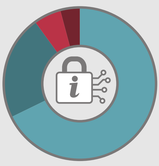
OTRS Spotlight: Corporate Security 2024

Parte 2: Segurança da informação e de dispositivos em risco. Recursos adicionais são necessários.

As soluções ISMS destinam-se a manter as empresas seguras. Muitas equipes já implementaram uma.



- 68 % Usa ativamente
- 22 % Não usa, mas planeja
- 6 % Não usa e não planeja
- 4 % Não sei

Para que um ISMS seja o mais útil possível, uma variedade de ferramentas e processos devem ser integradas. As equipes ainda lutam com isso.

1/3

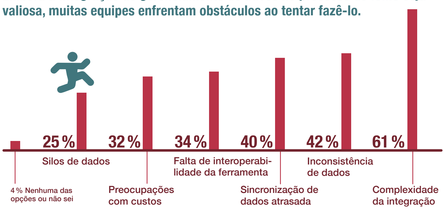
Apenas um terço das ferramentas estão integradas.

35 % Gerenciamento de configuração
34 % Gestão de ativos
34 % Treinamento de conscientização de segurança
34 % Relatórios de auditoria e conformidade
30 % Gerenciamento de patches

Ao integrar o gerenciamento de ativos aos processos do ISMS, as equipes se apoiam fortemente no software existente e nas ferramentas de integração.

- 10 % Usa scripts e APIs personalizados
- 10 % Usa transferência e reconciliação manual de dados
- 3 % Não sei

Embora a integração do gerenciamento de ativos no processo de ISMS seja valiosa, muitas equipes enfrentam obstáculos ao tentar fazê-lo.



O ISMS exige que as equipes implementem e monitorem as configurações. As equipes de TI e segurança enfrentam uma série de obstáculos ao tentar colocar isso em prática.

39 % Equipe ou recursos de TI limitados

33 % Problemas de escalabilidade devido ao número crescente de dispositivos
33 % Diversidade de serviços e sistemas operacionais
32 % Gerenciamento de dispositivos em ambientes de trabalho remotos ou híbridos

À medida que a IA se torna ainda mais popular, o desafio de monitorar as configurações do sistema aumenta. As equipes devem tomar medidas para evitar riscos de segurança.

87 %

Estão usando dispositivos habilitados para IA e tomam medidas para gerenciar riscos e conformidade.

7 % No momento, não estão usando dispositivos habilitados para IA.

5 % Estão usando dispositivos habilitados para IA e atualmente não estão tomando medidas para gerenciar riscos e conformidade.

1 % Não sei.

As equipes de TI avançaram em termos de conscientização de segurança por parte dos usuários finais. No entanto, isso significa que mais e mais perguntas começam a surgir.

45 % Preocupações com e-mails suspeitos ou possíveis tentativas de phishing
38 % Perguntas sobre a legitimidade de downloads, atualizações de software ou aplicativos
36 % Preocupações com a segurança dos dispositivos pessoais usados para o trabalho
34 % Notificações sobre segurança, privacidade e riscos potenciais para ferramentas e serviços de IA
32 % Problemas com login ou acesso seguro aos sistemas
26 % Relatar dispositivos perdidos ou roubados contendo dados confidenciais

Apesar da crescente conscientização sobre os riscos de segurança, as empresas devem permanecer vigilantes.

As empresas devem concentrar suas atenções e recursos no suporte às equipes de TI com metas de segurança da informação, incluindo a implementação de melhores ferramentas para gerenciamento de ativos e a busca de oportunidades de integração.

38 % Vulnerabilidades ou arquivos corrompidos em sistemas e dispositivos corporativos

38 % Vulnerabilidades, violações de dados ou uso indevido de ferramentas e serviços de IA

37 % Dispositivos perdidos ou roubados contendo dados confidenciais

36 % E-mails de phishing

35 % Downloads ou atualizações não autorizados de software ou aplicativos em dispositivos corporativos

32 % Problemas de bloqueio de conta ou acesso não seguro

30 % Funcionários que não mantêm seus dispositivos atualizados

29 % Dispositivos pessoais usados para o trabalho

Os dados usados são baseados em uma pesquisa online realizada pela Pollfish, Inc. em nome da OTRS AG, na qual 476 profissionais de TI e segurança cibernética nos EUA, Alemanha, Brasil, México, Austrália e Malásia participaram entre 22 de agosto e 17 de setembro de 2024. Salvo indicação em contrário, todos os valores referem-se às médias de todos os países pesquisados.

OTRS