Boletim IIA

*Perspectiva para auditores internos sobre as questões mais urgentes da atualidade* *Janeiro de 2020*

# Dia Internacional da Privacidade dos Dados

**Dia 28 de janeiro é o Dia Internacional da Privacidade dos Dados,** que serve como lembrete importante de que os líderes de auditoria interna devem estar cientes e entender os regulamentos relacionados à privacidade aplicáveis à sua organização, bem como a postura de suas organizações sobre a privacidade dos dados. A crescente lista de regulamentos de jurisdições do mundo todo está tornando a privacidade dos dados cada vez mais complexa e dinâmica. Esses regulamentos abrangem uma ampla gama de questões, incluindo requisitos específicos relacionados à coleta, gerenciamento, armazenamento e uso dos dados.

Por exemplo, há décadas existem orientações regulatórias sobre políticas de privacidade de dados para organizações financeiras que cumprem com a Lei Gramm-Leach-Bliley (GLBA). Enquanto isso, a Lei de Privacidade do Consumidor da Califórnia (CCPA) entrou em vigor em 1º de janeiro de 2020, mas os legisladores continuam a fazer alterações a essa legislação histórica. Da mesma forma, a implantação das *Global Data Protection Regulations* (GDPR) da União Europeia, desde sua data de início em maio de 2018, foi um pouco diferente do inicialmente previsto, deixando algumas organizações com mais perguntas do que respostas.

Os líderes de auditoria interna devem se manter atualizados sobre essa área de risco volátil (consulte os recursos na página 2) e incorporar auditorias com foco em governança de dados, ética de dados, gerenciamento de dados e práticas de privacidade de dados. A seguir, compilamos uma lista de perguntas gerais criadas para ajudar as organizações que ainda não fizeram uma avaliação de privacidade de dados.

## Perguntas gerais para avaliar a privacidade de dados de sua organização

**A seguir, algumas perguntas gerais** que seu departamento de auditoria interna deve fazer para determinar se sua organização está lidando devidamente com a privacidade de dados:

- Como a privacidade dos dados foi identificada na avaliação de riscos mais recente?
- Quem é designado como responsável pela proteção de dados da organização ou responsável pela privacidade e conformidade dos dados?
- Quem é o proprietário da política (políticas) da organização sobre a privacidade dos dados do consumidor?

- Onde a gestão mantém um inventário dos regulamentos aos quais sua organização está sujeita, e como ele é mantido atualizado?
- Onde a gestão mantém um inventário de todos os terceiros que aceitam, processam ou armazenam dados em nome da organização, e como ele é mantido atualizado?
- Quais programas e aplicativos armazenam dados confidenciais? Há controles gerais de TI, controles de aplicativos e controles de rede suficientes sobre eles? Esses controles estão operando com eficácia?
- Quais outros controles relevantes (preventivos e detectivos) existem quanto à privacidade dos dados? Eles estão operando com eficácia?
- Quem é responsável por garantir que exista um processo documentado que detalhe o que fazer no caso de uma violação de dados, e onde fica essa documentação?

## Seis passos para uma auditoria simples de privacidade de dados

**Embora as atividades executadas durante a auditoria de privacidade de dados** variem de organização para organização, o exemplo a seguir é um esboço para os auditores internos usarem ao planejar e executar uma auditoria de privacidade de dados simples, mas valiosa:

1. Colete o inventário de:
   - Todos os regulamentos aplicáveis com componentes de privacidade.
   - Todas as políticas de privacidade de dados da sua organização (p. ex., sites, mobile, correspondências, telefone, e-mail).
   - Todas as suas políticas de privacidade de dados de terceiros (aquelas às quais você redireciona seus clientes, como PayPal).
2. Compare todos os critérios regulatórios relacionados à privacidade aplicáveis às políticas de privacidade de dados da sua organização. Observe quaisquer exceções ou lacunas.
3. Compare todas as políticas de privacidade de terceiros aplicáveis às políticas de privacidade de dados de sua própria organização. Observe quaisquer inconsistências.
4. Mapeie a(s) política(s) alinhada(s) com os controles de sua organização. As lacunas mostrarão áreas potenciais de maior risco.
5. Verifique se o que está descrito na(s) política(s) está em prática (vinculado a processos e controles específicos). Observe quaisquer exceções. Elementos a validar incluem: quais dados são coletados? Quais dados são armazenados? Por quanto tempo são armazenados? Como são usados? Para quem são vendidos? Quem tem acesso de leitura? Quem tem acesso de gravação? Por quanto tempo são retidos? Como são destruídos? Anote se alguma dessas perguntas não for respondida em sua política.
6. Valide os controles. Um teste simples é logar em um aplicativo que deva estar em conformidade com sua política de privacidade de dados e, então, obter e revisar o conteúdo referente às suas atividades ao longo do caminho.

# RECURSOS DO THE IIA


**GTAGS**

- *Auditing Third-Party Risk Management*


**Guias Práticos**

- *Understanding and Auditing Big Data*

**Revista *Internal Auditor***

- *GDPR's Global Reach*
- *A Matter of Privacy*
- *The Consumer's Data Anxiety*
- *Assurance in the Privacy Regulatory Age*

***Internal Audit Foundation***

- *Cybersecurity: What the Board of Directors Needs to Ask*
- *Privacy In The Age Of Big Data: Recognizing Threats, Defending Your Rights, And Protecting Your Family*

SOBRE O THE IIA

*The Institute of Internal Auditors* (The IIA) é o mais reconhecido advogado, educador e fornecedor de normas, orientações e certificações da profissão de auditoria interna. Fundado em 1941, o The IIA atende, atualmente, mais de 200.000 membros de mais de 170 países e territórios. A sede global da associação fica em Lake Mary, na Flórida, EUA. Para mais informações, visite www.theiia.org.