Por CT Leste de Governança e Riscos[1]

Da realidade para o cinema ou do cinema para a realidade? Várias produções do cinema têm abordado, ao longo dos anos, processos de segurança da informação e suas vulnerabilidades. Entre elas podemos destacar: **Prenda-me se for capaz (**2002), **FireWall-Segurança em Rede (**2006), **Hacker (**2015).

Não é de hoje que assuntos sobre **segurança da informação in**spiram roteiros de cinema. Afinal, desde as mais simples abordagens e até as técnicas mais sofisticadas para roubar dados e paralisar operações, todas parecem próximas demais da realidade da tecnologia da informação que atualmente vivemos.

O que serve para nos alertar sobre o quão importante e vulneráveis são os processos relativos à segurança da informação, principalmente, no ambiente corporativo. Por isso, devem ser criteriosamente, elaborados, avaliados e monitorados.

Um levantamento da Check Point Software Technologies[2] apontou que em 2020 as tentativas de ataques cibernéticos se intensificaram, atingindo 2,5 milhões de ocorrências registradas, em um período de apenas seis meses.

Diante desse volume de tentativas de ataques, percebe-se que é impossível evitá-los; entretanto cabe às empresas definirem seus processos de segurança, controles e suas políticas, dando diretrizes para os aspectos físicos, tecnológicos e humanos da segurança da informação, a fim de se minimizar a efetivação dos ataques recebidos, tornando seu ambiente mais robusto e seguro.

Só pela segurança da informação em si, já se requer cuidados primorosos nos processos de coleta, guarda, tratamento, compartilhamento e descarte de dados. Mas, com o advento da Lei Geral de Proteção de Dados, os cuidados com os dados pessoais em uma empresa devem estar intrínsecos, verdadeiramente, nesses processos. Por esta razão, a edição do Saiba Como deste mês será dedicada, mais especificamente, a processos relacionados com a proteção de dados pessoais.

A seguir, é apresentado resumo com sugestões de práticas que devem ser considerados na busca de segurança da informação, dentro das organizações, em relação à coleta e tratamento, armazenamento, compartilhamento e descarte de dados, conforme Checklist-ISO27701 e Cys Controls – Frameworks.

a) Coleta e tratamento de dados

1. Identificação e documentação dos propósitos específicos	Identificar e documentar os propósitos específicos pelos quais os dados pessoais serão tratados.
2. Identificação de bases legais	Determinar, documentar e estar em conformidade com a base legal pertinente para o tratamento de dados pessoais para os propósitos identificados.
3. Determinando quando e como o consentimento deve ser obtido	Determinar e documentar um processo pelo qual ela possa demonstrar se, quando e como o consentimento para o tratamento de dados pessoais foi obtido dos titulares de dados pessoais.
4. Obtenção e registro de consentimento	Obter e registrar o consentimento dos titulares de dados pessoais de acordo com os processos documentados.
5. Avaliação de impacto de privacidade	Avaliar a necessidade para a coleta de dados, e

	implementar onde apropriado, uma avaliação de impacto de privacidade quando novos tratamentos de dados pessoais ou mudanças ao tratamento existente de dados pessoais forem planejados.
6. Contratos com Operadores de dados pessoais	Elaborar contrato por escrito com qualquer Operador de dados pessoais que ela utilize, e deve assegurar que os seus contratos com os Operadores de dados pessoais contemplem a implementação de controles apropriados, conforme descrito no Anexo B da ISO/IEC 27701.
7. Controlador conjunto de dados pessoais	Determinar as responsabilidades e respectivos papéis para o tratamento de dados pessoais (incluindo a proteção desses dados e os requisitos de segurança) com qualquer controlador conjunto.
8. Registros relativos ao tratamento de dados pessoais	Determinar e manter de forma segura os registros necessários ao suporte às suas obrigações para o tratamento dos dados pessoais.
9. Acordos com o cliente	Assegurar, onde pertinente, que o contrato para tratar dados pessoais considera os papéis da organização em fornecer assistência com as obrigações do cliente (considerando a natureza do tratamento e a informação disponível para a organização).
10. Propósitos da organização	Assegurar que os dados pessoais tratados em nome do cliente sejam apenas tratados para o propósito expresso nas instruções documentadas do cliente.
11. Uso de marketing e propaganda	Utilizar os dados pessoais tratados sob um contrato para o propósito de marketing e propaganda, sem o estabelecimento de que um consentimento antecipado foi obtido do titular de dados pessoais apropriados. A organização não pode fornecer este consentimento como uma condição para o recebimento do serviço.
12. Violando instruções	Informar ao cliente se, na sua opinião, uma instrução de tratamento viola uma regulamentação e/ou legislação aplicável.
13. Obrigações do cliente	Fornecer ao cliente informações apropriadas de tal modo que o cliente possa demonstrar conformidade com suas obrigações.
14. Registros relativos ao tratamento de dados pessoais	Determinar e manter os registros necessários à evidência de conformidade com suas obrigações (como especificado no contrato aplicável) para tratamento de dados pessoais realizado em nome do cliente.
15. Realizar inventário das informações sigilosas	Realizar inventário dos dados armazenados, processados ou transmitidos pelos sistemas de tecnologia da organização.
16. Utilizar modelos padrão de configurações de proteção para bancos de dados	Utilizar, para aplicativos que dependem de um banco de dados, modelos de configuração de mascaramento de dados e criptografia de dados.

b) Guarda

17. Garantir backups regulares automáticos	Verificar que todos os dados do sistema sejam regularmente copiados automaticamente para um backup.
18. Realizar backupscompletos dos sistemas	Garantir que todos os principais sistemas da organização salvos em backupcomo um sistema completo, por meio de processos como geração de imagens, para permitir a rápida recuperação de um sistema inteiro.
19. Validar e proteger os dados em backup	Realizar regularmente testes de restauração dos backups de sistemas e validações de integridade dos dados dos backups realizados, certificando-se que estejam adequadamente via segurança física ou criptografia quando forem armazenados e quando forem transferidos pela rede. Isso inclui backupsremotos e serviços em nuvem.
20. Garantir que todos os backups tenham pelo menos um destino de backup offline	Verificar se todos os backups têm pelo menos um destino de backup offline (ou seja, não acessível por uma conexão de rede).
21. Manter inventário das informações sigilosas	Manter inventário dos dados armazenados, processados ou transmitidos pelos sistemas de tecnologia da organização.
22. Remover dados sigilosos ou sistemas que não são acessados regularmente pela organização	Remover da rede dados sigilosos ou sistemas não acessados regularmente pela organização. Esses sistemas devem ser usados pela unidade de negócios apenas como sistemas independentes (desconectados da rede) que em caso de utilização ocasional precisam ser utilizados de forma completamente virtualizada e desligados até que sejam necessários novamente.
23. Monitorar e bloquear tráfego de rede não autorizado	Implementar ferramenta automatizada no perímetro das redes que monitore e bloqueie a transferência não autorizada de informações confidenciais enquanto alerta os profissionais de segurança da informação.
24. Permitir acesso apenas ao armazenamento em nuvem autorizado ou a provedores de e-mail	Permitir acesso apenas a provedores de armazenamento em nuvem ou e-mail autorizados.
25. Monitorar e detectar qualquer uso não autorizado de criptografia	Monitorar todo o tráfego que sai da organização e detecção de qualquer uso não autorizado de criptografia.
26. Criptografar dados de dispositivos móveis	Utilizar mecanismos criptográficos aprovados para proteger os dados corporativos armazenados em todos os dispositivos móveis.
27. Gerenciar dispositivos USB	Utilizar, caso seja imperativo o armazenamento em dispositivos USB, softwarecorporativo que possa configurar sistemas para permitir o uso de dispositivos específicos. Um inventário desses dispositivos deve ser mantido, com os dados devidamente criptografados.
28. Gerenciar configurações de leitura/gravação de mídia removível externa de sistemas.	Configurar os sistemas para não gravar dados em mídia removível externa, se não houver real necessidade comercial de oferecer suporte a estes tipos de dispositivos.
29. Criptografar todas as informações sigilosas em trânsito	Criptografar todas as informações sensíveis em trânsito.
30. Utilizar ferramenta de descoberta ativa para	Utilizar ferramenta de descoberta ativa para

identificar informações sigilosas	identificar todas as informações sigilosas armazenadas, processadas ou transmitidas pelos sistemas de tecnologia da organização, incluindo sistemas localizados localmente ou em provedores de serviços remotos para atualização do inventário de informações confidenciais da organização.
31. Proteger o acesso as informações através de listas de controle de acesso	Proteger todas as informações armazenadas em sistemas com listas de controle de acessos específicos dos sistemas de armazenamento e gerenciamento de arquivos, compartilhamento de rede, ticket/chamados, aplicativos ou banco de dados.
32. Aplicar controle de acesso aos dados por meio de ferramentas automatizadas	Utilizar ferramenta automatizada que previna a perda de dados baseada em host, para imposição de controles de acesso aos dados, mesmo quando os dados são copiados de um sistema.
33. Criptografar informações sigilosas em repouso	Criptografar todas as informações sigilosas em repouso usando uma ferramenta que requer um mecanismo de autenticação secundário não integrado ao sistema operacional, para acessar as informações.
34. Configurar logs detalhados que registrem acesso ou alterações em dados sigilosos	Implementar logs de auditoria detalhadas para acesso e alterações de dados sigilosos.

c) Compartilhamento, transferência e descarte de dados

35. Bases para a transferência de dados pessoais entre jurisdições	Informar ao cliente em tempo hábil sobre as bases para a transferência de dados pessoais entre jurisdições e de qualquer mudança pretendida nesta questão, de modo que o cliente tenha a capacidade de contestar estas mudanças ou rescindir o contrato.
36. Países e organizações internacionais para os quais os dados pessoais podem ser transferidos	Especificar e documentar os países e as organizações internacionais para os quais dados pessoais possam ser transferidos.
37. Registros de dados pessoais divulgados para terceiros	Registrar a divulgação de dados pessoais para terceiros, incluindo quais dados pessoais foram divulgados, para quem e quando.
38. Notificação de solicitações de divulgação de dados pessoais	Notificar ao cliente sobre quaisquer solicitações legalmente obrigatórias para a divulgação de dados pessoais.
39. Divulgações legalmente obrigatórias de dados pessoais	Rejeitar quaisquer solicitações para a divulgação de dados pessoais que não sejam legalmente obrigatórias, consultar o cliente em questão antes de realizar quaisquer divulgações dos dados pessoais e aceitar quaisquer solicitações contratualmente acordadas para a divulgação de dados pessoais, que sejam autorizadas pelo respectivo cliente.
40. Divulgação de subcontratados usados para tratar dados pessoais	Divulgar para o cliente qualquer uso de subcontratados para tratar dados pessoais, antes do uso.
41. Contratação de subcontratado para tratar dados pessoais	Subcontratar somente agente para tratar dados pessoais com base no contrato do cliente.
42. Mudança de subcontratado para tratar dados	Informar ao cliente, no caso de ter uma

pessoais	autorização geral por escrito, quaisquer alterações pretendidas relativas à adição ou substituição de subcontratados no tratamento de dados pessoais, dando assim ao cliente a oportunidade de se opor a essas alterações.

Nesta edição, ficamos por aqui. Mas não perca a nossa próxima edição: – “Saiba como tornar seus processos de T.I. robustos e capazes de prevenir ataques cibernéticos – Parte IV”.

Fonte: Abrapp em Foco, em 10.11.2021.

[1] Comissão Técnica Regional Leste de Governança e Riscos – Parte III

[2] Fonte: https://canaltech.com.br/seguranca/3-milhoes-de-ataques-em-2020-ja-tentaram-explorar-sistemas-desatualizados-173889/.