HACK3R_
RANGER5

LEIS E NORMAS *QUE EXIGEM* CONSCIENTIZAÇÃO EM CIBERSEGURANÇA

Você certamente já sabe que educar seus colaboradores a respeito dos riscos cibernéticos é uma excelente maneira de otimizar sua estratégia de segurança da informação e garantir que seus funcionários não caiam na crescente onda de golpes digitais que colocam seus dados sensíveis em xeque.

Porém, o que muitos empreendedores — especialmente os donos de pequenas e médias empresas — não sabem é que programas de conscientização também são recomendados e até mesmo exigidos em uma série de normas e legislações!

No total, se contarmos diretrizes e padrões a níveis locais (ou seja, municipais), estaduais, federais e internacionais, são mais de 8,5 mil regulações que citam o treinamento e a capacitação de seu pessoal como uma peça fundamental para garantir a segurança de informações confidenciais.

Claro, isso não significa que você precisa se adequar a todas elas; temos casos que são bem específicos para determinados segmentos comerciais. Porém, tantas outras são universais e algumas servem para demonstrar que seu negócio adota as melhores práticas do mercado, atuando como uma certificação.

TEM QUE OBEDECER!

Dentre as legislações mais importantes que podemos citar, as mais fáceis de se lembrar são, certamente, a brasileira **Lei Geral de Proteção de Dados (LGPD)** e a europeia **Regulamento Geral de Proteção de Dados** (General Data Protection Regulation ou GDPR).

A primeira é mandatória para qualquer empresa que preste serviços no Brasil e colete dados pessoais e/ou sensíveis de cidadãos no país; já a segunda aplica-se em qualquer empreendimento que tenha consumidores oriundos de qualquer estado-membro da União Europeia. Sendo assim, caso você tenha uma loja e envie, por exemplo, para Portugal, a GDPR também se aplica ao seu negócio — mesmo se você não tiver um escritório por lá.

- **LGDP (lei nº 13.709 de 14 de agosto de 2018):**

Diz em seu art. 50: “os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança", incluindo "as ações educativas.”

Também temos, no art. 41, §2°, o item que recomenda "orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais."

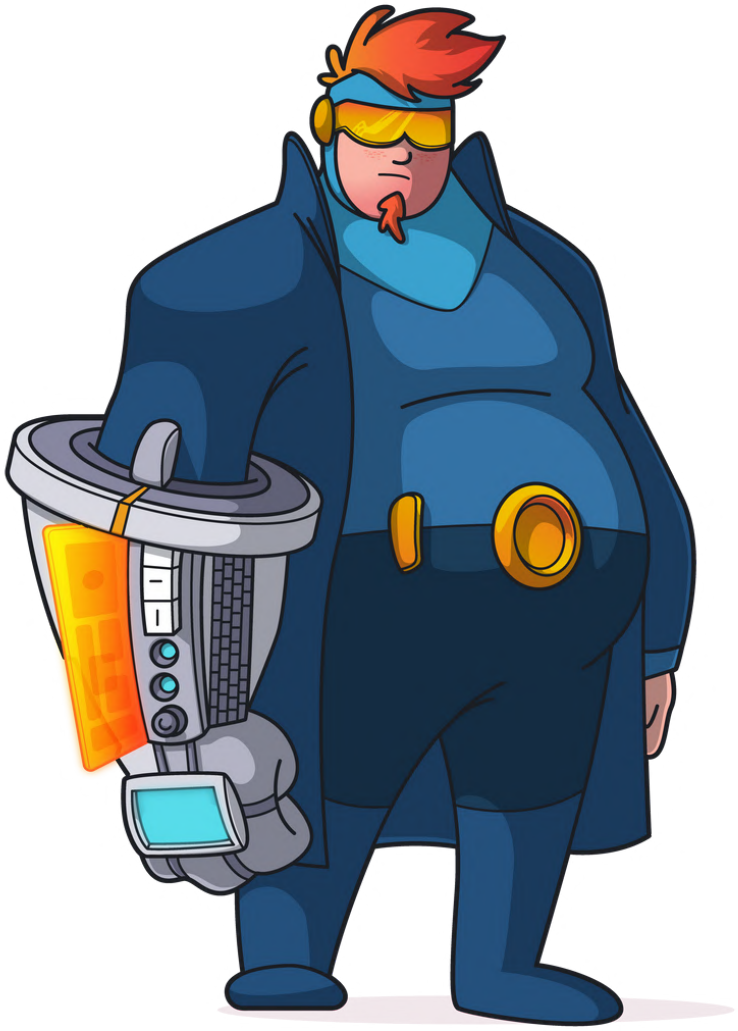
- **GDPR (2016/679)**

Conforme indicado pelo SANS Institute, “as organizações precisam garantir que todos os funcionários que lidam com dados pessoais recebam treinamento adequado sobre como manter de forma segura e proteger esses dados.”

- **Lei de Portabilidade e Responsabilidade do Seguro de Saúde (Health Insurance Portability and Accountability Act, HIPAA)**

De origem estadunidense e focada na segurança de dados de saúde, a HIPAA afirma, em seu padrão § 164.308 (A) (5) (I), que é obrigatória às instituições “implementar um programa de conscientização e treinamento de segurança para todos os membros de sua organização (incluindo a administração).”

SE VOCÊ FAZ PARTE...



Como dissemos anteriormente, algumas normativas são específicas para determinados segmentos comerciais. Dentre tais categorias, podemos destacar, por exemplo, as normas e resoluções que foram criadas especialmente para a indústria financeira, incluindo instituições de pagamento, bancos e emissores de cartões de crédito. Podemos citar:

- **Circular nº 3.909 de 16 de agosto de 2018 e Resolução nº 4.658 de 26 de abril de 2018 do Banco Central do Brasil (Bacen)**

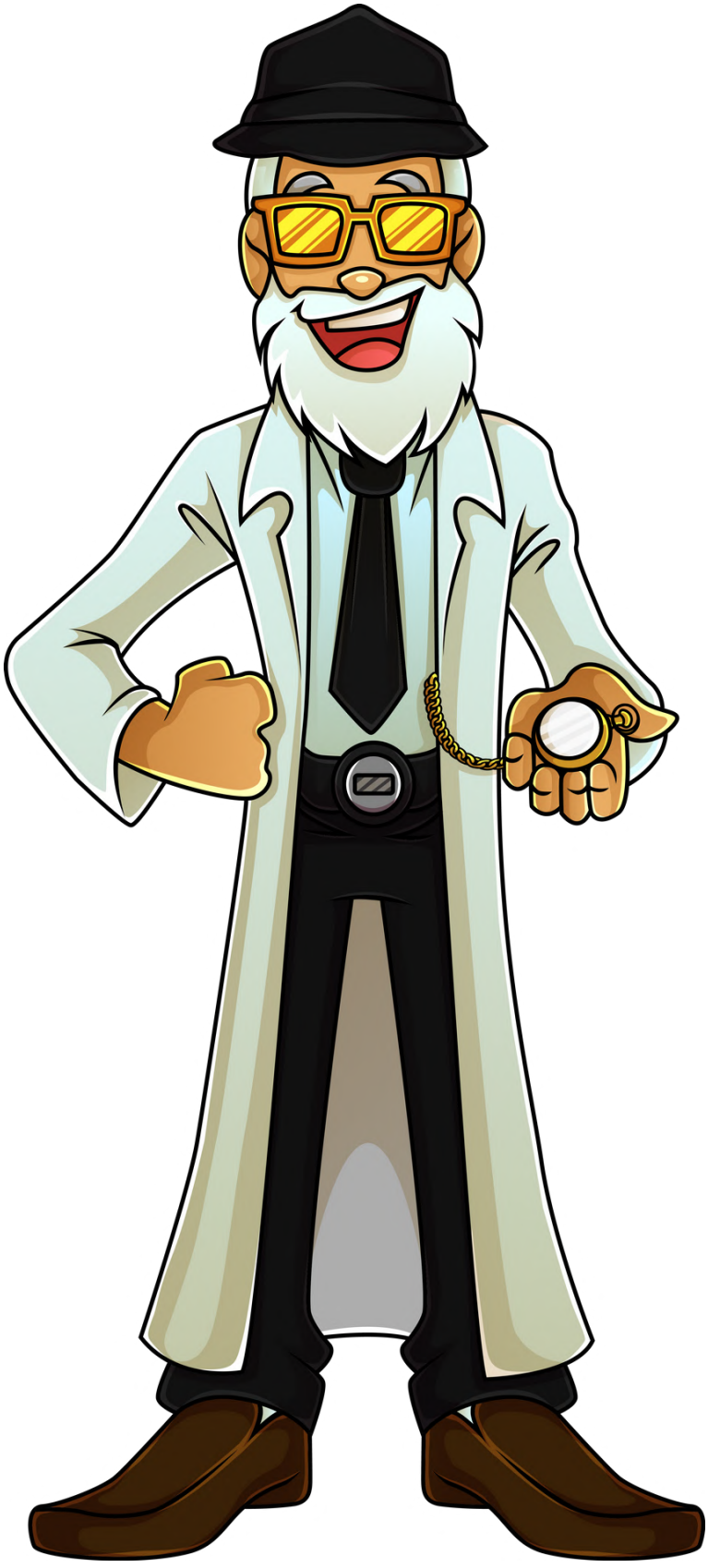
O art. 3º da circular afirma que a política de segurança cibernética de qualquer instituição bancária brasileira deve contemplar, dentre outros itens, "a implementação de programas de capacitação e de avaliação periódica de pessoal"; ademais, no art. 4º, diz que "a política de segurança cibernética deve ser divulgada aos funcionários da instituição de pagamento e às empresas prestadoras de serviços a terceiros, mediante linguagem clara, acessível e em nível de detalhamento compatível com as funções desempenhadas e com a sensibilidade das informações."

A resolução traz exatamente os mesmos artigos da circular, mas foi publicada em específico para tratar da contratação de serviços de armazenamento e processamento de dados em nuvem por parte de fornecedores terceiros.

- **Payment Card Industry Data Security Standard (PCI-DSS)**

Trata-se de uma norma criada pelo Conselho de Padrões de Segurança da Indústria de Cartões de Pagamento com o objetivo de padronizar boas práticas para quem emite cartões de crédito e/ou débito, tal como quem recebe pagamentos através desse método. Em seu parágrafo § 12.6, instrui que você "implemente um programa formal sobre conscientização de segurança para conscientizar todos os funcionários em relação à política e aos procedimentos de segurança dos dados do titular do cartão."

HACK3R_
RANGER5



- **Instruções nº 505, nº 558 e nº 612 da Comissão dos Valores Mobiliários (CVM)**

Ambas tratam de segurança da informação dentro do mercado de valores mobiliários — ou seja, ações, investimentos e afins. A de nº 505 (posteriormente atualizada na de nº 612) afirma que a política do intermediário deve "prever a periodicidade com que funcionários, prepostos e prestadores de serviços serão treinados quanto aos procedimentos previstos nos arts. 35-E e 35-F e quanto ao programa de segurança cibernética".

Já a instrução de nº 585 é focada no administrador de carteiras de valores mobiliários e afirma que ele, enquanto pessoa jurídica, deve "implantar e manter programa de treinamento de administradores, empregados e colaboradores que tenham acesso a informações confidenciais, participem de processo de decisão de investimento ou participem de processo de distribuição de cotas de fundos de investimento."

HACK3R_
RANGER5

BOAS MANEIRAS À MESA

Se até agora falamos sobre normas e leis que precisam ser seguidas à risca (sendo algumas universais e outras específicas para certos segmentos comerciais), também temos padrões que, embora não sejam obrigatórios, podem ser considerados diferenciais competitivos para qualquer empresa. Estamos falando de documentos que orientam as melhores práticas sobre segurança da informação; garantir conformidade com eles é mostrar, ao seu público e ao mercado, que você realmente se preocupa com a proteção de dados.

- **NBR ISO/IEC 27002**

Sendo uma das diretrizes mais importantes da família ISO/IEC 27000, a normativa 27002 estabelece boas práticas de gestão de segurança da informação em uma organização. Uma dessas práticas, estabelecida no artigo 7.2.2, é a “conscientização, educação e treinamento em segurança da informação”.

- **Control Objectives for Information and Related Technologies (COBIT)**

Similar à diretriz anterior, trata-se de um framework de boas práticas para a governança de tecnologias da informação, tendo sido criada (e constantemente atualizada) pela (Information Systems Audit and Control Association (Associação de Controle e Auditoria de Sistemas da Informação ou ISACA). Em seu PO 4.4, ele afirma que é necessário “fornecer aos funcionários de TI uma orientação apropriada quando contratados e treinamento contínuo para manter seus conhecimentos, habilidades, controles internos e conscientização de segurança no nível requerido para atingir os objetivos organizacionais.”

- **NIST Cybersecurity Framework Version 1.1**

Criado pelo National Institute of Standards and Technology (Instituto Nacional de Padrões e Tecnologia ou NIST) dos EUA, o Cybersecurity Framework, atualmente em sua versão 1.1, ressalta que, idealmente, “Os funcionários e parceiros da organização são treinados sobre a conscientização sobre segurança cibernética e são treinados para executar suas obrigações e responsabilidades relacionadas à segurança cibernética, de acordo com os procedimentos e acordos relacionados.”

- **Center for Internet Security Critical Security Controls for Effective Cyber Defense (CIS Control)**

Criado pelo Center for Internet Security (Centro de Segurança da Internet ou CIS), a série denominada Controls (Controles), orienta, em sua 17ª diretriz, que "a força de trabalho seja treinada sobre como identificar diferentes formas de ataques de engenharia social, como phishing, golpes telefônicos e personificações telefônicas.”

HACK3R_
RANGER5

PARA PROTEGER A NAÇÃO

Por fim, vale lembrar que foi aprovada, através do decreto 10.222 de 5 de fevereiro de 2020, a **Estratégia Nacional de Segurança Cibernética (E-Ciber)**, que deve ser seguida por todos os órgãos e entidades da administração pública federal.

Em seu capítulo 2.4 (Educação), a norma diz: "recomenda-se desenvolver uma cultura de segurança cibernética, por meio da educação, que alcance todos os setores da sociedade e níveis de ensino, a fim de prevenir incidentes e proporcionar o uso responsável das tecnologias, por ser um dos fatores chaves para o desenvolvimento do País."

HACK3R_
RANGER5

Bibliografia
Regulamentações sobre Conscientização e Treinamento em Segurança (SegInfo, 24 de junho de 2020)