

A chamada “trilha para o DPO” na visão da EXIN implica na realização de três certificações distintas: a *Information Security Foundation* (ISFS), a *Privacy and Data Protection Foundation* (PDPF) e, por fim, a *Privacy and Data Protection Practitioner* (PDPP). Ainda que não exista uma ordem obrigatória na realização destas certificações, considero recomendado que a preparação seja feita nesta ordem pelos motivos indicados a seguir.

A *Information Security Foundation* (ISFS), como seu próprio nome já diz, refere-se à necessária fundamentação no âmbito da segurança da informação. O foco desta certificação baseia-se em conteúdos originados da norma ISO 27001. São avaliados, portanto, conhecimentos que relacionam os conceitos de informação e de segurança, confiabilidade, ameaças e riscos, como realizar a gestão dos riscos e, ainda, questões referentes a aspectos organizacionais da segurança da informação – como a criação de políticas e de um comitê gestor. Por fim, exige-se conhecimento a respeito das medidas físicas, técnicas e organizacionais necessárias para o gerenciamento do risco.

Por sua vez, a *Privacy and Data Protection Foundation* (PDPF) está vinculada diretamente ao Regulamento Geral de Proteção de Dados europeu (“RGPD”). O foco do curso está no conhecimento geral e teórico que a pessoa deve ter a respeito do RGPD. O candidato deve conhecer os fundamentos gerais da proteção de dados, especialmente no que diz respeito aos princípios, bases legais e direitos dos titulares de dados, bem como questões referentes às violações de dados pessoais. O candidato precisa saber também a respeito de transferências internacionais, regras corporativas vinculantes e as funções da Autoridade Supervisora. Além disso, é exigido também conhecimento a respeito das avaliações de impacto sobre a proteção de dados e sobre o *privacy by design* e o *privacy by default*.

Por fim, a *Privacy and Data Protection Practitioner* (PDPP), como o próprio nome indica, traz a prática da proteção de dados pessoais. O foco central está na preparação do chamado *Sistema de Gestão de Proteção de Dados*, cujo objetivo é o gerenciamento completo de dados pessoais em todo o seu ciclo de vida. O candidato precisa conhecer todas as fases e etapas deste sistema, além de se aprofundar em outras questões do RGPD – tais como as funções de um DPO, os papéis do controlador e do processador e como realizar, na prática, uma avaliação de impacto sobre a proteção de dados. Destaca-se ainda que a certificação exige que o

candidato conheça em detalhes o procedimento para as devidas notificações decorrentes da violação de dados pessoais.

No que diz respeito à preparação, a única das certificações que exige oficialmente que o candidato realize um curso é a *Practitioner*. Como o objetivo desta certificação é avaliar o conhecimento prático do candidato sobre o tema, a EXIN exige que o mesmo realize uma atividade prática, que poderá variar conforme a escola de formação escolhida pelo candidato. No meu caso, na escola em que fiz o curso foram oferecidas quatro opções: criação de uma política de proteção de dados e de privacidade completa; criação de um procedimento para resposta a notificação de violação de dados pessoais; realizar uma avaliação de impacto sobre a proteção de dados completa; ou criar um código de conduta de privacidade indicando as medidas organizacionais a serem tomadas com base no RGPD.

Já para as outras duas certificações o candidato poderá fazer a prova da EXIN sem nenhum tipo de curso oficial prévio – o que, é claro, irá variar conforme a experiência do candidato. Por exemplo, no meu caso fiz um curso para a *Information Security Foundation* por acreditar que meu conhecimento prévio sobre o tema era insuficiente, mas não fiz nenhum curso para a *Privacy and Data Protection Foundation* porque já trabalhava como DPO no momento de realização da prova.

Em termos de dicas de estudo, não há dúvidas de que o candidato deverá conhecer de maneira razoavelmente profunda o texto do RGPD, já que ele será o ponto de partida não apenas do estudo em si, mas também das provas de certificação e da própria atuação prática do DPO. É necessário conhecer claramente as seis bases legais, os sete princípios, os vários direitos dos titulares de dados e os inúmeros deveres do responsável pelo tratamento e do subcontratante. Também é necessário conhecer as exigências do Regulamento no que diz respeito às avaliações de impacto, às transferências internacionais e a violações de dados pessoais. A leitura do texto do RGPD, portanto, se configura como elemento essencial para a correta preparação para as certificações.

Além disso, considero como válida a leitura das várias *Guidelines* do Grupo de Trabalho do Artigo 29 (WP29) e do Comitê Europeu para a Proteção de Dados (EDPB) a respeito destes

vários temas. Ainda que estas *Guidelines* não sejam exigidas explicitamente para as provas de certificação, sua leitura é relevante para que o candidato conheça a principal *interpretação* sobre o conteúdo do RGPD – o que se torna extremamente relevante especialmente para aqueles que não são originariamente da área jurídica. Além disso, estas *Guidelines* fornecerão o melhor rumo a ser seguido quando da atuação da pessoa como DPO.

Outra dica relevante diz respeito ao conhecimento mínimo de termos técnicos, especialmente por parte daqueles que não têm formação na área de TI. Saber o que é um *honeypot*, uma *DMZ*, um *DLP* ou quais são as diferenças entre criptografia *simétrica* e *assimétrica* é fundamental não apenas para a realização da prova em si, mas também – e principalmente – para a atuação prática na carreira de DPO, já que esta pessoa será responsável pela proteção de dados como um todo – não havendo necessariamente uma “separação” entre a atuação do DPO “jurídico” e do DPO “tecnológico” (ainda que isto pode variar de empresa para empresa). Conhecer os aspectos jurídicos e técnicos do RGPD é fundamental tanto para aqueles que pretendem trabalhar como DPO interno quanto para aqueles que pretendem trabalhar no formato de *DPO as a Service*.