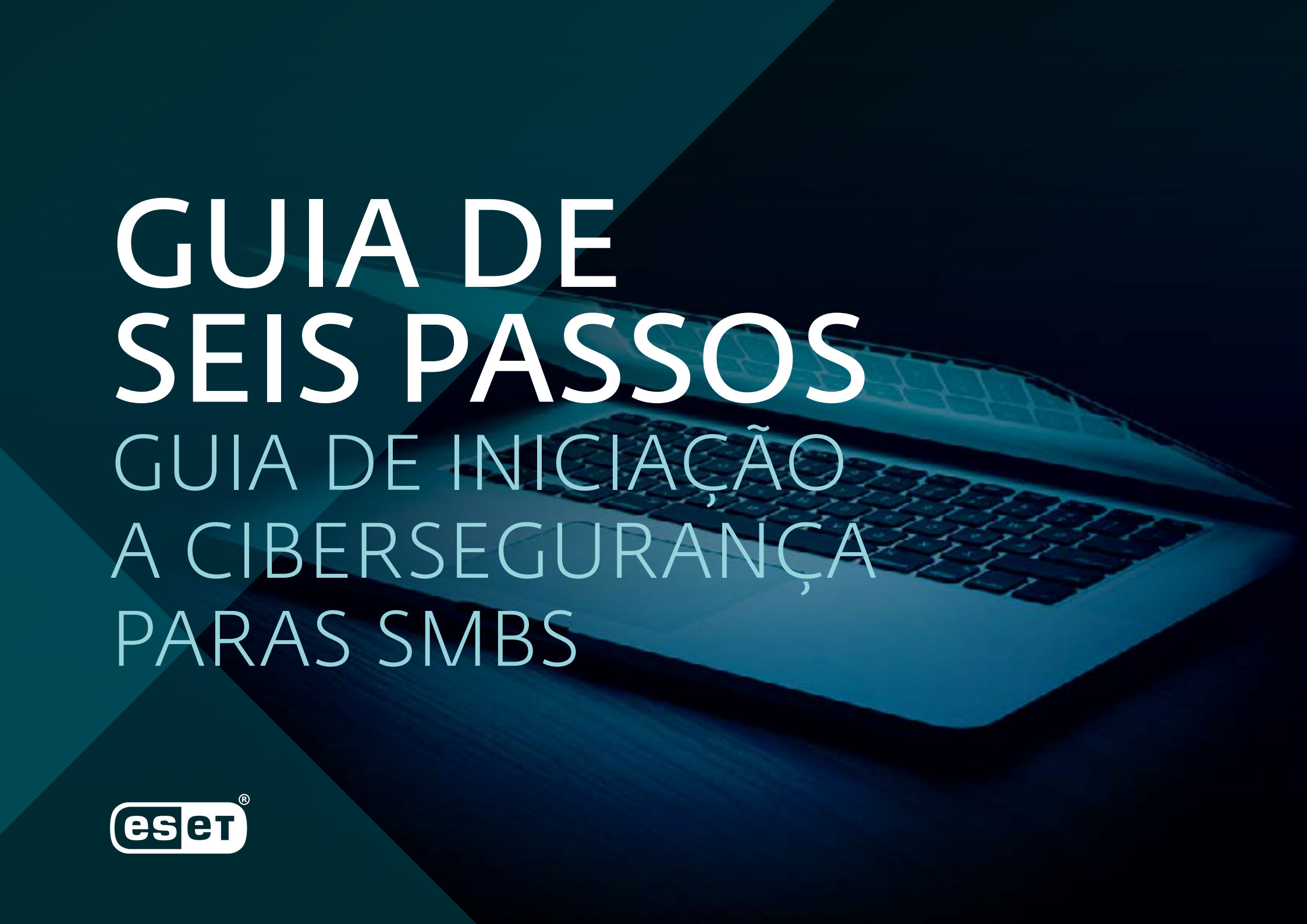


GUIA DE SEIS PASSOS

GUIA DE INICIAÇÃO A CIBERSEGURANÇA PARAS SMBS

SEIS PASSOS DE CIBERSEGURANÇA GUIA DE INICIAÇÃO PARA SMB

Os dispositivos e a internet trazem diversos benefícios às pequenas empresas. No entanto, não se trata de uma tecnologia isenta de riscos. Alguns desses riscos, como roubos físicos ou desastres naturais, podem ser reduzidos ou controlados por meio de condutas e precauções sensatas. Os riscos de cibercrime são os mais difíceis de lidar, como os que se caracterizam pelo roubo de informações por parte de invasores, que as vendem no mercado clandestino.

63% das pequenas e médias empresas sofreram uma violação de dados em 2019, mas muitos de seus proprietários acreditam não serem vulneráveis aos ataques cibernéticos, devido à pequena dimensão da empresa e seus ativos limitados. Infelizmente, não é essa a realidade.

Esse guia auxiliará na defesa da sua empresa contra ameaças cibernéticas.

Informações pessoais são um alvo comum de invasores. Mesmo no caso de empresas menores, é provável que lidem com alguns dados pessoais de clientes ou fornecedores, de interesse do invasor. Outro alvo comum de cibercriminosos são informações de conta, incluindo dados de cartão de crédito, números de contas bancárias, senhas de bancos on-line, contas de e-mail e credenciais de usuário para serviços como eBay, PayPal e TurboTax.

Tudo isso pode ser vendido no mercado clandestino, para outros criminosos especializados no uso de informações em uma ampla variedade de esquemas de golpes e fraudes.

dos ataques cibernéticos visam pequenas empresas

pequenas e médias empresas tiveram oito ou mais horas de inatividade devido a violações cibernéticas

Fuente: Agility SMB

CONSEQUÊNCIAS DO ROUBO DE DADOS

Visto que a maioria das pequenas empresas possui informações de conta e dados pessoais de que os criminosos podem se aproveitar, cabe lembrar que a sua empresa pode ser responsabilizada pelas consequências do roubo de dados — por exemplo, no caso de as informações sobre seus clientes serem roubadas e utilizadas em fraudes.

Alguns dados são protegidos por leis e regulamentos, como o Regulamento Geral de Proteção de Dados **(GDPR) da União Europeia ou a Lei de Privacidade do Consumidor da Califórnia (CCPA) da Califórnia, Estados Unidos**. Diversos estados dos Estados Unidos também exigem que as empresas relatem violações de segurança que expõem dados pessoais a potenciais invasões, como um laptop perdido, contendo detalhes do cliente, ou um pen drive com histórico médico.

Isso significa que, mesmo que sua empresa ainda seja pequena, deve-se adotar uma **abordagem sistêmica para a proteção de quaisquer dados** que lhe são confiados. À medida que realiza a tarefa de proteger os ativos digitais da sua empresa, registre a abordagem adotada. Isso auxiliará a **instruir os funcionários** sobre suas responsabilidades de segurança. Além disso, não é raro que grandes empresas exijam que fornecedores e contratados comprovem o conhecimento de seus funcionários sobre segurança,

bem como a implementação de medidas de segurança adequadas. Caso ocorra uma violação de segurança, uma política de segurança registrada auxilia na comprovação da dedicação e esforços da sua empresa com relação à proteção das informações.

Um terço dos custos relacionados a uma violação de dados são percebidos mais de um ano após o incidente.

Cerca de 22% desses custos ocorrem no segundo ano.

Fuente: ENISA

PASSO A PASSO:

Delineamos uma abordagem sistêmica para segurança cibernética em alguns passos.

- **A**valiar seus ativos, riscos e recursos;
- Em**B**asar sua política;
- Es**C**olher seus métodos de controle;
- A**D**otar esses controles
- **E**ducar funcionários, executivos e fornecedores
- **F**ornecer análises adicionais, auditorias e testes

AVALIE SEUS ATIVOS, RISCOS E RECURSOS

AVALIE SEUS ATIVOS, RISCOS E RECURSOS

Faça uma lista de todos os sistemas e serviços digitais utilizados pela sua empresa. É preciso saber o que se usa para conseguir proteger-se. Certifique-se de incluir dispositivos móveis, como smartphones e tablets, pelos quais a empresa e/ou funcionários acessam informações da empresa ou de clientes.

Essa análise é essencial, **pois 62% dos 1.100 profissionais** afirmaram ter alterado sua segurança móvel por questões de eficiência[1].

Além disso, serviços on-line, como Salesforce, sites de bancos digitais e serviços de nuvem, como iCloud ou Google Docs também devem ser considerados.

Depois disso, com a listagem completa em mãos, considere os riscos relacionados a cada item. Quem ou qual é a ameaça? Quais são os riscos relacionados ao trabalho remoto? Outra pergunta relevante é: **O que pode ser um risco em potencial?** Alguns riscos são mais prováveis do que outros, mas liste todos eles. Em seguida, classifique-os de acordo com o potencial dano e as chances de que ocorram.

Também é possível buscar ajuda externa para esse processo, por isso, faça uma outra lista com os **recursos que podem ser empregados para questões de segurança cibernética**. Conte com especialistas em segurança cibernética, partners ou fornecedores. A terceirização de sua segurança cibernética, ou parte dela, para provedores de serviços gerenciados (MSP) é outra opção, que fornecerá o suporte necessário em todos os momentos.

62%

dos profissionais reiterou alterar a segurança móvel por questão de eficiência

1) Fonte: Cyber Talk, março de 2020

EMBASE SUA POLÍTICA

CONSTRUA SUA POLÍTICA

Um programa de segurança sólido começa na política empregada, que inicia com a **adesão de nível C**. Caso você seja responsável pelo processo, explique em detalhes a todos os envolvidos a seriedade da questão de segurança cibernética e o comprometimento da empresa com a proteção da privacidade e segurança de todos os dados em seu domínio.

Em seguida, defina as políticas que serão aplicadas, como a proibição de **acesso não autorizado a sistemas e dados da empresa** e o não acesso de funcionários às configurações de segurança em seus dispositivos móveis, que não devem ser desativadas.

Deve-se definir quem pode acessar determinados dados na organização, para quais finalidades e quais ações estão autorizadas com esses dados. Também é importante estabelecer políticas de acesso remoto, como "traga o seu próprio dispositivo" (bring your own device, BYOD) ou software autorizado.

ESCOLHA SEUS MÉTODOS DE CONTROLE

ESCOLHA SEUS MÉTODOS DE CONTROLE

Utilizam-se métodos de controle para a aplicação de políticas. Por exemplo, para aplicar a política de acesso não autorizado aos sistemas e dados da empresa, pode-se optar pelo controle de todo o acesso aos sistemas da empresa, com um nome de usuário único, senha e alguma forma de **autenticação de dois fatores**.

Para controlar **quais programas têm permissão** de uso nos computadores da empresa, pode-se optar por não conceder **permissão administrativa** aos funcionários. Para evitar violações causadas por roubo ou perda de dispositivos móveis, os funcionários podem ter como regra relatar os incidentes no mesmo dia — com a determinação de que esses dispositivos serão bloqueados remotamente e deletados imediatamente.

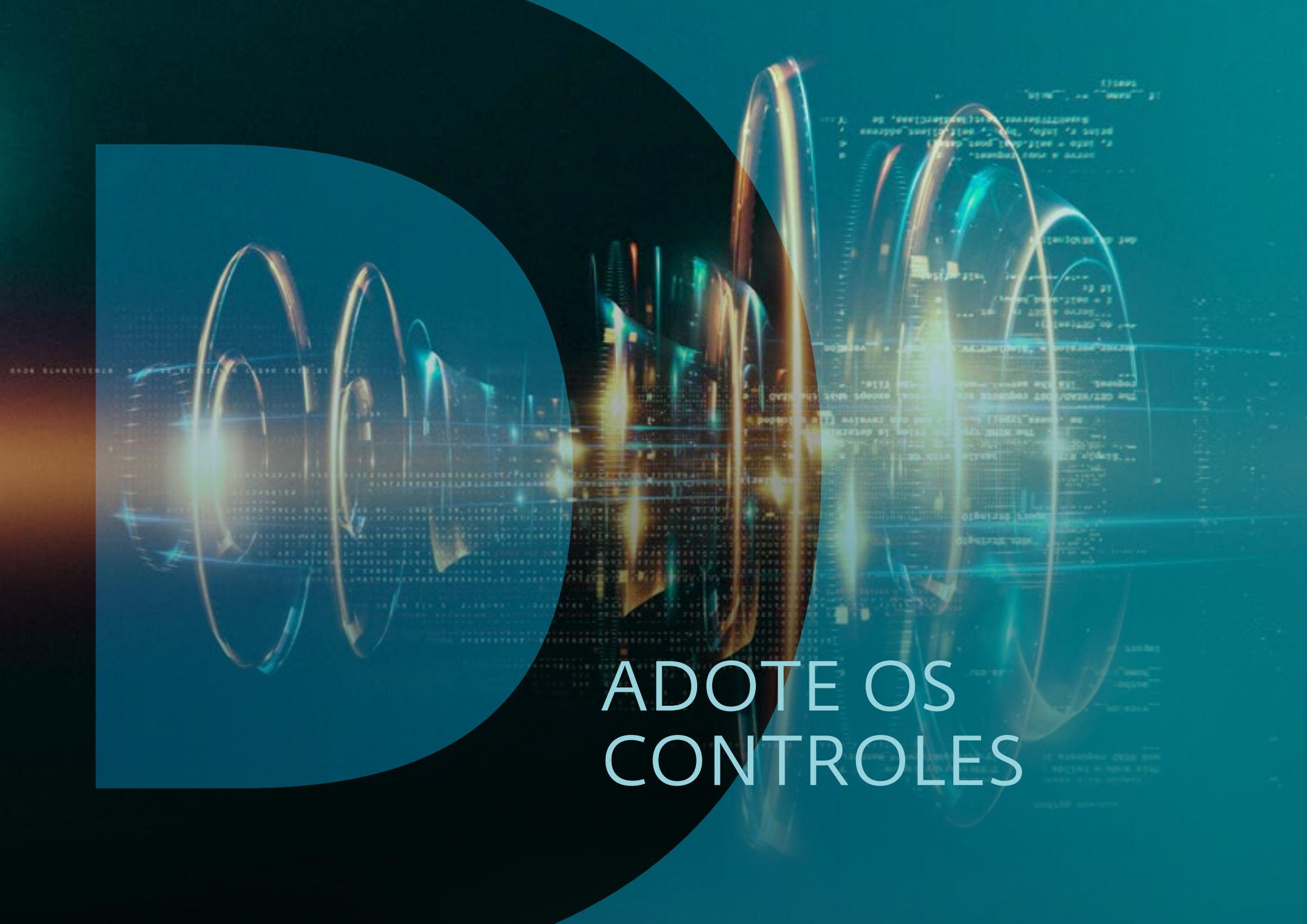
No mínimo, considere empregar as seguintes tecnologias de segurança:

- **Soluções de proteção de endpoint,** que impedirão que códigos maliciosos sejam baixados em seus dispositivos.
- **Software de criptografia,** que deixará inacessíveis os dados em dispositivos roubados, o que também é proposto pela GDPR da União Europeia.
- **Um sistema de autenticação de dois fatores,** de modo a contar com proteção adicional, para além de apenas um nome de usuário e senha ao obter acesso aos seus sistemas e dados.
- **Uma solução de VPN,** que adicionará uma camada extra de proteção para funcionários trabalhando de forma remota.Europeia.

A segurança cibernética da sua empresa pronta para o futuro

O cenário de segurança cibernética atual está em constante evolução com o uso de técnicas sofisticadas de ofuscação. O objetivo final dos agentes de malware é permanecerem despercebidos nos endpoints, evitando a detecção por antimalwares e criando ameaças até então desconhecidas, ou ataques de dia zero.

Um sandbox de segurança baseado em nuvem oferece uma camada defensiva fora da rede da empresa, evitando que ransomwares sejam executados em um ambiente de produção. O arquivo suspeito tem a execução nos endpoints bloqueada.



ADOTE OS CONTROLES

ADOTE OS CONTROLES

Ao implantar os controles, certifique-se de que eles funcionam. Por exemplo, você precisa ter uma política que não permita softwares não autorizados nos sistemas da empresa; um de seus controles será um **software antimalwares**, que verifica a existência decódigos maliciosos.

É necessário não apenas instalar e testar se o controle não interferirá nas operações normais da empresa, como também documentar os procedimentos a serem seguidos pelos funcionários assim que um código malicioso for detectado.

Ao escolher a solução de proteção de endpoints correta, algumas considerações importantes também devem ser observadas. Por exemplo, o objetivo é possuir a**s mais altas taxas de detecção possíveis**, ao passo que a incidência de falsos positivos (alertas sobre arquivos ou links que não sejam, de fato, maliciosos) deve ser a mínima possível. Além disso, **não deve haver impacto perceptível no desempenho do sistema** e o gerenciamento e a manutenção devem ser processos fáceis.

Console de gerenciamento de segurança para endpoints

Ao implantar a proteção para endpoints, busque uma visão geral de todos os seus endpoints em um único painel de controle. Um console baseado em nuvem, como o ESET PROTECT, oferece essa funcionalidade.

Ele garante visibilidade em tempo real para endpoints locais e externos, bem como relatórios completos e gerenciamento de segurança para todos os sistemas operacionais.

Também controla a prevenção, detecção e resposta de endpoints em todas as plataformas — abrangendo desktops, servidores, dispositivos virtuais e, até mesmo, dispositivos móveis gerenciados.

SAIBA MAIS


EDUQUE
AS PARTES
ENVOLVIDAS

EDUQUE FUNCIONÁRIOS, EXECUTIVOS E FORNECEDORES

Seus funcionários precisam conhecer mais do que apenas as políticas e procedimentos de segurança da empresa. É essencial que entendam por que elas são necessárias. Isso significa **investir na conscientização e instrução sobre segurança cibernética**, o que, em geral, é a medida de segurança mais eficaz que podemos implementar.

Ao trabalhar com a sua equipe, você pode promover a conscientização sobre problemas como os e-mails de phishing. Um estudo demonstrou que 43% dos funcionários não sabem ao certo o que é um ataque de phishing[2].

Nesse sentido, prepare um treinamento regular para seus funcionários: por exemplo, um quiz sobre phishing, a fim de instruí-los sobre quais técnicas estão sendo empregadas por agentes maliciosos. Torne a conscientização sobre segurança cibernética parte do processo de integração e forneça dicas de segurança em uma página da intranet.

Certifique-se de instruir todos que têm acesso aos seus sistemas, incluindo executivos, fornecedores e partners. Ressalte **que violações das políticas de segurança acarretam consequências**. A falha na aplicação das políticas prejudica todo o esforço de segurança de uma organização.

69%

das organizações foram violadas devido a uma ameaça interna, apesar das medidas preventivas adotadas[3]

2) Fuente: ZD Net, octubre de 2020
3) Fuente: Sapio Research Study, Reino Unido

FORNEÇA ANÁLISES ADICIONAIS, AUDITORIAS E TESTES

FORNEÇA ANÁLISES ADICIONAIS, AUDITORIAS E TESTES

Para qualquer empresa, seja grande ou pequena, a segurança cibernética é um processo contínuo, não um projeto único. É preciso planejar a **reavaliação da sua segurança periodicamente**, ao menos uma vez por ano.

Atualize as políticas e controles de segurança mais de uma vez por ano, dependendo das mudanças na empresa, como **novas relações com fornecedores, novos projetos, novas contratações ou saída de funcionários** (certificando-se de que todo o acesso ao sistema seja cessado sempre que alguém encerra suas atividades na empresa). Considere contratar um consultor externo para **realizar testes de intrusão e auditorias de segurança**, a fim de descobrir quais são os pontos fracos e trabalhar na sua otimização.

A onda atual de cibercrimes não terminará tão cedo, por isso, é necessário um esforço permanente para proteger dados e sistemas, que caracterizam a força fundamental das pequenas empresas de hoje.

IPara receber as últimas atualizações sobre as ameaças emergentes, acompanhe as notícias de segurança regularmente, inscrevendo-se em sites como:

WeLiveSecurity.com/latam

DataSecurityGuide.eset.com

Há mais de 30 anos, a ESET® vem desenvolvendo softwares e serviços de segurança líderes na indústria, para empresas e consumidores em todo o mundo. Com soluções de segurança que variam de endpoints e defesa de dispositivos móveis à criptografia e autenticação de dois fatores, os produtos ESET, com alto desempenho e de fácil uso, oferecem aos usuários e empresas a tranquilidade necessária para aproveitar todo o potencial da sua tecnologia. A ESET protege e monitora de forma discreta diariamente, 24h por dia, atualizando as defesas em tempo real para manter a segurança dos usuários e o funcionamento das empresas sem interrupções. Para mais informações, acesse www.eset.com.