Checklist para validação da segurança de dados ao integrar novos colaboradores

Deu recentemente as boas-vindas a novos colaboradores na sua organização? Se é esse o caso, é fundamental abordar o tema da segurança da informação logo no início do seu trabalho. O erro ou o descuido dos colaboradores é a principal causa de violações e fugas de dados. Uma integração e formação dedicada pode ajudar a mitigar este tipo de risco. Os gestores e as equipas de liderança podem ajudar a construir e a reforçar a cultura de segurança de uma organização, delineando estratégias e garantindo que os colaboradores reconhecem o seu papel na manutenção da segurança dos dados e informação.

SABIA QUE? Quase metade (49%) dos líderes empresariais entrevistados indica que a falta de conhecimento das ameaças e dos riscos para a organização, é a maior barreira para os colaboradores cumprirem as políticas de segurança da informação.1

Utilize esta checklist durante a integração, para verificar os tópicos de segurança da informação, tanto eletrónicos como em suporte papel.

- ☐ **Normas de segurança da informação.**
  As fugas de dados podem resultar em multas e prejudicar a reputação de uma organização. Familiarizar os colaboradores com os principais aspectos das leis de segurança de dados permite enquadrá-lo e desencadeará importantes e produtivas discussões sobre segurança de dados.

- ☐ **Relatórios de incidentes.**
  Apesar de todos os esforços, uma violação de dados pode sempre ocorrer. Para isso, os colaboradores devem saber quando e como relatar essas situações e ter certeza de que não serão penalizados por fazê-lo. Certifique-se de que os novos colaboradores estão informados, desde o início, sobre o funcionamento, circuito e relatório de incidentes, para que novos e antigos colaboradores saibam como reagir se ocorrer uma violação de dados.

- ☐ **Procedimentos para a impressão de documentos.**
  Erros comuns, como deixar documentos confidenciais inadvertidamente expostos em impressoras, aumentam o risco de violações de dados. É vital reforçar a importância de recolha rápida dos documentos impressos da impressora, pois isso pode reduzir a probabilidade de dados roubados. Se utiliza uma senha ou cartão para proteção das impressões, não se esqueça de dar indicações aos novos colaboradores sobre como aceder e preservar a segurança dessas senhas/formas de acesso.

- ☐ **Políticas para dispositivos eletrónicos.**
  Telemóveis pessoais e tablets no local de trabalho podem ser muito convenientes, mas podem também representar um elevado risco de segurança. Ao integrar novos colaboradores, certifique-se de que eles sabem como proteger os seus dispositivos.

Fonte: 1. Relatório de Proteção de Dados da Shred-it, 2021.

Protegemos o que importa.

Shred-it®
Uma Solução Stericycle®

CHECKLIST PARA VALIDAÇÃO DA SEGURANÇA DE DADOS AO INTEGRAR NOVOS COLABORADORES

☐ **Mantendo uma mesa limpa.**
Se a sua empresa tiver uma política "Clear Desk/Clear Screen" ou de mesa limpa/ecrã limpo, deve explicar exatamente o que isso significa aos novos colaboradores. Resumidamente, isso exige que os colaboradores mantenham protegidos todos os seus documentos que contenham informação confidencial; removam de cima da sua mesa de trabalho todos os documentos não essenciais; e bloqueiem o computador antes de abandonar o posto de trabalho por um período longo ou no final do dia.

☐ **Eliminação total de documentos.**
Os novos colaboradores devem saber de forma clara como encaminhar corretamente os documentos da sua organização após deixarem de ser úteis. Informá-los sobre os procedimentos de destruição de documentos pode ajudar a mitigar os riscos e limitar possíveis complicações na proteção de dados. Idealmente a solução seria adoptar uma Política Shred-it All ou de destruição total e aconselhá-los a colocar todos os documentos numa consola segura para garantir a sua destruição segura. Isso eliminará as dúvidas sobre o que pode ser confidencial ou não. E não apenas ajuda na segurança dos documentos confidenciais mas, como todo papel triturado é reciclado, também é uma boa prática em termos de sustentabilidade.

☐ **Protocolos de passwords.**
A gestão de senhas ou passwords é um dos aspectos essenciais na manutenção da segurança da sua organização. Os novos colaboradores devem conhecer a política de senhas/passwords da sua organização e saber como criar senhas fortes. Uma boa senha incorpora letras maiúsculas e minúsculas, números e símbolos e deve ser atualizada regularmente. Se a sua empresa tiver um programa obrigatório de atualização reguar de senhas, certifique-se de que os novos colaboradores o conhecem.

☐ **Cuidados a ter com o e-mail.**
Os incidentes de Cibersegurança normalmente acontecem porque os colaboradores clicam em e-mails que não deviam. Os novos colaboradores devem ser formados sobre como reconhecer e-mails suspeitos, incluindo malware, esquemas de phishing e ransomware, para que possam aprender a evitar situações prejudiciais.

Para saber mais sobre as melhores práticas de segurança da informação, visite o site shredit.pt ou ligue 808 200 246.

Protegemos o que importa.

© 2022 Stericycle, Inc. Todos os direitos reservados.

Shred-it®
Uma Solução Stericycle®