GESTÃO DE RISCO EMPRESARIAL E PROTEÇÃO DE DADOS
(VIOLAÇÃO DE PRIVACIDADE)

A Gestão do Risco Empresarial (GRE) é um processo estratégico de gestão, o qual tem como principal objetivo mitigar e controlar os eventuais impactos negativos que determinados eventos poderão ter no negócio, sejam eventos de origem interna ou externa à organização, eventos estes que perturbam parcial ou totalmente a boa execução dos processos de negócio. Deste modo a materialização destes eventos de risco tem consequências negativas ao nível do cumprimento dos objetivos estratégicos definidos e certamente impactos financeiros relevantes. Os riscos poderão ser de diferentes tipos, tais como: riscos estratégicos, financeiros, operacionais, de sistemas de informação, fraude interna, fraude externa, riscos de privacidade de dados e segurança de informação, entre outros.

A GRE proporciona às organizações uma melhoria da capacidade para um alinhamento dos níveis de aceitação dos riscos com a estratégia da Empresa. No fundo permite definir qual o grau de risco que a Empresa está disposta a aceitar para cumprir com os seus objetivos. E proporciona uma melhoria da capacidade para identificar e avaliar os riscos, permitindo melhorar o processo de tomada de decisão no que concerne a resposta ao risco, aumentando assim o seu retorno. A GRE proporciona um maior rigor para identificar e selecionar as respostas alternativas ao risco - anulação, redução, partilha e aceitação do risco - proporcionando metodologias e técnicas para a tomada de decisão.

Outro dos principais objetivos da GRE é a minimização de eventos operacionais surpresa e os respetivos prejuízos. A GRE permite melhorar a capacidade das organizações para identificar potenciais eventos, avaliar os riscos e estabelecer respostas, reduzindo deste modo a ocorrência de surpresas e a sua relação com custos ou perdas. Com a melhoria da capacidade das organizações para a identificação e gestão efetiva dos riscos transversais à organização, como por exemplo a atual situação do COVID-19. Não obstante, a equipa de gestão necessita de gerir os riscos de forma individual e compreender quais os de maior relevância e quais os seus impactos inter-relacionados.

É muito importante que a gestão capacite a organização com os mecanismos adequados para proporcionar uma resposta integrada aos diferentes tipos de riscos. Os processos de negócio têm muitos riscos inerentes e a GRE permite integrar soluções para gerir os riscos.

Numa perspetiva integrada de um modelo de gestão de riscos empresariais, a gestão de topo deve considerar os eventos potenciais, como oportunidades de melhoria e decidir implementar os referidos mecanismos para mitigação dos riscos no futuro. Desta forma, e considerando uma maior disponibilidade de informação, de forma integrada, sobre os riscos existentes e os possíveis no futuro, permite uma gestão mais eficaz da avaliação das necessidades de capital e da melhoria na sua partilha.

Em situações extremas, como a atual epidemia COVID-19, a gestão do risco tem um papel ainda mais relevante, não apenas para prevenir, mas sobretudo para apoiar numa resposta célere a eventos extraordinários em curso e, desta forma, minimizar o impacto associado aos mesmos e garantindo a devida continuidade do negócio.

Vivendo atualmente a nossa sociedade um período único e conturbado, impossibilitando que a generalidade das organizações opere de acordo com os seus usuais processos internos, as organizações, tal como a APDL, colocam os seus colaboradores em ambiente remoto de teletrabalho e como tal com uma maior exposição ao risco. Desta forma, devem existir mecanismos de adequados para controlar os possíveis eventos de risco, principalmente os que estão associados aos temas da Segurança de informação e da Privacidade dos Dados, pelo facto de haver uma maior partilha de informação, a qual contém dados relevantes da organização e por sua vez conteúdos que poderão conter dados pessoais. Em ambientes de trabalho remoto, há uma maior utilização de sistemas digitais, virtualizados e uma maior adesão à utilização das novas tecnologias e aplicações. Aplicações que são usadas em prol do teletrabalho; no entanto o mesmo dispositivo é utilizado em atividades de cariz privado e.g. os Smartphones, a utilização de ambientes virtualizados na "nuvem" (*cloud*) e aquisição de subscrições de soluções em modelo de SaaS (*Software as a Service*), entre outros.

O uso das novas tecnologias, com maior regularidade e para os diferentes fins, provoca uma necessidade maior, por terceiros, em recolher esses dados para alcançar diferentes objetivos, do ponto de vista da analítica de dados, análise de padrões e principalmente de comportamentos, de forma a garantir um melhor fornecimento dos serviços digitais por parte dos fornecedores e de acordo com a experiência dos utilizadores. Relativamente à experiência dos utilizadores, o objetivo é certamente a geração de receita para as organizações.

As organizações recolhem, armazenam e processam cada vez mais dados e os quais são de facto hoje um dos ativos mais importantes e um bem muito valioso. Na maioria das vezes os dados recolhidos são efetivamente os chamados dados sensíveis, como por exemplo os dados que atualmente do ponto de vista da COVID-19 são recolhidos hoje, tais como dados genéticos, dados biométricos tratados simplesmente para identificar um ser humano ou dados relacionados com a saúde e que levam à necessidade de um controlo maior sobre a forma como estes dados são tratados e processados, de forma a controlar o risco associado à sua privacidade. O acesso indevido a este tipo de dados pode ter um impacto devastador na vida de um indivíduo e, como tal, no âmbito da gestão dos riscos de privacidade dos dados e da segurança de informação, implica que sejam implementados controlos para mitigar estes riscos e reduzir os impactos dos mesmos quer do ponto de vista do colaborador quer do ponto de vista da Empresa e da sua reputação.

O facto de uma cada vez maior partilha de dados pessoais, por cada uma das pessoas, com as empresas em relações e em ambiente de negócio digital, tem-se traduzido num maior número de ataques por parte de *Hackers* a diferentes empresas dos mais diversos setores de negócio. Por sua vez este tipo de ataques traduziu-se obviamente numa maior preocupação com a gestão riscos associados ao roubo ou utilização de forma ilícita dos dados, assim como um crescimento significativo na área da segurança da informação nos últimos anos. Os grupos ou comunidades que exploram as mais diversas vulnerabilidades dos sistemas e aplicações, assim como de dispositivos de rede, os quais são utilizados pelas pessoas, cresceu de igual forma reduzindo a eficácia das medidas de segurança existentes.

A recolha dos dados pessoais e os fins para os quais os mesmos são utilizados e o tratamento que é dado aos mesmos é de facto outro problema, assim como a transmissão desses dados para terceiros sem qualquer autorização do titular dos dados.

De forma reduzir as ameaças existentes foi necessário implementar controlos nesta área por via do desenvolvimento de regulamentação comunitária e a nível nacional de forma a especificar e legislar as medidas e os cuidados a ter com a segurança, na recolha, no tratamento, no armazenamento e na transmissão dos dados pessoais, conforme descrito no Regulamento Geral de Proteção de Dados (RGPD), na Lei nº 58/2019 (execução, na ordem jurídica nacional, do Regulamento (UE) 2016/679 do Parlamento e do Conselho), na Lei nº 46/2018 (regime jurídico da segurança do ciberespaço), bem como a Resolução do Conselho de Ministros nº 41/2018 (orientações técnicas para a Administração Pública em matéria de arquitetura de segurança das redes e sistemas de informação relativos a dados pessoais).

As organizações são assim obrigadas as implementar mecanismos que tornem os seus sistemas mais seguros, de forma a evitar que os dados pessoais sejam obtidos por terceiros com objetivo de tratar esses dados de forma diferente do propósito para os quais foram recolhidos, ou por entidades maliciosas que pretendam utilizar esses dados para fins fraudulentos ou maliciosos. Como forma de mitigação, as empresas têm hoje que implementar controlos detetivos que permitam reduzir os riscos de coimas, com impacto financeiro ou reputacional e paralelamente garantir que os titulares são informados em tempo regulamentar e que têm conhecimento do que acontece com os seus dados.

Com obrigatoriedade da implementação dos mecanismos associados ao cumprimento do RGPD, e mais tarde com a Resolução do Conselho de Ministros 41/2018, aplicável aos sistemas de informação da Administração Publica no que concerne a Segurança de Informação, (orientações técnicas para a Administração Pública em matéria de arquitetura de segurança das redes e sistemas de informação relativos a dados pessoais), as Organizações que o fizeram reduziram de forma significativa o risco associado à Segurança da Informação e da privacidade dos dados pessoais contra os abusos do uso da informação e ameaças.