PROTEGENDO INFORMAÇÕES DIGITAIS

Como você está mantendo sua empresa e seus clientes seguros?

Confira!

AS INFORMAÇÕES DIGITAIS SÃO HOJE A FORÇA VITAL DE QUALQUER EMPRESA

Escritórios sem papel se tornaram a norma em todos os setores, e o trabalho remoto depende da capacidade de compartilhar informações eletrônicas para comunicação, anúncios e colaboração.

As informações digitais devem ser adequadamente protegidas em todos os dispositivos usados na empresa, seja no acesso a esses dados, na transmissão ou no armazenamento. O checklist preparado pela ISH fornece uma estratégia para implementar a máxima proteção de segurança para suas informações digitais.

PARA UTILIZAR DE FORMA EFICAZ ESTE CHECKLIST, CLASSIFIQUE AS INFORMAÇÕES EM QUATRO CATEGORIAS

Público

Todos os colaboradores e indivíduos externos podem acessar essas informações. Essas informações digitais costumam ser muito genéricas e não representam risco para a empresa; por exemplo, um comunicado de imprensa descrevendo as características de um novo produto.

Interno

Informações de toda a empresa que são acessíveis apenas aos colaboradores. Essas informações digitais podem incluir um manual do colaborador, políticas operacionais e anúncios destinados apenas a usuários internos.

Confidencial

As informações digitais confidenciais são baseadas em uma abordagem de acesso de equipe e os exemplos podem incluir detalhes do projeto, informações pessoais de contato, valores financeiros ou metas de final de ano.

Restrito

Apenas indivíduos específicos, como executivos C-level, gerentes de negócios ou analistas financeiros, devem ter acesso a essas informações digitais. Isso pode envolver segredos comerciais, dados do titular do cartão ou planos de preços de produtos que estão em desenvolvimento.

OS ESPECIALISTAS EM SEGURANÇA DA ISH CRIARAM ESSE CHECKLIST PARA A PROTEÇÃO CIBERNÉTICA DE INDIVÍDUOS OU EMPRESAS

Você pode usar o checklist de duas maneiras:

OPÇÃO 1

Marque as caixas para respostas SIM e calcule seus pontos.

A melhor pontuação é 400. Uma pontuação abaixo de 380, ou várias marcas de verificação ausentes, indicam a necessidade de melhorias na área de segurança.

OPÇÃO 2

Use esta avaliação como um guia geral para sua equipe e sua equipe/provedor de TI. Não se preocupe com os pontos, apenas fique protegido!

PRÁTICAS RECOMENDADAS GERAIS

( ) Você tem uma política bem documentada para todos os itens a seguir? Uso aceitável, acesso à Internet, acesso remoto e BYOD (traga seu próprio dispositivo), e-mail e comunicações, recuperação de desastres, criptografia e privacidade **(10 pontos por item)**.

( ) Você usa software moderno, válido e atualizado para todos os fins e aplica patches de segurança regularmente? **(70 pontos)**.

( ) Você realiza treinamento regular de colaboradores que abrange o que há de mais recente em segurança de dados? **(70 pontos)**.

SEGURANÇA DO USUÁRIO

(10 pontos por item)

( ) As senhas de colaboradores são complexas e atualizadas regularmente?

( ) Você precisa de senhas de colaboradores complexas e atualizadas regularmente?

( ) Você audita e desativa regularmente contas desatualizadas?

( ) Você evita contas e senhas compartilhadas?

( ) Você indica a criação de senhas fortes e diferentes para cada login e site?

( ) Os colaboradores verificam se todos os sites são seguros (https://) ao compartilhar informações ou senhas da empresa?

SEGURANÇA DO E-MAIL

(10 pontos por item)

( ) Você tem uma solução de filtragem de segurança de e-mail? As soluções de filtragem protegem contra e-mails maliciosos que você não consegue reconhecer.

( ) Sua política de e-mail determina que informações confidenciais não serão enviadas por e-mail? Por exemplo, senhas, dados bancários e pessoais.

( ) Os colaboradores conseguem distinguir um e-mail de um golpe de phishing?

SEGURANÇA DO SITE

(10 pontos por item)

( ) Seu certificado SSL está atualizado?

( ) Você usa uma empresa de hospedagem segura na web? Eles devem isolar as contas de hospedagem, manter os logs do servidor e fazer backup do seu site regularmente.

SEGURANÇA DE REDE

(10 pontos por item)

( ) Você usa um firewall de nível comercial?

( ) Você protege seu roteador com senha e torna o Wi-Fi interno acessível apenas aos colaboradores? (Configure as redes de convidados separadamente).

( ) Você usa a tecnologia VPN (rede privada virtual) para acesso remoto ao escritório?

( ) Os computadores de trabalho bloqueiam automaticamente a tela e exigem login novamente após um período de inatividade?

( ) Você limita e registra o acesso aos locais físicos ou salas que contêm dispositivos de rede (como switches) e quaisquer servidores internos?

( ) Você armazena dados com segurança no software em nuvem, usando as melhores práticas de senha para acessar esses dados?

PERGUNTE AO ESPECIALISTA DE TI EM SUA EMPRESA

(10 pontos por item)

( ) Seus firewalls estão executando o firmware mais atual, considerado hardware de última geração e coberto pela garantia do fabricante ou pelo suporte contratado pelo fabricante?

( ) Você verifica regularmente sua rede em busca de vulnerabilidades? Por exemplo, vírus, malware e dispositivos não autorizados.

( ) Você armazena senhas como valores criptografados?

( ) Você realiza backups regulares de dados e configurações, bem como restauração de teste?

QUAL O SEU TOTAL? AVALIE OS SEUS PONTOS.

A melhor pontuação é **400**. Uma pontuação abaixo de **380**, ou várias marcas de verificação ausentes, indicam a necessidade de melhorias na área de segurança.

A TRANSFORMAÇÃO DIGITAL, O CRESCIMENTO DE DISPOSITIVOS E REDES CONECTADAS AUMENTAM A SUPERFÍCIE DE ATAQUE CORPORATIVO

Cada dispositivo conectado à sua rede para acessar ou transferir dados é um possível alvo. Proteger um ecossistema de TI tão distribuído requer uma solução de segurança que possa fechar lacunas e ajudá-lo a ficar à frente de ataques cibernéticos.

Os componentes essenciais para uma empresa segura incluem:

Visibilidade e Detecção de Rede

Vulnerabilidades de software e pontos cegos de rede são desafios de segurança comuns que se tornam ainda mais difíceis conforme as empresas implementam a transformação digital. Reduzir esses pontos críticos à medida que sua superfície de ataque se expande requer o controle sobre todo o tráfego, bem como a capacidade de monitorar dispositivos ou usuários não autorizados que solicitam acesso à rede.

Gerenciamento centralizado de políticas

As redes corporativas de hoje são altamente distribuídas, tornando mais fácil para ataques cibernéticos passarem despercebidos. Os ataques geralmente acontecem por meio de dispositivos não autorizados de colaboradores conectados a redes corporativas ou por meio de acessos à aplicativos e dados em Wi-Fi não seguro. Os recursos de controle de políticas e acesso em camadas ajudam as empresas a gerenciar e unificar centralmente as políticas de acesso à rede para todos os usuários, dispositivos e redes, incluindo conexões com fio, sem fio e VPN. Além de atender a requisitos de negócio e legislações específicas, a exemplo da LGPD. Isso garante que apenas dispositivos e usuários autorizados possam se conectar, forçando a verificação da identidade do usuário e do dispositivo para proteger melhor as redes.

Segmentação

Quanto mais tempo demorar para detectar um ataque cibernético, maior poderá ser o dano e o impacto. Depois que a entrada na rede é obtida, os ataques cibernéticos se movem lateralmente nas zonas confiáveis para evitar a detecção, espalhando-se pela empresa para comprometer dados e sistemas. A segmentação baseada em intenção mitiga esse risco dividindo a rede em zonas para evitar movimentos laterais. Depois que a segmentação for implementada com base em classificações de dados e processos, as equipes de segurança podem revisar continuamente os controles e monitorar atividades incomuns. Os controles de segurança e a tecnologia são perecíveis, por isso é importante avaliar continuamente as políticas de segurança.

ESTRADA PARA O FUTURO

Sobre a **ISH**

Nós cuidamos da **segurança digital** da sua empresa para que você **foque no crescimento do seu negócio**

Use inteligência em tempo real para identificar e corrigir vulnerabilidades.

ACESSE

ISH.COM.BR/

EMPRESA CERTIFICADA

ISO9001 | ISO20000 | ISO27001