LEIS E NORMAS *QUE EXIGEM* CONSCIENTIZAÇÃO EM CIBERSEGURANÇA

HACK3R_
RANGER5

LGDP (LEI N° 13.709 DE 14 DE AGOSTO DE 2018)

Legislação nacional, informa que, dentre as boas práticas para evitar incidentes cibernéticos, estão as "ações educativas" internas e orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas com relação à proteção de dados pessoais.

GENERAL DATA PROTECTION REGULATION (2016/679)

Legislação europeia, deixa claro que “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.”

CIRCULAR N° 3.909 E RESOLUÇÃO N° 4.658 DO BACEN

Focadas no setor bancário, ambas pedem que a política de segurança da informação circule entre todos os funcionários de instituições financeiras, empresas de pagamentos e bancos, especialmente durante a contratação de fornecedores de cloud computing.

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT, HIPAA

Afirma que é obrigatório para as companhias “implementar um programa de conscientização e treinamento de segurança para todos os membros de sua organização (incluindo a administração).”

AS MULTAS PREVISTAS PELO DESRESPEITO A LEGISLAÇÕES COMO A LGPD E A GDPR VARIAM DE 2% A 4% DO FATURAMENTO ANUAL DA EMPRESA, PODENDO CHEGAR A R$ 50 MILHÕES OU ABSURDOS € 20 MILHÕES. VAI ARRISCAR?

PAYMENT CARD INDUSTRY DATA SECURITY STANDARD (PCI-DSS)

Específica para quem emite cartões de crédito e/ou débito, diz que é crucial implementar "um programa formal de segurança para conscientizar" funcionários.

INSTRUÇÕES N° 505, N° 558 E N° 612 DA CVM

De autoria da Comissão dos Valores Mobiliários, as três instruções pedem a implementação de programas de conscientização para intermediários e administradores de carteiras de valores mobiliários.

CONTROL OBJECTIVES FOR INFORMATION AND RELATED TECHNOLOGIES (COBIT)

Similar à ISO/IEC 27002, afirma que é necessário fornecer aos funcionários "uma orientação apropriada" para manter os níveis de segurança dentro da organização.

NBR ISO/IEC 27002

Um dos mais famosos membros do grupo de diretrizes ISO/IEC 27000, tal documento propõe boas práticas de gestão de segurança da informação e possui um artigo inteiro dedicado à "conscientização, educação e treinamento em segurança da informação."

ESTRATÉGIA NACIONAL DE SEGURANÇA CIBERNÉTICA

Também conhecida como E-Ciber, trata-se de uma diretriz que deve ser seguida por órgãos e entidades governamentais. Em seu capítulo 2.4 (Educação), a norma diz que “recomenda-se desenvolver uma cultura de segurança cibernética, por meio da educação, que alcance todos os setores da sociedade e níveis de ensino."

Bibliografia

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

HACK3R_
RANGER5

TESTE A NOSSA PLATAFORMA GRATUITAMENTE DURANTE 15 DIAS!
HACKERRANGERS.COM.BR