# Análise dos dados – P7. Estratégia para a privacidade

## 1. Dados das entrevistas

Variável dependente – Participante

### P7.V1.1

| | |
|---|---|
| P7.V1.1 – P4ULSNA#06 | Acima de tudo nós temos que desenvolver uma estratégia comum. Devemos começar por esta estratégica comum. Sei que é muito complicado, mas em parte já está a ser feito. A SPMS tem liderado o processo de desenvolvimento para os sistemas de informação que tem trazido alguma sistematização a este sector, que não existia. O que acontecia anteriormente, era que o suporte do IGIF/ACSS limitava-se apenas ao papel de interlocutor de soluções para os sistemas de informação para as instituições de saúde, hospitais ou unidades locais de saúde. Não existia uma estratégia global para o desenvolvimento dos sistemas de informação. Durante muito tempo cada instituição foi acreditando na estratégia comercial dos vários fornecedores, dando origem a uma proliferação de soluções.<br>A SPMS inverteu esta situação, intervindo no desenvolvimento dos sistemas de informação.<br>Agora os dados ao serem reconhecidos como um valor para a instituição vai facilitar uma estratégia para a sua proteção, não podem ser apenas matéria-prima. |
| P7.V1.1 – P4USF#05 | A privacidade é um valor para a organização que tem que ser planeado. Tem que haver instrumentos ao nível da gestão da privacidade (…) |
| P7.V1.1 – P4INEM#08 | A implementação de uma política de sistemas de informação, e de gestão da qualidade. Se eu tiver um sistema da qualidade que vise, que tenha por objetivo, que o *core business*, que a atividade principal esteja certificada, todos os mecanismos, todos os processos, de acreditação e certificação, de áreas que tenham a ver com a gestão do risco, e a segurança vão bater neste ponto [a proteção dos dados]. Hoje não é aceitável que eu tenha um conjunto de equipamentos, e que não tenha uma determinada garantia, o mesmo se passa com os dados. |
| P7.V1.1 – P4HFF#05 | Antes de mais a privacidade, antes de qualquer âmbito de gestão é uma ofensa em casos de uma organização que tem dados muito, mas muito sensíveis, e ponde passam milhares de pessoas diariamente. Todos os individuo têm o direito à sua privacidade. Não se põe em causa a privacidade dos dados dos utentes. Isto é um princípio, um valor. A questão de ser importante ou não, não se põe, porque existe, faz parte da função do hospital, garantir a privacidade dos dados, estejam eles onde estiverem. |
| P7.V1.1 – P4SPMS#05 | A privacidade seja mais relevada? São os processos em tribunal. Se é um valor não se deve “estragar”, desvalorizar, nem corromper. Por isso é que as pessoas recorrem ao tribunal – porque se estragam os valores. |
| P7.V1.1 – P4HES#06 | A privacidade tem que ser vista como um valor organizacional. É um valor importantíssimo e tem que ser pensado de uma forma estratégica. |

### P7.V1.2

| | |
|---|---|
| P7.V1.2 – P4ULSNA#06 | É importante este reconhecimento. Vou ser muito claro. Sou muito cauteloso no que toca ao investimento em sistemas de informação. |

| | |
|---|---|
| | E esta desconfiança surge pelo conhecimento da história das organizações no que toca aos sistemas de informação. Mas também sou aberto, e incentivo que se possa caminhar e evoluir para conseguirmos melhores ferramentas de resposta à prestação de cuidados. Atualmente a geração que está a sair das faculdades, é uma geração da era tecnológica e logo mais bem preparada nestas questões, são ferramentas auxiliares muito importantes.<br>Já estive ligado à implementação de vários sistemas, nomeadamente imagiologia, e as questões da privacidade foram muito escalpelizadas, sendo que em algumas situações poderia ir-se mais longe. Em algumas situações existe uma preocupação com a proteção de dados, nomeadamente com a anonimização de determinados dados. A nível médico, que é quem lida com estes dados, e no exemplo um utente que seja internado, quem tem acesso aos exames, fá-lo de acordo com níveis de acesso à informação, o que não acontecia com o processo clínico em suporte papel. Ao estar junto ao doente, qualquer pessoa podia consultar esta informação. Ou seja existem medidas de segurança implementadas para este objetivo.<br>Recentemente surgiu uma notícia sobre um sistema de informação que vai ser disponibilizado sobre os funcionários públicos, as pessoas que materializam a função do Estado, para obedecer ao princípio da transparência, em que a opinião CNPD sobre este sistema, é que este tinha ido longe demais, ao colocar informação à disposição das pessoas sobre processos disciplinares, notificações, baixas por doença. O resultado é a criação de um ambiente de desconfiança e desmotivação. |
| P7.V1.2 – P4USF#05 | Um individuo nesta posição tem que ter, obrigatoriamente, uma formação nesta área, que desenvolvam conhecimento nesta matéria. Só assim podem incrementar medidas. |
| P7.V1.2 – P4INEM#08 | A proteção de dados é uma das maiores responsabilidades ao nível da gestão. Os gestores têm responsabilidades nestas questões. Mas muitas vezes, não lhe dão o valor que merece. O nível de implicação legal e da responsabilidade é muito grande. Por exemplo aqui no INEM, todas as situações de fornecimento de dados para fora [ao exterior] e quem tem a ver com proteção de dados, são analisados juridicamente |
| P7.V1.2 – P4HFF#05 | Sim, ao nível do conselho de administração esta responsabilidade é reconhecida. Garantir a legislação. Não há discussão. |
| P7.V1.2 – P4SPMS#05 | Eu não sei se eles têm muita responsabilidade. Quem está a fazer prestação de cuidados é que tem muita responsabilidade. É aqui que está a primeira linha de defesa da segurança da informação e da privacidade dos dados. Não é no gestor da organização. Quando um médico utiliza a informação de um doente e a divulga a outro, e não o deveria ter feito, ele está a incumprir, não é necessário chegar ao diretor do hospital. A grande parede está nos profissionais de saúde e não o topo da organização. |
| P7.V1.2 – P4HES#06 | Em teoria seria muito interessante. Mas como na prática o que existe é legislação que temos que cumprir a margem de intervenção de cada organização é muito pequena. Existe uma intervenção da nossa parte no desenho de uma visão estratégica para os sistemas de informação. Esta peça que é a proteção de dados deveria ser encarada como mais uma peça [componente] do sistema de informação. Infelizmente a legislação não nos permite. |

## P7.V2.1

| | |
|---|---|
| P7.V2.1 – P4ULSNA#06 | Faz sentido a existência de uma estratégia de desenvolvimento da privacidade como um todo. |
| P7.V2.1 – P4USF#05 | É desejável uma colaboração, uma interação entre os responsáveis das organizações. Vamos desenvolver a privacidade, mas vamos desenvolver todos em conjunto, e não de uma forma isolada. E isto depende de medidas de nível superior. |
| P7.V2.1 – P4INEM#08 | |

| | |
|---|---|
| P7.V2.1 – P4HFF#05 | Através da tutela, que fornece essas orientações. Deve emanar orientações que permitam um desenvolvimento integrado. Deve fazer as auditorias aos sistemas, à sua segurança e também ao nível da privacidade. A segurança para garantir a privacidade e a segurança de dados. A CNPD emite orientações, pareceres, também importantes para o funcionamento da privacidade e proteção dos dados. Mas não monitoriza o funcionamento dos sistemas, depois de um parecer positivo sobre o objetivo da recolha de dados. |
| P7.V2.1 – P4SPMS#05 | Os gestores têm que gerir a evolução dos conhecimentos e das competências da sua *workforce* nestas matérias, como em muitas outras. Claro que neste sentido são eles os dinamizadores. Estas questões são na minha opinião das chefias intermédias e das chefias operacionais. Tem mais responsabilidade o chefe de equipa de uma urgência do que tem o diretor clínico. |
| P7.V2.1 – P4HES#06 | É importante pensarmos seriamente e estrategicamente nestas questões. À semelhança dos sistemas de informação. A linguagem médica, a linguagem dos profissionais de saúde foi evoluindo ao longo dos anos. Foi sendo criada de forma a ganhar progressivamente clareza e produtibilidade. Aprendemos na universidade, aquilo que foi a evolução da linguagem médica e isso foi feito ao longo de 100 anos. Até se chegar a um estado atual, muito avançado em termos de clareza de linguagem, de forma que um médico que lê um registo clinico de outro médico saiba o que é que aquilo quer dizer. Quando se passou para os sistemas informáticos não houve a preocupação de beber o resultado deste trabalho de uma centena de anos (esta experiência) e foram tomadas decisões completamente divorciadas da realidade. E o resultado não pode ser bom. Do ponto de vista estratégico não houve nenhuma estratégia, de tipificar informação, de priorizar informação, de perceber o que é informação importante e informação não importante.<br>Nós temos que no futuro caminhar no sentido de partilhar serviços e informação. Mas temos aqui um grande problema relacionado com a proteção de dados. [...] Em termos de agilidade a colocação da PDS no terreno foi excelente. A solução encontrada para a partilha de dados através da PDS foi a solução certa. Ou seja, vários países tentaram e fracassaram ao criar sistemas de registo eletrónico sistémico. A filosofia da PDS está certíssima. Agora não foi feita com as competências necessárias, e tem duas falhas enormes: a confidencialidade dos dados e a tipificação da informação, que trata os vários tipos de informação da mesma maneira.<br>Mesmo em relação ao consentimento, deveria ter sido parametrizado ao contrário – tudo bloqueado. E quando o utente vai ao médico desbloqueia a sua informação. Não é por uma questão de custos, do saber fazer – é uma questão de visão. Ter acesso a tudo neste momento é mais importante que a confidencialidade das pessoas. Uma coisa é eu ter acesso à informação de um doente meu, outra coisa é ter acesso à informação de um outro doente. |

## P7.V3.1

| | |
|---|---|
| P7.V3.1 – P4ULSNA#06 | Claro é essencial para minimizar os eventos adversos que possam surgir, porque estamos a falar de partilha de dados, em que coexistem uma multiplicidade de sistemas de informação. É vital para que depois se possam aplicar medidas de proteção. Contudo, existe uma previsão do risco ao nível da segurança, mas ao nível da proteção de dados ainda não existe. Tenho algumas dúvidas sobre a facilidade de desenvolver uma análise de risco para a informação. |
| P7.V3.1 – P4USF#05 | Faz parte da formação. Conhecer o risco e o que dai advém é importantíssimo. Conhecer os riscos, os malefícios que podem advir, como fugas de informação. |
| P7.V3.1 – P4INEM#08 | Sim, entendo a sua questão. O desconhecimento do risco pode fazer com que não se atue. Agora como é que um gestor, no exercício do seu trabalho diário, se confronte com frequência com as questão dos dados, sendo que tem responsabilidade de autorizar ou não o fornecimento de dados, lida com a fuga de dados, dizer que não conhece os riscos, ou que não está sensibilizado, até porque tem implicações legais, é porque está "distraído", não está a prestar a devida atenção a estas questões. Provavelmente não dispõe é de |

| | |
|---|---|
| | ferramentas que lhe permitam esta gestão.<br><br>Havendo por parte de um gabinete de gestão da qualidade uma análise do risco e que demonstre o risco que se está a correr, e se eu esbarrar num processo em que quero garantias de qualidade da minha atividade core, e se no processo de garantia da qualidade esbarro em algo que tem a ver com a proteção de dados e com a privacidade obviamente que eu vou intervir no sentido resolver o assunto, com base na análise risco feita. |
| P7.V3.1 – P4HFF#05 | O risco, todos nós sabemos, que decorre de não cumprir as orientações para a privacidade, seja ele legal, ético. Não deve ser uma organização por si, a desenvolver esta estratégia, eventualmente pode fazê-lo, mas eu acho que o âmbito deve partir da tutela, uma vez que estamos a falar de uma área tão sensível como é a saúde e os dados da saúde, serem efetivamente definidos orientações para iniciar este caminho.<br><br>Em tecnologia o risco é exponencial, com a sua utilização. Os riscos a este nível estão identificados. Não estão é solucionados. Mesmo definindo políticas de proteção nada nos assegura que amanha não surge uma alternativa de acesso à informação. é um ciclo de desenvolvimento. Contudo a tecnologia ultrapassa facilmente qualquer normativo que seja publicado. |
| P7.V3.1 – P4SPMS#05 | O risco da utilização ou o risco da não utilização? Existe um risco imenso, que é o risco da não utilização dos dados. E este risco é imenso e não é medido. Tal como o risco de se demorar meia hora a enviar um email devido à segurança, pelo que não consigo trabalhar em tempo útil. Também é um risco. Normalmente os diretores dos sistemas de informação, e estas análises de risco, têm um erro gravíssimo – assumem que a aplicação das regras de segurança e privacidade não têm impacto na eficiência, mas têm um enorme impacto na eficiência. E esse impacto tem um risco. Ou seja, eu, ao não conseguir, por exemplo como enfermeiro, aceder a um conjunto de informações dentro de um processo clínico, porque alguém achou que no âmbito do risco eu não deveria ter acesso aos registos, posso medicar mal um doente. Este risco também tem que ser medido. Os instrumentos de que está a falar estão desenhados, todos, com um princípio, que quanto a mim está errado – que é o princípio de que a adição de níveis de controlo de risco não tem impacto na performance do sistema em causa, mas eu acho que tem muito impacto. No caso da saúde o impacto é muito grande. Pode até ser maior o impacto da devassa da informação, posso acreditar que possa ser. Mas o impacto da ausência de partilha de dados, ausência de acesso, não está estudado, porque nunca houve esse acesso [devido à PDS]. O risco aqui não é um risco. É aquilo que chamo um delta, isto é, é o resultado de dois riscos: o risco da proteção e o risco do inverso. Quando se fala em proteção está sempre a referir-se a não se partilhar, não se mostrar, não se expor, mas eu posso sempre referir-me ao inverso, a proteção dos meus dados é eles estarem disponíveis quando são mesmo precisos para me salvar a vida, e isto também é proteger os meus dados. |
| P7.V3.1 – P4HES#06 | Numa situação de falência técnica do sistema de informação, era um caos completo dentro desta instituição. Os processos em registo papel são residuais.<br><br>Quando implementamos o SONHO (aplicação administrativa) no hospital. Quando foi implementado negociamos com a ACSS e com o ministério que o detentor dos dados era o hospital e que instituições externas não entravam nos nossos dados. Foi essa a condição para instalemos o SONHO. Depois a legislação mudou e neste momento entram no nosso sistema e nós nem sabemos que eles cá entraram. Quisemos instalar uma aplicação eletrónica para prescrição e obrigaram-nos a instalar uma aplicação de prescrição nacional. Sabemos que estes dados são recolhidos e vendidos. Ou seja, a legislação é que nos impõe estes riscos. Temos lutado contra isto.<br><br>É precisamente o conhecimento destes riscos que muda a atitude e preocupação existente a nível coletivo. Um hospital deveria ser autónomo neste aspeto. Se querem os nossos dados pedem-nos. Agora as nossas aplicações estão abertas.<br><br>Quando falamos de privacidade dos dados este é o centro da questão - a abertura imposta das nossas aplicações ao acesso externo. É necessário definir o que é preciso partilhar. Identificamos o que é preciso partilhar, partilhamos o que é necessário partilhar, |

| | |
|---|---|
| | estabelecemos os mecanismos de controlo, e acabou. Agora esta coisa do partilhamos tudo não faz sentido. Há coisas que eu até acho que temos o direito de não partilhar – enquanto profissional. Podemos não querer partilhar um diagnóstico, que é uma atitude criativa, um trabalho intelectual do profissional de saúde, no suporte à decisão. Eu tenho direito a querer que este meu trabalho não seja copiado por outros. Isto leva a que as pessoas não façam relatórios, raciocínios clínicos. Pois os raciocínios clínicos, certos ou errados, são da minha responsabilidade.<br>Aqui falamos de três tipos de dados: dados clínicos, pessoais, e a atividade intelectual do médico, do profissional. Ninguém tem o direito de copiar a minha atividade intelectual. |

## P7.V4.1

| | |
|---|---|
| P7.V4.1 – P4ULSNA#06 | Eu vejo uma primeiro que a outra. Vejo a estratégia primeiro, e depois como consequência desta a cultura. Havendo uma estratégia de topo para a privacidade, facilita o desenvolvimento de uma cultura de privacidade. |
| P7.V4.1 – P4USF#05 | Uma estratégia de privacidade pode desenvolve uma cultura de privacidade e uma cultura de privacidade também pode influenciar a estratégia. Estão intimamente ligados. |
| P7.V4.1 – P4INEM#08 | Quando falamos de cultura estamos a falar de um conhecimento maior sobre este assunto. Não adianta estar a criar uma cultura sem saber o caminho. Existe já uma cultura. Não existe é uma estratégia concertada, que tenha como objetivo criar uma plataforma comum, uma abordagem comum. E acho que deve ser definida no âmbito da administração pública, esta estratégia, para conseguirmos um maior conhecimento, para caminharmos num determinado sentido. Deve existir um plano de desenvolvimento, com um conjunto de ações que implementem uma estratégia. |
| P7.V4.1 – P4HFF#05 | A estratégia influencia a cultura. A cultura não aparece se não existir uma estratégia bem definida. |
| P7.V4.1 – P4SPMS#05 | Primeiro têm que existir internamente alguém que se preocupe com este assunto. Depois é necessário que estes partilhem as suas dificuldades. Daí depois decorre partilharem ideias e formação. |
| P7.V4.1 – P4HES#06 | Isto é um assunto estratégico de futuro. O acesso à informação é um assunto fundamental e também formas expeditas de gerir informação também são fundamentais. Para a eficiência e para o desempenho dos profissionais de saúde é necessário ter uma aplicação que lhe dá o que ele precisa num minuto. Atingimos um estado de maturidade tal, que faz com que tenhamos um desempenho com o registo clinico eletrónico semelhante ao que tínhamos em papel. O que já é uma vitória fantástica. Com os ganhos adicionais de fiabilidade, legibilidade da informação, de podermos ter confidencialidade. Mas estamos com riscos muito elevados, temos que os identificar.<br>*Tivemos uma empresa farmacêutica que nos apresentou uma aplicação para controlo da medicação dos doentes. Um dos problemas que existe nos doentes oncológicos é que os medicamentos são agressivos, e muitas vezes os doentes não fazem a medicação. A aplicação ajudava os doentes a cumprirem a medicação. Para o projeto precisavam de instalar no hospital um posto de trabalho e um funcionário em que ficavam com acesso à informação dos doentes. Este funcionário o que fazia era ligar para o doente a confirmar a medicação, agendar consultas, etc. Fizeram isto em vários hospitais. Aqui não deixamos porque não faz sentido, deixar a indústria farmacêutica instalar um posto de trabalho de recolha de dados dos nossos doentes oncológicos e da medicação que fazem, alimentado pelo nosso sistema de informação.* |

## P7.V5.1

| | |
|---|---|
| P7.V5.1 – P4ULSNA#06 | A área da saúde é uma área de excelência. Seria desejável e importantíssimo construir uma estratégia conjunta para as questões da privacidade. Contudo, naquilo que é e minha experiência, tudo que seja partilha, gera sempre desconfiança entre as organizações. Esta confiança tem que ser gerida. Estamos sempre muito cientes da nossa "quinta", o que significa que isto só se consegue com o apoio ou patrocínio de uma entidade como o ministério da saúde, ou da própria administração regional. |
| P7.V5.1 – P4USF#05 | É necessário uma colaboração ao nível da gestão para se desenvolverem estas questões de uma forma transversal. A falta de conhecimento, de formação nestas questões pode impedir o desenvolvimento da colaboração. Caso contrário estas questões podem passar ao "lado". |
| P7.V5.1 – P4INEM#08 | Existem aqui aspetos que têm a ver com a informação que é transversal às organizações, que têm a ver com a gestão do cidadão perante a administração pública. Estou-me a referir à área daquilo que é gestão e a responsabilidade dos organismos públicos na gestão da informação do cidadão. Que tem implicações a vários níveis, o que leva a que tenha que haver um contributo do ponto de vista de implicações jurídicas, dar suporte, autorização. Obviamente do ponto de vista dos instrumentos legislativos tem que haver um ajuste que decorra do funcionamento, em que cada vez que se introduz um novo suporte ele já deve ter requisitos de utilização da informação que respondam à luz daquilo que seria útil para os utilizadores, cumprir com certos requisitos. Tem que se fazer uma adaptação daquilo que são os direitos, as obrigações, transpô-los para um conjunto de requisitos do ponto de vista de gestão dos sistemas de informação, e de segurança, que possam ser obrigatoriamente incorporados cada vez que nós desenvolvemos um novo sistema de informação ou estamos a trabalhar a informação de uma instituição. Que esses requisitos sejam conhecidos para quem fornece os sistemas de informação os cumpra e esteja certificado nesse âmbito.<br><br>Teria que haver aqui uma partilha de experiências, de definição de diretrizes comuns entre todas as organizações. Andamos todos demasiado concentrados em querer inventar o nosso sistema, com segurança própria. Estas questões não são complexas e não são diferentes de outras situações. A informação em saúde é tão importante e confidencial como a informação sobre a minha ida de metro de um local para o outro. Ou a minha fatura num restaurante. Qualquer uma destas situações pode criar-me um transtorno muito grande na minha vida pessoal, tal como saberem a minha situação de saúde.<br><br>Todas as instituições da administração pública devem partilhar da mesma estratégia comum para este problema. |
| P7.V5.1 – P4HFF#05 | O alinhamento de todas as estratégias em termos organizacionais, depende da tutela do ministério da saúde. Se nós estamos a passar dados para o exterior, apesar de os dados continuarem no hospital, tem de ser a tutela a definir esta estratégia. Deve contudo haver uma maior disponibilidade das organizações para colaborar com outras organizações na definição destas questões. São questões muito importantes, muito atuais, mas ou existem diretrizes que permitam desencadear estas questões localmente ou então nunca vamos chegar a lado nenhum. As pessoas estão sensíveis para estas questões da privacidade, pretendem desenvolvê-las, mas apercebem-se que sozinhos não conseguem. Têm de ter por base uma estratégia global. |
| P7.V5.1 – P4SPMS#05 | |
| P7.V5.1 – P4HES#06 | O futuro passa pelas soluções de interoperabilidade. Este deveria ser o papel principal do ministério. O ministério deveria estar a regular em vez de pensar que é uma *software house*. A falta de recursos leva a que se façam soluções limitadas. E quando falamos em interoperabilidade verificamos que o SONHO não comunica com nada. Nunca vai comunicar. [basicamente o SONHO tem um módulo de identificação do doente, um módulo de consulta, um módulo de internamento e um módulo de bloco operatório]. O ALERT cobre o hospital todo. |

| | |
|---|---|
| | NOSOLOGIA – terminologia que permite que qualquer diagnóstico médico seja entendido globalmente (parte da medicina que trata da classificação das diferentes patologias). Em Portugal utilizam a norma CID9 (Classificação Internacional de Doenças) - tem códigos para diagnósticos e códigos para procedimentos.<br>O output de um diagnóstico é um conjunto de códigos de diagnósticos e de códigos de procedimentos. [...] Contudo no SONHO esta informação tem que ser registada nos vários módulos, pois estes não comunicam entre si sob a forma de interoperabilidade. Um episódio de internamento obriga ao registo da mesma informação em três módulos do SONHO. Na atualidade não faz sentido uma situação destas. |

## 2. *Data Reduction*

| **P7.V1** | **P7.V1.1**<br>Fator determinante ao desenvolvimento de uma estratégia para a privacidade dos dados. | **P7.V1.2**<br>É da responsabilidade dos gestores executivos a iniciativa no desenvolvimento de uma estratégia de suporte à privacidade dos dados. |
|---|---|---|
| *Padrão encontrado*<br><br>Valor organizacional<br>Responsabilidade | "Acima de tudo nós temos que desenvolver uma estratégia comum. Devemos começar por esta estratégica comum." (P7.V1.1 – P4ULSNA#06) | "É importante este reconhecimento." (P7.V1.2 – P4ULSNA#06) |
| | "Agora os dados ao serem reconhecidos como um valor para a instituição vai facilitar uma estratégia para a sua proteção, não podem ser apenas matéria-prima." (P7.V1.1 – P4ULSNA#06) | "Já estive ligado à implementação de vários sistemas, [...], e as questões da privacidade foram muito escalpelizadas, sendo que em algumas situações poderia ir-se mais longe. Em algumas situações existe uma preocupação com a proteção de dados, nomeadamente com a anonimização de determinados dados." (P7.V1.2 – P4ULSNA#06) |
| | "A privacidade é um valor para a organização que tem que ser planeado. Tem que haver instrumentos ao nível da gestão da privacidade [...]" (P7.V1.1 – P4USF#05) | "Um individuo nesta posição tem que ter, obrigatoriamente, uma formação nesta área, que desenvolvam conhecimento nesta matéria. Só assim podem incrementar medidas." (P7.V1.2 – P4USF#05) |
| | "A implementação de uma política de sistemas de informação, e de gestão da qualidade. [...] Hoje não é aceitável que eu tenha um conjunto de equipamentos, e que não tenha uma determinada garantia, o mesmo se passa com os dados." (P7.V1.1 – P4INEM#08) | "A proteção de dados é uma das maiores responsabilidades ao nível da gestão. Os gestores têm responsabilidades nestas questões. Mas muitas vezes, não lhe dão o valor que merece. O nível de implicação legal e da responsabilidade é muito grande." (P7.V1.2 – P4INEM#08) |
| | "Não se põe em causa a privacidade dos dados dos utentes. Isto é um princípio, um valor. A questão de ser importante ou não, não se põe, porque existe, faz parte da função do hospital, garantir a privacidade dos dados, estejam eles onde estiverem." (P7.V1.1 – P4HFF#05) | "[...] todas as situações de fornecimento de dados para fora [ao exterior] e quem tem a ver com proteção de dados, são analisados juridicamente" (P7.V1.2 – P4INEM#08) |
| | "Se é um valor não se deve "estragar", desvalorizar, nem corromper. Por isso é que as pessoas recorrem ao tribunal – porque se estragam os valores." (P7.V1.1 – P4SPMS#05) | "Sim, ao nível do conselho de administração esta responsabilidade é reconhecida. Garantir a legislação. Não há discussão." (P7.V1.2 – P4HFF#05) |
| | "A privacidade tem que ser vista como um valor organizacional. É um valor importantíssimo e tem que ser pensado de uma forma estratégica." (P7.V1.1 – P4HES#06) | "Eu não sei se eles têm muita responsabilidade. Quem está a fazer prestação de cuidados é que tem muita responsabilidade. É aqui que está a primeira linha de defesa da segurança da informação e da privacidade dos dados. Não é no gestor da organização." (P7.V1.2 – P4SPMS#05) |
| | | "Existe uma intervenção da nossa parte no desenho de uma visão estratégica para os sistemas de informação. Esta peça que é a proteção de dados deveria ser encarada como mais uma peça [componente] do sistema de informação. Infelizmente a legislação não nos permite." (P7.V1.2 – P4HES#06) |

| **P7.V2.1** | **Planeamento estratégico é uma ferramenta necessária**<br>O planeamento e integração de todas as iniciativas dirigidas à privacidade dos dados devem acontecer com base numa estratégia? |
|---|---|
| *Padrão encontrado*<br><br>Importante<br>Colaboração | "Faz sentido a existência de uma estratégia de desenvolvimento da privacidade como um todo." (P7.V2.1 – P4ULSNA#06) |
| | "É desejável uma colaboração, uma interação entre os responsáveis das organizações. Vamos desenvolver a privacidade, mas vamos desenvolver todos em conjunto, e não de uma forma isolada. E isto depende de medidas de nível superior." (P7.V2.1 – P4USF#05) |
| | "Através da tutela, que fornece essas orientações. Deve emanar orientações que permitam um desenvolvimento integrado. Deve fazer as auditorias aos sistemas, à sua segurança e também ao nível da privacidade." (P7.V2.1 – P4HFF#05) |
| | "Os gestores têm que gerir a evolução dos conhecimentos e das competências da sua *workforce* nestas matérias, como em muitas outras. Claro que neste sentido são eles os dinamizadores. Estas questões são na minha opinião das chefias intermédias e das chefias operacionais. Tem mais responsabilidade o chefe de equipa de uma urgência do que tem o diretor clínico." (P7.V2.1 – P4HES#06) |
| | "É importante pensarmos seriamente e estrategicamente nestas questões. À semelhança dos sistemas de informação." (P7.V2.1 – P4HES#06) |
| | "Quando se passou para os sistemas informáticos não houve a preocupação de beber o resultado deste trabalho de uma centena de anos (esta experiência) e foram tomadas decisões completamente divorciadas da realidade. E o resultado não pode ser bom. Do ponto de vista estratégico não houve nenhuma estratégia, de tipificar informação, de priorizar informação, de perceber o que é informação importante e informação não importante." (P7.V2.1 – P4HES#06) |
| | "Nós temos que no futuro caminhar no sentido de partilhar serviços e informação. Mas temos aqui um grande problema relacionado com a proteção de dados. [...] Em termos de agilidade a colocação da PDS no terreno foi excelente. A solução encontrada para a partilha de dados através da PDS foi a solução certa." (P7.V2.1 – P4HES#06) |

| P7.V3.1 | **Visão estratégia dependente do conhecimento do risco**<br>O conhecimento dos risco associados à utilização dos dados pode influência o desenvolvimento de uma visão estratégica? |
|---|---|
| *Padrão encontrado* | "Claro é essencial para minimizar os eventos adversos que possam surgir, porque estamos a falar de partilha de dados, em que coexistem uma multiplicidade de sistemas de informação." (P7.V3.1 – P4ULSNA#06) |
| | "É vital para que depois se possam aplicar medidas de proteção." (P7.V3.1 – P4ULSNA#06) |
| | "Contudo, existe uma previsão do risco ao nível da segurança, mas ao nível da proteção de dados ainda não existe. Tenho algumas dúvidas sobre a facilidade de desenvolver uma análise de risco para a informação." (P7.V3.1 – P4ULSNA#06) |
| | "Faz parte da formação. Conhecer o risco e o que dai advém é importantíssimo. Conhecer os riscos, os malefícios que podem advir, como fugas de informação." (P7.V3.1 – P4USF#05) |
| | "O desconhecimento do risco pode fazer com que não se atue. Agora como é que um gestor, no exercício do seu trabalho diário, se confronte com frequência com as questão dos dados, sendo que tem responsabilidade de autorizar ou não o fornecimento de dados, lida com a fuga de dados, dizer que não conhece os riscos, ou que não está sensibilizado, até porque tem implicações legais, é porque está "distraído", não está a prestar a devida atenção a estas questões. Provavelmente não dispõe é de ferramentas que lhe permitam esta gestão." (P7.V3.1 – P4INEM#08) |
| | "Havendo por parte de um gabinete de gestão da qualidade uma análise do risco e que demonstre o risco que se está a correr, e se eu esbarrar num processo em que quero garantias de qualidade da minha atividade core, e se no processo de garantia da qualidade esbarro em algo que tem a ver com a proteção de dados e com a privacidade obviamente que eu vou intervir no sentido resolver o assunto, com base na análise risco feita." (P7.V3.1 – P4INEM#08) |
| | "Não deve ser uma organização por si, a desenvolver esta estratégia, eventualmente pode fazê-lo, mas eu acho que o âmbito deve partir da tutela, uma vez que estamos a falar de uma área tão sensível como é a saúde e os dados da saúde, serem efetivamente definidos orientações para iniciar este caminho." (P7.V3.1 – P4HFF#05) |
| | "Em tecnologia o risco é exponencial, com a sua utilização. Os riscos a este nível estão identificados. Não estão é solucionados. Mesmo definindo políticas de proteção nada nos assegura que amanha não surge uma alternativa de acesso à informação. é um ciclo de desenvolvimento. Contudo a tecnologia ultrapassa facilmente qualquer normativo que seja publicado." (P7.V3.1 – P4HFF#05) |
| | "Existe um risco imenso, que é o risco da não utilização dos dados. E este risco é imenso e não é medido. Tal como o risco de se demorar meia hora a enviar um email devido à segurança, pelo que não consigo trabalhar em tempo útil. Também é um risco." (P7.V3.1 – P4SPMS#05) |
| | "Normalmente os diretores dos sistemas de informação, e estas análises de risco, têm um erro gravíssimo – assumem que a aplicação das regras de segurança e privacidade não têm impacto na eficiência, mas têm um enorme impacto na eficiência. E esse impacto tem um risco. Ou seja, eu, ao não conseguir, por exemplo como enfermeiro, aceder a um conjunto de informações dentro de um processo clínico, porque alguém achou que no âmbito do risco eu não deveria ter acesso aos registos, posso medicar mal um doente. Este risco também tem que ser medido." (P7.V3.1 – P4SPMS#05) |
| | "Mas o impacto da ausência de partilha de dados, ausência de acesso, não está estudado, porque nunca houve esse acesso [devido à PDS]. O risco aqui não é um risco. É aquilo que chamo um delta, isto é, é o resultado de dois riscos: o risco da proteção e o risco do inverso. Quando se fala em proteção está sempre a referir-se a não se partilhar, não se mostrar, não se expor, mas eu posso sempre referir-me ao inverso, a proteção dos meus dados é eles estarem disponíveis quando são mesmo precisos para me salvar a vida, e isto também é proteger os meus dados." (P7.V3.1 – P4SPMS#05) |
| | "É precisamente o conhecimento destes riscos que muda a atitude e preocupação existente a nível coletivo." (P7.V3.1 – P4HES#06)<br>Atingimos um estado de maturidade tal, que faz com que tenhamos um desempenho com o registo clinico eletrónico semelhante ao que tínhamos em papel. O que já é uma vitória fantástica. Com os ganhos adicionais de fiabilidade, legibilidade da informação, de podermos ter confidencialidade. Mas estamos com riscos muito elevados, temos que os identificar." (P7.V4.1 – P4HES#06) |

| **P7.V4.1** | **Uma visão estratégia da privacidade influência um cultura de privacidade**<br>Qual a dependência entre estes dois conceitos? |
|---|---|
| *Padrão encontrado*<br><br>Influencia a cultura de privacidade | "Eu vejo uma primeiro que a outra. Vejo a estratégia primeiro, e depois como consequência desta a cultura. Havendo uma estratégia de topo para a privacidade, facilita o desenvolvimento de uma cultura de privacidade." (P7.V4.1 – P4ULSNA#06) |
| | "Uma estratégia de privacidade pode desenvolve uma cultura de privacidade e uma cultura de privacidade também pode influenciar a estratégia. Estão intimamente ligados." (P7.V4.1 – P4USF#05) |
| | "Quando falamos de cultura estamos a falar de um conhecimento maior sobre este assunto. Não adianta estar a criar uma cultura sem saber o caminho. Existe já uma cultura. Não existe é uma estratégia concertada, que tenha como objetivo criar uma plataforma comum, uma abordagem comum. E acho que deve ser definida no âmbito da administração pública, esta estratégia, para conseguirmos um maior conhecimento, para caminharmos num determinado sentido. Deve existir um plano de desenvolvimento, com um conjunto de ações que implementem uma estratégia." (P7.V4.1 – P4INEM#08) |
| | "A estratégia influencia a cultura. A cultura não aparece se não existir uma estratégia bem definida." (P7.V4.1 – P4HFF#05) |
| | "Primeiro têm que existir internamente alguém que se preocupe com este assunto. Depois é necessário que estes partilhem as suas dificuldades. Daí depois decorre partilharem ideias e formação." (P7.V4.1 – P4SPMS#05) |
| | "Isto é um assunto estratégico de futuro. O acesso à informação é um assunto fundamental e também formas expeditas de gerir informação também são fundamentais." (P7.V4.1 – P4HES#06) |

| **P7.V5.1** | **Colaboração no desenvolvimento de uma estratégia conjunta**<br>A harmonização das estratégias com base na colaboração, é fundamental ao desenvolvimento de um ambiente alargado da partilha confiante de dados? |
|---|---|
| *Padrão encontrado* | "A área da saúde é uma área de excelência. Seria desejável e importantíssimo construir uma estratégia conjunta para as questões da privacidade." (P7.V5.1 – P4ULSNA#06) |
| Necessária mais colaboração | "Contudo, naquilo que é e minha experiência, tudo que seja partilha, gera sempre desconfiança entre as organizações. Esta confiança tem que ser gerida." (P7.V5.1 – P4ULSNA#06) |
| Estratégia comum | "Estamos sempre muito cientes da nossa "quinta", o que significa que isto só se consegue com o apoio ou patrocínio de uma entidade como o ministério da saúde, ou da própria administração regional." (P7.V5.1 – P4ULSNA#06) |
| | "É necessário uma colaboração ao nível da gestão para se desenvolverem estas questões de uma forma transversal. A falta de conhecimento, de formação nestas questões pode impedir o desenvolvimento da colaboração. Caso contrário estas questões podem passar ao "lado"." (P7.V5.1 – P4USF#05) |
| | "Existem aqui aspetos que têm a ver com a informação que é transversal às organizações, que têm a ver com a gestão do cidadão perante a administração pública." (P7.V5.1 – P4INEM#08) |
| | "Tem que se fazer uma adaptação daquilo que são os direitos, as obrigações, transpô-los para um conjunto de requisitos do ponto de vista de gestão dos sistemas de informação, e de segurança, que possam ser obrigatoriamente incorporados cada vez que nós desenvolvemos um novo sistema de informação ou estamos a trabalhar a informação de uma instituição. Que esses requisitos sejam conhecidos para quem fornece os sistemas de informação os cumpra e esteja certificado nesse âmbito." (P7.V5.1 – P4INEM#08) |
| | "Teria que haver aqui uma partilha de experiências, de definição de diretrizes comuns entre todas as organizações. Andamos todos demasiado concentrados em querer inventar o nosso sistema, com segurança própria. Estas questões não são complexas e não são diferentes de outras situações." (P7.V5.1 – P4INEM#08) |
| | "Todas as instituições da administração pública devem partilhar da mesma estratégia comum para este problema." (P7.V5.1 – P4INEM#08) |
| | "O alinhamento de todas as estratégias em termos organizacionais, depende da tutela do ministério da saúde. Se nós estamos a passar dados para o exterior, apesar de os dados continuarem no hospital, tem de ser a tutela a definir esta estratégia. Deve contudo haver uma maior disponibilidade das organizações para colaborar com outras organizações na definição destas questões." (P7.V5.1 – P4HFF#05) |
| | "São questões muito importantes, muito atuais, mas ou existem diretrizes que permitam desencadear estas questões localmente ou então nunca vamos chegar a lado nenhum. As pessoas estão sensíveis para estas questões da privacidade, pretendem desenvolvê-las, mas apercebem-se que sozinhos não conseguem. Têm de ter por base uma estratégia global." (P7.V5.1 – P4HFF#05) |
| | "O futuro passa pelas soluções de interoperabilidade. Este deveria ser o papel principal do ministério. O ministério deveria estar a regular [...]" (P7.V5.1 – P4HES#06) |

## 3. Data Display

| **P7** | **Matriz de análise da opinião sobre P7. Estratégia para a privacidade** | | |
|---|---|---|---|
| *Variáveis dependentes* | *Padrão encontrado* | *A privacidade como um fator estratégico* *(Uma estratégia deve estar na base de um programa integrado e continuo de proteção dos dados)* | *Colaboração necessária para uma visão estratégica para a privacidade* *(questões que dependem da interoperabilidade organizacional)* |
| **P7.v1.** Uma estratégia para a privacidade está associada ao reconhecimento da privacidade como fator estratégico para a organização, e da sua responsabilidade sobre este assunto. | Valor organizacional<br>Responsabilidade | Os dados não podem ser apenas matéria-prima.<br>O reconhecimento dos dados e da privacidade como um valor para a instituição vai facilitar uma estratégia para a sua proteção.<br>A privacidade é um valor, que não se pode desvalorizar, nem corromper, e que tem que ser pensada de uma forma estratégica. | Acima de tudo é necessário desenvolver uma estratégia comum.<br>A proteção de dados é uma das maiores responsabilidades ao nível da gestão. Pode existir colaboração a este nível. |
| **P7.v2.** Uma estratégia para a privacidade constitui uma ferramenta essencial ao planeamento e integração de mecanismos de proteção e controlo da privacidade. | Importante<br>Colaboração | Faz sentido a existência de uma estratégia de desenvolvimento da privacidade como um todo.<br>Os gestores devem ser os dinamizadores e promover a preparação dos profissionais.<br>Incluir a privacidade no desenvolvimento estratégico dos SI. | Colaboração, interação entre responsáveis das organizações no desenvolvimento de uma estratégia comum.<br>Desenvolver a proteção de dados para as situações de partilha de serviços e de informação.<br>O Ministério deve promover a colaboração necessária ao desenvolvimento de uma estratégia integrada. |
| **P7.v3.** O conhecimento e consciência das práticas existentes de processamento de dados e a identificação do risco associado à ausência de políticas de proteção da privacidade e proteção de dados são impulsionadores de uma visão estratégica para a privacidade. | "Não encontrado" | O conhecimento dos riscos das situações de utilização e partilha de dados muda a atitude e preocupação existentes a nível coletivo.<br>A análise de risco ainda é insuficiente, não inclui a privacidade dos dados.<br>Os riscos atuais com a informação em suporte digital são muito elevados e devem ser identificados. | Análise do risco para as situações de partilha de dados.<br>Analisar o impacto da ausência de partilha de dados, o risco de os dados não estarem acessíveis.<br>É essencial para minimizar os eventos adversos que possam surgir, porque estamos a falar de partilha de dados, em que coexistem uma multiplicidade de SI. |
| **P7.v4.** Uma estratégia para a privacidade é promotora de uma cultura de privacidade. Uma cultura de privacidade emerge em cenários em que as questões associadas à privacidade e proteção dos dados têm por base uma estratégia de desenvolvimento em detrimento de auditorias pontuais de conformidade. | Influencia a cultura de privacidade | A estratégia primeiro, e depois como consequência desta a cultura de privacidade.<br>Uma estratégia de topo para a privacidade facilita o desenvolvimento de uma cultura de privacidade.<br>A cultura não aparece sem uma estratégia bem definida. | Desenvolvimento de uma estratégia concertada, que tenha como objetivo criar uma plataforma comum, uma abordagem comum.<br>Definição do âmbito para esta estratégia, que permita orientar o conjunto de ações necessárias à sua implementação. |
| **P7.v5.** Em ambientes de interoperabilidade, a colaboração para o desenvolvimento de uma estratégia conjunta para a privacidade potenciaria o desenvolvimento de uma plataforma confiável para a recolha, partilha e utilização de dados pessoais. | Necessária mais colaboração<br>Estratégia comum | O futuro passa pelas soluções de interoperabilidade.<br>As pessoas estão sensíveis para estas questões da privacidade, pretendem desenvolvê-las, mas apercebem-se que sozinhos não conseguem. Têm de ter por base uma estratégia global.<br>Existem aspetos que têm a ver com a informação que são transversais a todas as organizações.<br>A falta de conhecimento e formação podem impedir o desenvolvimento da colaboração necessária.<br>Tudo o que implica partilha, gera desconfiança. | O alinhamento de todas as estratégias em termos organizacionais depende da tutela, do Ministério da Saúde.<br>Todas as instituições da administração pública devem partilhar da mesma estratégia comum para este problema.<br>Necessário promover a partilha de experiências, e a definição de diretrizes comuns. São questões similares entre organizações. |