadas onde trabalhei, fui sensibilizado todos os meses para a obrigação de sigilo profissional, e com exame escrito. Além da sensibilização regular, um *refresh*, com exames práticos.
P1.V4.1 – P3HFF#04	Pode começar nos programas académicos. Nós não temos o conceito de cidadania explorado, nem o conceito de privacidade e de todo o resto que aqui falamos. Fazia todo o sentido em termos curriculares adaptados obviamente a cada nível de progressão no ensino. Também a formação dos cidadãos nesta área em concreto. Muitas pessoas já saíram do sistema escolar e temos que chega a elas também. Na comunicação audiovisual, com debates televisivos, as pessoas ouvem. E quando ouvem comentam com outras estes temas, na sua esfera familiar ou social. Cria-se uma onda de debate, partilha de ideias, e de boas práticas. Isto leva a que as pessoas comecem a questionar o outro, com quem interage, ou começa a questionar a organização de saúde onde vai depositar os seus dados. Este debate é importante.
P1.V4.1 – P4HFF#05	Termos um organismo que nos dê as linhas mestras e que depois vá desenvolvendo em conjunto com as organizações todo o normativo de suporte legal, técnico, de gestão que seja necessário à implementação. Temos um conjunto alargado de instituições públicas e privadas que devem ter acesso ao mesmo nível de informação. Por mais eventos que se façam, se não existir um normativo de base, o desenvolvimento é mais complexo.
P1.V4.1 – P1SPMS#02	Promover reuniões com os responsáveis de várias instituições, hospitais nomeadamente. Organizar congressos e abordar a questão da privacidade, até para os profissionais de saúde, apesar de estes terem esta perceção. Todas as formações existentes relacionadas com BI, extração de dados, tratamento de dados, deveriam abordar este tema. Deveria ser obrigatório, os responsáveis dos sistemas de informação terem formação neste domínio. Acredito que quando estas pessoas se consciencializarem que a questão a privacidade é crítica, se vai criar esta preparação global. Dou um exemplo, existem várias técnicas de anonimização de dados. Mas depois fica-se sem saber o contexto e a justificação da sua aplicação. Deveriam existir regras. Por exemplo na extração de um registo clinico de um utente, que informação é que vou anonimizar?
P1.V4.1 – P2SPMS#03	Fazer workshops muito direcionados, para aquilo que são as nossas áreas. Promover formação no sentido de preparar as pessoas para a implementação de um conjunto mínimo de princípios. Nem todos conseguem chegar a uma norma e depois conseguir

	transpor essa norma para a própria organização. O facto de podemos transpor processo de uma organização para outras, promove a partilha do conhecimento sobre estas matérias, sobre os processos que se vão aplicando e dos mecanismos que se vão utilizando. Nestas questões não necessitamos de estar todos a inventar a mesma coisa, podemos partilhar conhecimento. Seria um princípio facilitador. Depois mudar o paradigma para o cidadão é muito importante. Aos poucos vamos tendo pequenos avanços. Nas farmácias já é obrigatório a utilização do cartão de cidadão para aceder à minha informação. Significa que não podem aceder à minha informação sem que eu dê autorização para isso. Às vezes, são pequenas funcionalidades que se implementam e que trazem grandes ganhos em privacidade. Não podemos atuar depois de o problema ter acontecido, mas sim antes. Monitorizar a utilização dos dados e se necessário ativar mecanismos de proteção antes de acontecer o problema. Implica que se olhe para os dados, para o cidadão e se façam transformações ao nível dos sistemas de informação, uma vez que não foram concebidos desde o seu início para terem controlos de privacidade. Trabalhamos com alguns sistemas estruturantes que têm vinte anos. E os problemas que se colocavam há vinte anos, nada têm a ver com os problemas que se colocam hoje me dia.
P1.V4.1 – P2SPMS#04	Eventos ou *workshops* temáticos, onde possam ser apresentados os projetos, experiências, problemas existentes. Promover ações de formação neste domínio.
P1.V4.1 – P1HES#01	É necessário que as organizações falem sobre isto. Deve ser promovido um debate, conferência, que façam as pessoas pensar sobre estas questões. São coisas que nós não pensamos no nosso dia-a-dia, não porque pensamos que não são importantes, mas devido à falta de tempo. Posteriormente promover ações de formação especializadas. Promover encontros entre responsáveis pelos sistemas de informação, à semelhança do que aconteceu com a implementação da PDS. Sessões de trabalho em grupo, em que são analisadas uma série de assuntos. São experiências riquíssimas. Permitem ver os problemas de acordo com a opinião especializada dos vários perfis profissionais. E numa questão destas, em que se sabe tão pouca coisa, poderia ser um bom ponto de partida.
P1.V4.1 – P2HES#02	Formação base para todos os profissionais para utilizarem de forma correta as aplicações. Ainda temos pessoas que não dominam as tecnologias. Formação sobre legislação de proteção e dados. Seria importante. Este deveria ser um conhecimento que devia constar nos currículos ao nível de cursos superiores. Eventos que permitam consciencializar as pessoas da importância para a privacidade dos dados e da partilha destes mesmos dados.
P1.V4.1 – P2HES#03	A informação e a formação são importantes a este nível. Não só dos técnicos de informática, mas também quem trata e trabalha com os dados. É necessário poder falar-se sobre a segurança informática, e a experiência em cada instituição, para conhecermos cada instituição, porque a nossa realidade é diferente mas semelhante a outras. Eventos para partilhar experiências. Eventos com o apoio de empresas de novas tecnologias, para podermos conhecer qual a evolução a desenhar. Dar formação às pessoas dentro do domínio da análise do risco, para que as pessoas percebam o que é uma análise do risco, que normas existem, e depois construírem aquilo que é a segurança em bases mais solidas. É muito importante. Existe um défice muito grande ao nível da informação, do que é que existe a nível nacional, do que é que se está a desenvolver. Ainda não existe muita colaboração entre profissionais. As pessoas saem pouco daquilo que são as fronteiras do seu sistema. Para a evolução que a SPMS quer que as instituições tomem no futuro, a colaboração é fundamental. Os sistemas estão preparados em termos de disponibilidade, mas depois temos grandes lacunas em conhecimento e informação sobre partilha de dados. Começa-se a partilhar dados de uma forma não segura.

	A investigação é também importante, porque acaba por se traduzir em melhorias na organização. Isto já acontece. Havendo uma maior disponibilidade das pessoas para a investigação, melhorar aquilo que é processos, pode ser uma forma de canalizar conhecimento para a organização. Os sistemas de informação da saúde não podem evoluir apenas com base na investigação de profissionais externos. Quem está no terreno não está a ser valorizado em termos de formação. Tem que se começar a preparar pessoas nestas matérias.
P1.V4.1 – P3HES#05	Não é falta de preparação, é falta de meditação sobre estas coisas. Esta temática deve fazer parte da formação dos jovens médicos e enfermeiros. Depois deveria ser obrigatório, alguma formação anual sobre isto. Esta não pode ser uma coisa individual, tem que ser uma coisa institucional. Não pode ser de outra maneira.
P1.V4.1 – P4HES#06	Periodicamente nos EUA existe uma exposição em que cada empresa expõe os seus equipamentos, as suas aplicações, e a sua capacidade de interoperabilidade. Não é uma feira, é uma sessão de trabalho. A SPMS deveria da mesma forma mostrar as soluções de interoperabilidade das soluções que desenvolve com outros sistemas. Eles estão neste momento com uma frente para a interoperabilidade. Existem já hospitais com soluções implementadas de interoperabilidade. É necessário, sempre, mais formação em proteção de dados para todos os profissionais. É necessário contar com a necessidade de atualização de normas, legislação.

2. *Data Reduction*

P1.V1.1	***Perfil 1** / Responsáveis pela implementação e coordenação da PDS*	***Perfil 2** / Técnicos e responsáveis pelos sistemas de informação*
Padrão	"Sem dúvida" (P1.V1.1 – P1ULSNA#01)	"Com toda a certeza, quanto mais projetos maior a experiência" (P1.V1.1 – P2ULSNA#02)
Conhecimento dependente da experiência	"A PDS [...] está a obrigar as pessoas a pensar de maneira diferente, [...], e o seu conceito interiorizado nos profissionais para que estes vejam a PDS como uma boa ferramenta de trabalho. A PDS é um excelente exemplo de partilha de dados" (P1.V1.1 – P1ULSNA#01)	"É o caso da PDS, [...], e pequenas ligações a bases de dados do hospital de Évora, onde obtemos dados de exames feitos lá, que não conseguirmos fazer localmente. A própria troca de informação a nível de videoconferência, partilha de informação clinica, apesar de resumida entre especialistas" (P1.V1.1 – P2ULSNA#02)
Experiência é fundamental ao sucesso da partilha de dados e na redução do risco	"Se não houver um rigor na disponibilização de informação, [...], a qualidade da informação disponibilizada acaba por retrair os profissionais na sua utilização " (P1.V1.1 – P1ULSNA#01)	"Completamente, eu acho que sim" (P1.V1.1 – P2ULSNA#03)
Tendência para uma maior atenção para com a proteção de dados	"Está, acima de tudo dependente disso. Ou seja, quanto mais experiência os profissionais tiverem dentro deste domínio, mais garantido está o sucesso da proteção de dados" (P1.V1.1 – P1USF#01)	"Temos um projeto de interoperabilidade, que embora interno é abrangente, trata-se de uma plataforma que pesquisa dados em várias aplicações" (P1.V1.1 – P2ULSNA#03)
A interoperabilidade é um desafio recente.	"É necessária uma disponibilidade dos profissionais para a partilha de dados" (P1.V1.1 – P1USF#01)	"Acho que sim. [...] Existe um contexto propício para que sejam consideradas as questões da proteção de dados a "sério" (P1.V1.1 – P2USF#02)
	"Pode depender muito" (P1.V1.1 – P1INEM#01)	"Neste momento e como está tudo muito vago, sim. Quanto mais experiência a equipa tiver dentro destas áreas, mais fácil se implementa políticas de proteção. Estão mais rotinados com aquilo que poderão ser os problemas a ser encontrados." (P1.V1.1 – P2INEM#03)
	"Numa fase iniciar as pessoas são muito sépticas quanto às soluções de integração e recolha de dados, mas depois quando começam a aperceber-se dos benefícios, são os principais dinamizadores destas soluções" (P1.V1.1 – P1INEM#01)	"Uma instituição que não tenha experiência em projetos de partilha de dados, de interoperabilidade dificilmente vai conseguir desenvolver políticas conjuntas de proteção de dados." (P1.V1.1 – P2INEM#04)
	"Estes projetos [de interoperabilidade], estas iniciativas despertam nas pessoas uma atitude de preocupação em relação aos dados, em relação á troca de dados." (P1.V1.1 – P1SPMS#02)	"Uma organização pela sua natureza, pela natureza daquilo que desenvolve, pode ainda não ter tido a oportunidade de observar um conjunto de preocupações e de problemas que outra organização poderá ter antecipado e estar na posse de um conjunto de soluções que pode partilhar com quem ainda está a iniciar este processo." (P1.V1.1 – P2INEM#04)
	"Pode haver aqui uma dependência direta entre a experiência da partilha de dados e a proteção desses dados." (P1.V1.1 – P1SPMS#02)	"Sim podemos afirmar que sim." (P1.V1.1 – P2INEM#09)
	"É esta a tendência, de caminharmos para um sistema único, com base na interoperabilidade, e esta tendência está a despertar nas pessoas uma maior atenção nas questões de proteção de dados. Assim como as pessoas estão mais desconfiadas pelo facto de haver um maior controlo sobre a informação." (P1.V1.1 – P1SPMS#02)	"Sim a experiência aqui é fundamental" (P1.V1.1 – P2INEM#10)
	"Existe uma relação e que transmite confiança" (P1.V1.1 – P1HES#01)	"Sim quanto mais experiência melhor – diminui o risco de haver problemas de privacidade. Quanto mais experiência se tiver em projetos de partilha de dados maior a probabilidade de sermos proactivos e não reacionários. Gradualmente é mais simples efetuar alterações, desenhar medidas." (P1.V1.1 – P2HFF#02)
		"Ao nível dos hospitais o que nós fazemos ao nível da interoperabilidade é

	ainda muito imaturo. A experiência que há é mínima. [...] Deveria haver um maior investimento neste domínio." (P1.V1.1 – P2HFF#03)
	"[...] numa primeira fase eu não consigo ver como vamos aplicar modelos de privacidade à informação, se a informação não estiver ela própria bem categorizada" (P1.V1.1 – P2HFF#03)
	"Tenho de garantir primeiro a base, que a informação está lá, e que está devidamente estruturada num repositório digital. Depois posso aplicar práticas de interoperabilidade. [...] A interoperabilidade também é um desafio recente. Só há poucos anos a que de facto os hospitais começaram a fazer que os sistemas falassem entre eles." (P1.V1.1 – P2HFF#03)
	"Mas na minha opinião o meio tecnológico da partilha de dados passou a existir, não que com isso também tenha aumentado a preocupação em relação á proteção de dados." (P1.V1.1 – P2SPMS#03)
	"Gradualmente, temos cada vez mais situações de partilha de dados e de serviços, e como consequência, uma maior atenção e consciência em relação às questões da proteção de dados." (P1.V1.1 – P2SPMS#04)
	"Responsáveis dos sistemas de informação e técnicos ao nível local, a partir do momento em que começam a desenvolver soluções de partilha de dados com outras instituições, começam a olhar para estas questões [da privacidade dos dados] de uma outra maneira" (P1.V1.1 – P2HES#02)
	"É um fator que surge com a experiência, com o conhecimento" (P1.V1.1 – P2HES#02)
	"Sim é mais fácil para alguém que já tenha experiência em gestão da informação, que saiba com o que é que está a trabalhar, que tipo de informação se trata, a sua criticidade, desenhar medida de proteção" (P1.V1.1 – P2HES#03)
	"A experiência que nós temos de partilha de dados com outras instituições ainda é pouca. O aumento destas situações vai sem dúvida despertar questões sobre a proteção de dados. A nossa experiência em interoperabilidade de bases de dados ainda está numa fase inicial" (P1.V1.1 – P2HES#03)

P1.V2.1	***Perfil 1** / Responsáveis pela implementação e coordenação da PDS*	***Perfil 2** / Técnicos e responsáveis pelos sistemas de informação*
Padrão Segurança Proteção de dados Dinamização da colaboração local Conhecimento dos dados, da sua importância e da sua criticidade Legislação Visão global e estratégica dos sistemas de informação	"Matéria de segurança decididamente sim, e privacidade e proteção de dados também. Estas três vertentes estão muito interligadas." (P1.V2.1 – P1ULSNA#01)	"Conhecimento dos sistemas TI, o ambiente dos profissionais, as tendências de trabalho dos profissionais, conhecimento das entidades externas com quem se colabora, conhecer os serviços, onde estão os dados críticos." (P1.V2.1 – P2ULSNA#02)
	"Experiência tecnológica é muito importante. Conhecimentos ao nível da segurança. Os conhecimentos ao nível da privacidade dependem das tecnologias utilizadas." (P1.V2.1 – P1USF#01)	"No tratamento de dados. Preservar os dados primários, neste caso os utentes. Saber construir uma hierarquização de dados (classificação), níveis. É muito importante esta classificação para depois conhecer melhor o que se está a partilhar." (P1.V2.1 – P2ULSNA#03)
	"É importante e exigível que no futuro os responsáveis pelos sistemas de informação ou outro tipo de técnicos venham a ganhar experiência em matéria de proteção de dados." (P1.V2.1 – P1INEM#01)	"[…] é necessário que este saiba os requisitos legais e como devem ser aplicados, não é necessário um conhecimento como as aplicar tecnicamente. É necessário que na organização, nos diferentes peris técnicos, dentro do IT disponível, que seja capaz de fazer cumprir estas imposições, implementar estes requisitos." (P1.V2.1 – P2USF#02)
	"E queremos aproveitar esta experiência [certificação ISO 9000] para avançarmos para a certificação da ISO 27000, em segurança da informação. A proteção de dados é assim um caminho a seguir." (P1.V2.1 – P1INEM#01)	"[…] tenha conhecimentos de segurança, principalmente durante o desenvolvimento de soluções. Por outro lado é necessário um conhecimento dos conceitos de privacidade, que ainda estão muito vagos. Se até determinada altura as pessoas não tinham uma cultura de segurança, passaram a ter uma cultura de segurança, e a implementar soluções de segurança, hoje em dia estamos no dados e temos que começar a ter uma cultura muito virada para os dados […] " (P1.V2.1 – P2INEM#03)
	"O ideal é os responsáveis perceberem desta necessidade [da proteção de dados], e serem eles próprios os indutores da mudança internamente. Ou seja, este compreende, absorve, divulga por todas a instituição, e estabelece o compromisso" (P1.V2.1 – P1HFF#01)	"[…] é essencial que estes deixem de olhar para cada sistema como uma caixa fechada, e troquem experiências com outros de outras organizações. São as pessoas ideais para desencadear estes processos [proteção de dados]" (P1.V2.1 – P2INEM#04)
	[…] pode criar-se um gabinete para o *chief security information officcer*, ou alguém com esta responsabilidade. Ou seja, um grupo de trabalho dedicado" (P1.V2.1 – P1HFF#01)	"Tecnologicamente conhecem os sistemas como ninguém. Conhecem os processos e conseguem dinamizar colaboração com alguma facilidade, mas falta-lhes um conhecimento mais aprofundado em matérias de proteção de dados." (P1.V2.1 – P2INEM#04)
	"O *privacy information officer* é sem dúvida o caminho a seguir no futuro" (P1.V2.1 – P1HFF#01)	"[…] preponderante é a gestão de sistemas e de informação [bases de dados], segurança de sistemas e infraestruturas. É necessário, cada vez mais apostar na proteção de dados" (P1.V2.1 – P2INEM#09)
	"Para estes profissionais esta questão da privacidade tem que ser clara. Ter uma estratégia para a segurança e para a proteção de dados. Difundir esta informação pelas instituições" (P1.V2.1 – P1SPMS#02)	"Garantidamente tem que ter conhecimentos em segurança. Experiência em segurança. Ao nível da proteção de dados acaba por se aplicar a mesma regra" (P1.V2.1 – P2INEM#10)
	[…] "com o avançar da era da informação, é que as pessoas comecem a dar o mesmo valor ou até cada vez mais a proteção da informação" (P1.V2.1 – P1SPMS#02)	"Isto não é um problema de uma instituição mas do conjunto" (P1.V2.1 – P2INEM#10)
	[…] "devem ser preparados e consciencializados para a questão da privacidade e mais focados na questão dos dados" (P1.V2.1 – P1SPMS#02)	[…] "comecem a ter competências na área de proteção e dados e não apenas naquilo que é segurança de infraestruturas e informação " (P1.V2.1 – P2HFF#02)
	[…] mas temos que começar a olha para a informação. Nós não temos a noção da criticidade da informação que está a	

	ser disponibilizada" (P1.V2.1 – P1SPMS#02)	"O posicionamento preferencial para estas questões é dentro do *IT Governace*" (P1.V2.1 – P2HFF#03)
	"Cada vez mais deveríamos apostar em profissionais especializados, principalmente se tivermos em conta a criticidade que a informação representa neste momento, a forma como esta informação está a ser gerada, distribuída, pelo país fora, não tenho dúvidas nenhumas" (P1.V2.1 – P1HES#01)	"Profissionais que possam estar preparados, para que de alguma forma, vejam a globalidade do sistema e consigam desenhar medidas que sejam eficientes para a proteção de dados"
		"É claro que a visão da floresta (*IT Governance*) é fundamental, assim como um conhecimento da legislação, e uma preocupação em relação a estes assuntos" (P1.V2.1 – P2HFF#03)
		"Pessoas que têm a visão do projeto do sistema de informação, e que sejam capazes de induzirem esse trabalho" (P1.V2.1 – P2HFF#03)
		[...] "um conhecimento sobre a legislação" (P1.V2.1 – P2SPMS#03)
		"Perceber quais os princípios que devem estar na base de proteção de dados. Ajudaria se existissem princípios generalizados" (P1.V2.1 – P2SPMS#03)
		"Ter conhecimento e competências neste nível de informação seria muito útil" (P1.V2.1 – P2SPMS#03)
		"É necessário olhar para os sistemas mais numa visão estratégica e não apenas tecnológica" (P1.V2.1 – P2SPMS#03)
		"Conhecer tudo em termos de legislação, normas e segurança de dados" (P1.V2.1 – P2SPMS#04)
		"Alguém dentro da equipa [de sistemas de informação] deve dar este suporte" (P1.V2.1 – P2HES#02)
		"A experiencia em segurança pode ter aqui algumas vantagens, podendo ser numa primeira fase ser suficiente, mas depois tem que ser mais desenvolvida" (P1.V2.1 – P2HES#02)
		"A área da privacidade é um mundo à parte da segurança. Tem que ser uma pessoa com um grande domínio tecnológico, um grande domínio organizacional e também jurídico" (P1.V2.1 – P2HES#02)
		"Em termos de dados é essencial que conheça quais é que são os dados mais críticos, como é que são partilhados" (P1.V2.1 – P2HES#03)
		"O conhecimento existente em termos de proteção de dados é pouco, pelo que é necessário que desenvolva conhecimentos neste domínio. É necessário conhecer o que é que implica [a proteção de dados], evoluir na proteção de dados" (P1.V2.1 – P2HES#03)
		"Basta ter uma experiência que correu bem, e as pessoas aprendem muito com esta experiência. Ficamos a saber quais os requisitos mínimos que temos que contemplar. A próxima experiência já corre melhor. Também é importante aprender com os erros dos outros, o que implica a colaboração" (P1.V2.1 – P2HES#03)
		"Os sistemas estão preparados em termos de disponibilidade, mas depois temos grandes lacunas em conhecimento e informação sobre partilha de dados" (P1.V4.1

	– P2HES#03)	

P1.V2.2	***Perfil 1** / Responsáveis pela implementação e coordenação da PDS*	***Perfil 2** / Técnicos e responsáveis pelos sistemas de informação*
Padrão Impacto positivo Bastante importante Fundamental É necessário um maior conhecimento Desperta a atenção para a proteção de dados	"Contribuir positivamente para a melhoria da implementação de medidas adequadas à legislação" (P1.V2.2 – P1ULSNA#01)	"Sem dúvida alguma" (P1.V2.2 – P2USF#02)
	"Pode ter um efeito prático bastante importante" (P1.V2.2 – P1USF#01)	"Legalmente tem que haver alguém em permanência com conhecimento em legislação, e pedir a alguém a sua aplicação. O não conhecimento da lei não é resposta para coisa nenhuma. Temos que conhecer, saber o que existe e aplicar" (P1.V2.2 – P2USF#02)
	"Ao nível dos responsáveis pelos sistemas seria importante este conhecimento, dado que na maioria das vezes a sua maior preocupação é desenvolver as aplicações e colocá-las disponíveis" (P1.V2.2 – P1USF#01)	"Sim teria um efeito benéfico" (P1.V2.2 – P2INEM#03)
	"Seriam mais sensíveis, em momentos como os de criar utilizadores, atribuir permissões. Acima de tudo restringiam mais o acesso aos dados. Este conhecimento passa muito pela sensibilidade de cada um para estas questões" (P1.V2.2 – P1INEM#01)	"Se estamos a tratar de dados confidenciais, é necessário trata-los o mais seguro possível e de acordo com aquilo que é exigível" (P1.V2.2 – P2INEM#03)
	"Um maior conhecimento nesta área é sem dúvida fundamental. É necessário um maior reforço neste conhecimento" (P1.V2.2 – P1HFF#01)	"As pessoas que fazem a ponte com outros sectores, nomeadamente as administrações, deveriam ter um maior conhecimento nestas matérias" (P1.V2.2 – P2INEM#04)
	"Seria muito útil, sem dúvida. [...] Esta prática deveria ser fomentada nas organizações" (P1.V2.2 – P1SPMS#02)	[...] "ser importante o desenvolvimento de uma maior sensibilidade para estas questões" (P1.V2.2 – P2INEM#04)
	"É como uma cultura, que faça com que as pessoas sempre que pegam nesta temática leiam a legislação, uma vez que temos que estar informados sobre a legislação que sai sobre proteção de dados" (P1.V2.2 – P1SPMS#02)	"Um maior conhecimento da legislação poderia ajudar" P1.V2.2 – P2INEM#09
	"Seria um catalisador de algumas medidas imediatas" (P1.V2.2 – P1HES#01)	"Sim, pelo menos as pessoas pensavam melhor antes de disponibilizar um conjunto de dados" (P1.V2.2 – P2INEM#10)
		"Despertava a consciência e a preparação, para questionarem o porquê da utilização dos dados" " (P1.V2.2 – P2INEM#10)
		"Despertava logo alguns profissionais. Como não existe esta preocupação constante acabamos por não dar atenção a esta questão" (P1.V2.2 – P2HFF#02)
		"Sem dúvida que é importante um conhecimento a este nível" (P1.V2.2 – P2HFF#03)
		"Existe um conhecimento generalizado sobre o problema, mas depois não existe um conhecimento especializado, detalhado" (P1.V2.2 – P2HFF#03)
		"Eu tenho muita dificuldade em saber o que devo exigir em termos de propriedade, segurança, responsabilidade. Saber aplicar a legislação é complicado" (P1.V2.2 – P2HFF#03)
		"Só o simples conhecimento da legislação, dos regulamentos, teria um impacto positivo. [...] As pessoas têm de perceber a lei, pois só assim é que conseguem avaliar depois. Podem agir com conhecimento" (P1.V2.2 – P2SPMS#03)
		"O feito prático seria muito positivo. As pessoas não têm este hábito" (P1.V2.2 – P2SPMS#04)
		"Uma maior consciencialização das pessoas, sem dúvida nenhuma" (P1.V2.2 – P2HES#02)
		"Daí que um conhecimento maior em legislação, diminuía o facilitismo" (P1.V2.2 – P2HES#02)
		Só com um conhecimento sobre o que implica a legislação de proteção de dados desencadearia um conjunto de medidas" (P1.V2.2 – P2HES#03)
		"Mas não há como inverter o caminho da evolução dos sistemas. E o caminho é partilhar. Se houvesse mais informação em todos os intervenientes, em termos de legislação, dados, técnicos, acho que era mais fácil evoluir" (P1.V2.2 – P2HES#03)

P1.V3.1	*Recursos humanos de suporte*	*Estrutura organizativa de suporte*
Padrão *Recursos humanos dedicados exclusivamente* *Especialistas focados nos dados* *Responsabilidade de vários decisores* *Equipa pluridisciplinar ou comissão estruturada* *//* *Equipa permanente que coordene o contexto global da colaboração*	[...] "especialistas em segurança, área de redes. Especialistas em proteção de dados, acabam por abranger todas as áreas transversais que levam à proteção de dados" (P1.V3.1 – P1ULSNA#01)	[...] "para o contexto da colaboração justifica-se a existência de uma equipa a trabalhar estas questões" (P1.V3.1 – P1ULSNA#01)
	"É fundamental o envolvimento da parte jurídica" (P1.V3.1 – P1ULSNA#01)	"Ao nível do ministério da saúde já se justifica a existência de uma equipa permanente. [...] Compensava ter uma equipa permanente para o desenvolvimento conjunto. Poderia salvaguardar as questões da privacidade na PDS" (P1.V3.1 – P1INEM#01)
	"Sim deveriam existir recursos humanos dedicados á privacidade" (P1.V3.1 – P1USF#01)	"Justifica-se uma estrutura de suporte ao contexto alargado de partilha de dados" (P1.V3.1 – P1INEM#01)
	"Talvez não seja necessário uma pessoa a tempo inteiro dedicada a estas questões. Pelo menos justifica-se a existência de um grupo de trabalho que de vez em quando faça e defina estes assuntos" (P1.V3.1 – P1INEM#01)	"[...] faz todo o sentido que exista uma instituição que consiga ligar todas as organizações em relação a estas questões. [...] Isto é muito mais conceptual ao nível da gestão da informação, do que questões técnicas." (P1.V3.1 – P1HFF#01)
	"É importante a participação de um gabinete de gestão de risco, e se pensarmos ao nível do *IT Governance*, um *chief security information officer*" (P1.V3.1 – P1HFF#01)	"Para o todo da colaboração [...], deveria haver uma equipa que colaborasse com as equipas de TI dos hospitais mais para as questões de proteção dos dados" (P1.V3.1 – P2ULSNA#02)
	"[...] a gestão da informação é a parte mais importante. Contudo, tudo isto depende da grande maturidade do responsável por um gabinete a este nível que consiga dialogar com todos os outros departamentos" (P1.V3.1 – P1HFF#01)	"Concordo com a necessidade de existirem profissionais dedicados a estas matérias, a tempo inteiro, nomeadamente ao nível da ARS" (P1.V3.1 – P3USF#03)
	"Uma equipa tripartida, administração, área clinica, e TI" (P1.V3.1 – P2ULSNA#02)	"Ao nível do ministério, aqui sim justifica-se profissionais em privacidade, dedicado a criar normas transversais para todo o ministério da saúde "(P1.V3.1 – P2USF#02)
	[...] "seria uma mais-valia ter alguém focado nos dados" (P1.V3.1 – P2ULSNA#02)	"Mas para o universo que é a rede da saúde, [...] faz sentido ter uma equipa de apoio, de topo, que desenvolva projetos comuns " (P1.V3.1 – P2INEM#03)
	"De facto é necessário, um técnico [...] com conhecimentos em proteção de dados, nem que sejam conhecimentos básicos. Sem dúvida que a administração, sistemas de informação e a parte jurídica devem estar relacionados com estas questões" (P1.V3.1 – P2ULSNA#03)	"[...] sempre se justificou a existência de profissionais especializados, não só em proteção de dados, como na segurança dos dados. Para á área da saúde justifica-se uma equipa permanente a desenvolver estas questões" (P1.V3.1 – P2INEM#04)
	[...] "uma equipa multidisciplinar que tenha uma visão transversal, que tenha elementos de redes, elementos de sistemas, juristas [...] (P1.V3.1 – P2USF#02)	"Em simultâneo deve haver um staff mais alargado que cobrisse todo o ministério da saúde" (P1.V3.1 – P2INEM#09)
	[...] "é importante apostar-se nestes profissionais. O princípio ético, que nos diz muito respeito, tem que ser transportado para as ferramentas informáticas" (P1.V3.1 – P3USF#04)	"[...] se justifica haver recursos humanos dedicados à questão da proteção de dados. É algo que é importante, que é sério, logo justifica ter recursos humanos dedicados. Para o âmbito mais alargado, [...], no sentido de fazer as reavaliações, é necessário uma equipa permanente [...]" (P1.V3.1 – P2INEM#09)
	[...] ao nível mais local, [...], tem que existir alguém que tenha uma maior preparação, que tenha uma facilidade nestas questões. Uma equipa pluridisciplinar faz sentido" (P1.V3.1 – P2USF#02)	"Justificava-se ao nível da SPMS haver profissionais dedicados a tempo inteiro a estas questões. [...] Que pode realizar auditorias, [...]. Desenhar soluções de uma forma centralizada, [...], harmonizar soluções, uniformizar os processos de privacidade e segurança. O caminho é centralizar e caminhar para a certificação. Esta estrutura poderia revolucionar as organizações" (P1.V3.1 – P2HFF#02)
	"Tem que ser um individuo multidisciplinar, por um lado um tecnólogo e por outro tem que ser também um individuo com competências em gestão, fazer auditorias regulares, as análises de conformidade que falamos" (P1.V3.1 – P2INEM#03)	"Sim justifica-se [uma estrutura organizativa de suporte]" (P1.V3.1 – P4ULSNA#06)
	"Sim considero necessário haver recursos humanos dedicados a estas questões" (P1.V3.1 – P2INEM#09)	
	" haver [...] uma pessoa exclusivamente dedicada a estas questões, a colocar medidas no terreno, a auditar, seria uma mais-valia" (P1.V3.1 – P3USF#06)	
	"Localmente é necessário haver um auditor em privacidade e segurança, que não existe - um profissional com competências em privacidade, especializado nestas matérias" (P1.V3.1 – P2HFF#02)	
	"Esta necessidade vai começar a sentir-se mais, com o surgir de novas tecnologias e ferramentas, será muito natural que surjam estes profissionais" (P1.V3.1 – P3USF#06)	
	"[...] justifica-se numa organização como a nossa a presença de profissionais especializados em proteção de dados, com esta função" (P1.V3.1 – P3INEM#05)	
	"É necessário um maior desenvolvimento de direitos e deveres dos profissionais em relação aos dados" (P1.V3.1 – P3INEM#05)	

“Seria um passo muito importante” ” (P1.V3.1 – P3INEM#05)	“Quem desenvolve estes sistemas [para o SNS] devem ter recursos que estejam dentro da área da privacidade” (P1.V3.1 – P4USF#05)
[...] “se justifica profissionais dedicados a estas questões, e cada vez mais vão ser importantes, pois cada vez mais vai haver maior partilha” (P1.V3.1 – P3INEM#06)	“Se existir no ministério da saúde um organismo que tem como função, auditar os sistemas de informação, analisar o risco, e implementar ferramentas que garantam a proteção de dados, será ótimo” (P1.V3.1 – P4INEM#08)
[...] é necessário especialistas em análise de impacto sobre a privacidade. Faz todo o sentido a presença nas organizações de profissionais especializados em privacidade, que acompanhassem o dia-a-dia das instituições, fazendo auditorias, melhorias continuas“ (P1.V3.1 – P3INEM#07)	“Os exemplos bons que eu conheço, de desenvolvimentos de coisas deste género, passam por haver equipas a nível nacional, dedicados exclusivamente durante um prazo. [...]. Isto é indutor de um movimento completamente diferente, porque existe uma transparência e obriga a um *benchmarking* constante. Depois em cada instituição existe um elo de ligação com esta responsabilidade” (P1.V3.1 – P2HFF#03)
[...] “a introdução de um profissional como “delegado de dados”, o meu receio é que as instituições tenham que o fazer por imposição e não por iniciativa própria” (P1.V3.1 – P4ULSNA#06)	“Para o domínio da saúde, a globalidade destas questões, depende da existência de uma entidade que tenha esta preocupação, caso contrário acabamos por ter apenas situações pontuais de desenvolvimento” (P1.V3.1 – P4HFF#05)
[...] “é importante existirem recursos humanos dedicados a esta matéria” (P1.V3.1 – P4USF#05)	“A nível nacional poderia ser criado um grupo para coordenar este desenvolvimento” (P1.V3.1 – P1SPMS#02)
“[...] a organização tem que ter acesso a um conhecimento técnico, que obriga a uma especialização, a fazer uma diferenciação” (P1.V3.1 – P4INEM#08)	“Isto vai surgir. É necessário como que uma “revolução silenciosa”” (P1.V3.1 – P1SPMS#02)
“[...] vai ter que haver um responsável pela privacidade da informação. Vamos chegar um dia a um *privacy information officer*.” (P1.V3.1 – P2HFF#03)	“Para o domínio alargado da partilha de dados, para o SNS, faria todo o sentido haver uma equipa que coordena-se esta questão. O objetivo deste grupo é definir um denominador comum. Ou seja, no mínimo o que é que todos temos que ter. E depois dar um apoio às entidades para conseguirem chegar a este mínimo.” (P1.V3.1 – P2SPMS#03)
“Dentro das organizações deveria existir uma comissão estruturada. Nós temos a comissão de ética, informatização, auditoria, qualidade e segurança do doente, onde está implícito os dados. Deveria haver recursos humanos a tempo inteiro afetos a estas questões e a promover o seu desenvolvimento dentro das organizações. Facilita também aquilo que é a colaboração com outras organizações” (P1.V3.1 – P3HFF#04)	“Para o âmbito nacional, faz sentido, haver uma equipa responsável, que fomente este desenvolvimento, caso contrário vamos ter apenas situações pontuais de desenvolvimento” (P1.V3.1 – P2SPMS#04)
“É importante que dentro das organizações comecem a surgir pessoas com uma maior especialidade nestas matérias” (P1.V3.1 – P4HFF#05)	“Para o domínio mais alargado de partilha de dados, a SPMS como regulador, tem que olhar para esta questão. Justifica-se haver uma estrutura organizativa que suporte, que de alguma forma olhe para estas questões como um todo, e que promova uma maior colaboração entre especialistas, com base num conjunto de objetivos para a privacidade dos dados” (P1.V3.1 – P1HES#01)
“Justifica-se nas organizações pessoas dedicadas às questões da privacidade” (P1.V3.1 – P1SPMS#02)	“Justifica-se que exista uma equipa multidisciplinar a nível nacional, que pudesse reunir e trocar informação, composta por elementos das principais instituições do ministério. À semelhança de algumas iniciativas semelhantes na área clinica. [...] Tem que ser criada com base na colaboração entre as principais instituições, na partilha de experiências, de recursos, na otimização de processos” (P1.V3.1 – P2HES#02)
“Temos que ter alguém preocupado com a evolução, com as novas orientações, estar sempre a par do que está as ser publicado, e implementar na organização. Em termos futuros são profissionais que vão desempenhar um papel importantíssimo nas organizações” (P1.V3.1 – P1SPMS#02)	“O ideal era haver uma equipa de suporte ao nível a SPMS. Uma equipa que consiga estar algum tempo nas instituições e dar alguma preparação às pessoas localmente” (P1.V3.1 – P2HES#03)
“Antes de mais as pessoas têm de ser informadas e alertadas sobre todas estas questões da privacidade. Têm que ter noção desta necessidade e desta responsabilidade” (P1.V3.1 – P1SPMS#02)	
[...] justifica que comece a haver dentro das instituições perfis profissionais em privacidade. É necessário pessoas a olhar para os dados e que percebem como implementar estas questões. Poderia dar-se um salto qualitativo nesta matéria” (P1.V3.1 – P2SPMS#03)	
“É necessário, começar por criar pontos de contacto dentro das organizações, figuras formais que pudessem transpor estas iniciativas e que as promovessem dentro das organizações” (P1.V3.1 – P2SPMS#03)	
“Começa a justificar-se que existam nas instituições pessoas dedicadas a estas questões” (P1.V3.1 – P2SPMS#04)	
“Haver dentro das instituições profissionais especializados em proteção de dados. Que possa por exemplo abranger aquilo que é a análise de risco” (P1.V3.1 – P1HES#01)	
“É fundamental haver profissionais especializados em proteção e privacidade dos dados nas instituições” (P1.V3.1 – P2HES#02)	

	"[...] nestas questões da informática cada vez mais é necessário um conhecimento especializado e não generalizado" (P1.V3.1 – P2HES#02)	
	"É importante haver um profissional, ou mais do que um, para a proteção de dados. [...] Alguém que depois consiga fazer a ponte com a área tecnológica" (P1.V3.1 – P2HES#03)	
	"É necessário profissionais especializados em privacidade" (P1.V3.1 – P3HES#05)	
	"Há três anos atrás já se justificava a presença de profissionais especializados em proteção de dados nas instituições. Isto antes de implementar sistemas de partilha de dados" (P1.V3.1 – P4HES#06)	

P1.V4.1	*Exemplos*	*Contributo para uma preparação global*
Padrão *Formação específica* *Colóquios e congressos* *Internet e Portal do Utente* *Ações de sensibilização* *Disponibilidade de informação* *Debate, partilha de conhecimentos/experiências*	"Sessões de sensibilização, casos de estudo, projetos de investigação que permitam refletir sobre a privacidade" (P1.V4.1 – P1ULSNA#01)	"[...] meios informais que permitam a partilha de conhecimento e experiências podem contribuir muito positivamente" (P1.V4.1 – P1ULSNA#01)
	"Eventos internos não públicos [...] Criar grupos de trabalho" (P1.V4.1 – P2ULSNA#02)	"[...] mostrar a determinados grupos as facilidades e riscos de acesso a determinadas informações sobre os utentes. [...] mostrar como devemos utilizar a informação que guardamos" (P1.V4.1 – P2ULSNA#02)
	"Colóquios ou congressos [...].Formação contínua para todos os profissionais" (P1.V4.1 – P2ULSNA#03)	"[...] que permitam a troca de experiências. É necessário sensibilizar as instituições" (P1.V4.1 – P2ULSNA#03)
	"Todo o tipo de eventos não só de natureza formativa [...]. Sejam seminários formativos de natureza obrigatória ou não, promover reuniões conjuntas entre organizações, aferir o nível de desenvolvimento de uma organização e fazer a aprendizagem com outras organizações" (P1.V4.1 – P4ULSNA#06)	"[...] há génese a incutir nas pessoas e de adesão livre as organizações devem traçar objetivos para a participação obrigatória das pessoas" (P1.V4.1 – P4ULSNA#06)
	"Essencialmente através de ações de formação" (P1.V4.1 – P1USF#01)	"[...] que permitam debater este tipo de segurança" (P1.V4.1 – P1USF#01)
	"[...] promovidos alguns Workshops uteis. Algo que vá além das deliberações da CNPD" (P1.V4.1 – P2USF#02)	"Esta questão tem que ser vista como um todo. [...] com uma maior cultura em privacidade, o resultado vai surgir" (P1.V4.1 – P3USF#04)
	"Seria importante em futuros congressos incluir esta questão. De uma forma informal, mais pratica, através de manuais das aplicações, através da internet" (P1.V4.1 – P3USF#03)	"Junto dos utentes é importante desenvolver estes conceitos – fazer-lhes chegar essa informação a casa" (P1.V4.1 – P3USF#06)
	"Formações acima de tudo. Acima de tudo as pessoas têm que estar informadas. Desde que a informação chegue canais informais também podem ajudar, como a internet, email, distribuição de cartazes, portal do utente e do profissional" (P1.V4.1 – P3USF#04)	"[...] que permita discutir com as pessoas e técnicos como é que se pode melhorar, identificar as dificuldades, de modo a haver uma interação entre todos. As próprias estruturas organizativas têm que ser mais ágeis nesta matéria e é necessário que tenham consciência dos problemas existentes" (P1.V4.1 – P4USF#05)
	"Os eventos dos embaixadores da PDS são um exemplo importante" (P1.V4.1 – P3USF#06)	
	"Reuniões e formação [...]" (P1.V4.1 – P4USF#05)	
	"Desenvolver eventos focados no perfil profissional" (P1.V4.1 – P1INEM#01)	"Não impor soluções, é necessário envolver as pessoas, sensibilizá-las para a proteção de dados" (P1.V4.1 – P1INEM#01)
	"[...] fazer algum tipo de ação de formação, de workshop. Mesmo meios informais, por divulgação, fazer chegar informação às pessoas" (P1.V4.1 – P2INEM#03)	"[...] que consiga dar a entender melhor esta problemática" (P1.V4.1 – P2INEM#03)
	"Formação, qualquer que seja o modelo" (P1.V4.1 – P2INEM#04)	"A presença de profissionais especializados nas organizações seria fundamental, para que estas questões fossem abordadas com maior responsabilidade" (P1.V4.1 – P2INEM#04)
	"[...] iniciativas como ações de formação, ações de sensibilização. Até mesmo o desenvolvimento de folhetos informativos, que divulguem esta informação" (P1.V4.1 – P2INEM#09)	"A coisa tem que ser tratada para que não sature as pessoas" (P1.V4.1 – P2INEM#09)
	"[...] através dos meios de comunicação social. Através de profissionais dedicados" (P1.V4.1 – P2INEM#10)	"[...] sensibiliza-los para o facto de lidarem com informação sensível, e que não devem facilitar" (P1.V4.1 – P2INEM#10)
	"[...] adequar formação específica às pessoas responsáveis pelo desenvolvimento das tecnologias" (P1.V4.1 – P3INEM#05)	"[...] sensibilização das pessoas mas focalizada" (P1.V4.1 – P3INEM#05)
	"Formação específica e devidamente orientada" (P1.V4.1 – P3INEM#06)	"[...] sensibilização sobre estes aspetos" (P1.V4.1 – P3INEM#06)
	"Formação e divulgação de quais são os deveres e direitos dos profissionais de saúde" (P1.V4.1 – P3INEM#07)	"[...] permita uma preparação global nestas matérias" (P1.V4.1 – P4INEM#08)
	"Seminários, formação específica, são tudo ações que têm que decorrer, é necessário segmentar as pessoas, os organismos, o tipo de dados, o tipo de utilizador, para direcionar a cada um plano de comunicação" (P1.V4.1 – P4INEM#08)	"Preparar um grupo para criação de certificação para os sistemas de informação" (P1.V4.1 – P2HFF#02)
		[...] alertar para estas questões, informar como se deve proceder em

	"Promover encontros com especialistas não académicos, com experiência" (P1.V4.1 – P1HFF#01)	situações de utilização de dados (P1.V4.1 – P2HFF#02)
	"[...] eventos sobre segurança e privacidade" (P1.V4.1 – P2HFF#02)	"Poder sensibilizar através da mais-valia, ou porque houve problemas e os profissionais foram sancionados, ou porque existem casos práticos de problemas" (P1.V4.1 – P2HFF#03)
	"[...] apostar em *IT Governance"* (P1.V4.1 – P2HFF#02)	"Cria-se uma onda de debate, partilha de ideias, e de boas práticas" (P1.V4.1 – P3HFF#04)
	"[...] ações de formação para responsáveis de sistemas de informação, mesmo até informalmente cartazes, emails" (P1.V4.1 – P2HFF#02)	"Temos um conjunto alargado de instituições públicas e privadas que devem ter acesso ao mesmo nível de informação" (P1.V4.1 – P4HFF#05)
	"[...] alguns casos práticos, quer a nível nacional como internacional" (P1.V4.1 – P2HFF#03)	"[...] quando estas pessoas se consciencializarem que a questão a privacidade é crítica, se vai criar esta preparação global" (P1.V4.1 – P1SPMS#02)
	"[...] nos programas académicos. [...] a formação dos cidadãos nesta área em concreto. Na comunicação audiovisual [...]" (P1.V4.1 – P3HFF#04)	"[...] no sentido de preparar as pessoas para a implementação de um conjunto mínimo de princípios" (P1.V4.1 – P2SPMS#03)
	"[...] existir um normativo de base" (P1.V4.1 – P4HFF#05)	"Implica que se olhe para os dados, para o cidadão e se façam transformações ao nível dos sistemas de informação, uma vez que não foram concebidos desde o seu início para terem controlos de privacidade" (P1.V4.1 – P2SPMS#03)
	"Promover reuniões com os responsáveis de várias instituições. Organizar congressos e abordar a questão da privacidade, até para os profissionais de saúde" (P1.V4.1 – P1SPMS#02)	"Permitem ver os problemas de acordo com a opinião especializada dos vários perfis profissionais" (P1.V4.1 – P1HES#01)
	"Fazer workshops muito direcionados, para aquilo que são as nossas áreas. Promover formação [...]" (P1.V4.1 – P2SPMS#03)	"A informação e a formação são importantes a este nível. [...] É necessário poder falar-se sobre a segurança informática, e a experiência em cada instituição, para conhecermos cada instituição, porque a nossa realidade é diferente mas semelhante a outras" (P1.V4.1 – P2HES#03)
	"[...] promover a partilha do conhecimento sobre estas matérias, sobre os processos que se vão aplicando e dos mecanismos que se vão utilizando" (P1.V4.1 – P2SPMS#03)	"Esta não pode ser uma coisa individual, tem que ser uma coisa institucional" (P1.V4.1 – P3HES#05)
	"Eventos ou workshops temáticos, onde possam ser apresentados os projetos, experiências, problemas existentes. Promover ações de formação neste domínio" (P1.V4.1 – P2SPMS#04)	
	"Deve ser promovido um debate, conferência, que façam as pessoas pensar sobre estas questões" (P1.V4.1 – P1HES#01)	
	"Posteriormente promover ações de formação especializadas. Promover encontros entre responsáveis pelos sistemas de informação, à semelhança do que aconteceu com a implementação da PDS. Sessões de trabalho em grupo, em que são analisadas uma série de assuntos" (P1.V4.1 – P1HES#01)	
	"Formação sobre legislação de proteção e dados. [...] Eventos que permitam consciencializar as pessoas da importância para a privacidade dos dados e da partilha destes mesmos dados" (P1.V4.1 – P2HES#02)	
	"Eventos para partilhar experiências. Eventos com o apoio de empresas de novas tecnologias, para podermos conhecer qual a evolução a desenhar" (P1.V4.1 – P2HES#03)	
	"A investigação é também importante, porque acaba por se traduzir em melhorias na organização" (P1.V4.1 – P2HES#03)	
	"Esta temática deve fazer parte da formação dos jovens médicos e enfermeiros. Depois deveria ser obrigatório, alguma formação anual sobre isto" (P1.V4.1 – P3HES#05)	
	"[...] mais formação em proteção de dados para todos os profissionais. É necessário contar com a necessidade de atualização de normas, legislação" (P1.V4.1 – P4HES#06)	

3. Data Display

P1	**Matriz de análise da opinião sobre P1. Experiência**		
Variáveis dependentes	*Padrão encontrado*	*Compreensão individual e coletiva* (*Qual a influência/relação sobre a preparação individual e coletiva para o desenvolvimento conjunto de medidas de proteção - colaboração*)	*Planeamento e suporte* (*Requisitos fundamentais ao planeamento e ao suporte de uma maior preparação coletiva ou da organização*)
P1.v1. É fundamental uma experiência em partilha de dados, em interoperabilidade, em projetos internos do próprio sistema de informação e em projetos de colaboração com outras organizações.	Conhecimento dependente da experiência Experiência é fundamental ao sucesso da partilha de dados e na redução do risco Tendência para uma maior atenção para com a proteção de dados A interoperabilidade é um desafio recente.	Existe uma dependência direta entre a experiência em projetos de partilha de dados e a proteção destes dados. A interoperabilidade está a mover a atenção e a preocupação das pessoas para a proteção de dados. Melhor conhecimento sobre a informação. Numa fase inicial as pessoas são muito céticas [...], mas depois começam a aperceber-se dos benefícios. Necessária experiência em gestão da informação, que saiba com que tipo de informação se trata e a sua criticidade. A PDS está a contribuir para uma mudança de atitude, e é o contexto propício para o desenvolvimento destas questões.	Necessária uma maior disponibilidade por parte dos profissionais para iniciativas de partilha de dados. Partilha de experiências como forma de diminuir o risco para a privacidade dos dados. Experiência em projetos de partilha de dados essencial ao desenvolvimento de políticas conjuntas de proteção de dados. A experiência diminui o risco de haver problemas de privacidade [...] maior a probabilidade de sermos proativos e não reativos.
P1.v2. Experiência em questões de privacidade, em proteção de dados, no seu enquadramento legislativo (nacional e internacional), em avaliações do impacto sobre a privacidade (PIA), ao nível dos sistemas locais permitem uma colaboração mais produtiva com outras organizações no desenvolvimento de um ambiente seguro de partilha de dados.	Segurança e proteção de dados Conhecimento dos dados O conhecimento da legislação é fundamental	É importante e exigível que no futuro os responsáveis pelos SI ou outro tipo de técnicos venham a ganhar experiência em matéria de proteção de dados. Compreensão de forma clara dos conceitos e dos princípios de proteção de dados, assim como a sua necessidade. Classificar e conhecer a criticidade dos dados. Capacidade de transposição da legislação para os SI. Fundamental ao conhecimento do nível de exigência a desenvolver quanto à segurança e proteção dos dados.	Os responsáveis pelos SI devem ser os indutores da mudança e dinamizadores da colaboração. É necessária uma cultura de segurança orientada para os dados. Constituição do *privacy information officer*. Deveríamos apostar em profissionais especializados. Fomentar a prática do conhecimento especializado da legislação de uma forma permanente.
P1.v3. É essencial a existência de profissionais especializados em proteção e privacidade, a cooperação entre estes, e de um órgão de supervisão para o contexto da colaboração, para garantir que as políticas de privacidade são atendidas por todos.	Recursos humanos dedicados Especialistas focados nos dados Responsabilidade de vários decisores Equipa pluridisciplinar Equipa permanente.	Facilita a colaboração com outras organizações. Suporte à realização de análises de impacto sobre a privacidade. Suporte à evolução e à implementação. São necessários profissionais com maturidade suficiente para dialogar com todos os profissionais. Transporta para a prática os requisitos da legislação.	Justifica-se a existência a nível local de profissionais especializados e dedicados às questões da privacidade dos dados. Para o contexto de colaboração justifica-se a criação de uma equipa permanente, para uniformizar medidas transversais e harmonizar soluções, com possível evolução para a certificação dos sistemas.
P1.v4. Eventos como programas periódicos de educação, formação e sensibilização entre os profissionais da organização, participação em workshops, seminários nacionais ou internacionais, no domínio da privacidade e proteção de dados, são importantes para uma melhor experiência e preparação coletiva.	Formação específica Colóquios e congressos Ações de sensibilização Disponibilidade de informação Debate, partilha de conhecimentos/experiências	Envolver as pessoas, sensibilizá-las para a privacidade de dados. Informar e alertar as pessoas. Partilha de conhecimento e experiências. Uniformizar a informação sobre privacidade em todas as organizações.	Promover o debate sobre privacidade dos dados. Promover ações de formação, colóquios, congressos. Utilizar a Internet e o portal do utente e do profissional para difundir informação. Depende de um grupo de trabalho dedicado.