ENJOY SAFER TECHNOLOGY™

GUIA DO

Funcionário Seguro

Introdução

Ano a ano, a Segurança da Informação nas empresas ganha cada vez mais importância e, em condições ideias, é responsabilidade propriamente da área de Segurança - em grandes organizações -, ainda que em função das características de cada uma, pode depender de outras áreas, como TI ou Operações.

Em um ambiente onde novas ameaças e vulnerabilidades são identificadas diariamente, os riscos de segurança são cada vez mais dinâmicos.

Por isso, independentemente da área que dependa, proteger a informação é uma tarefa que envolve toda a empresa, já que todos os funcionários interatuam com ela.

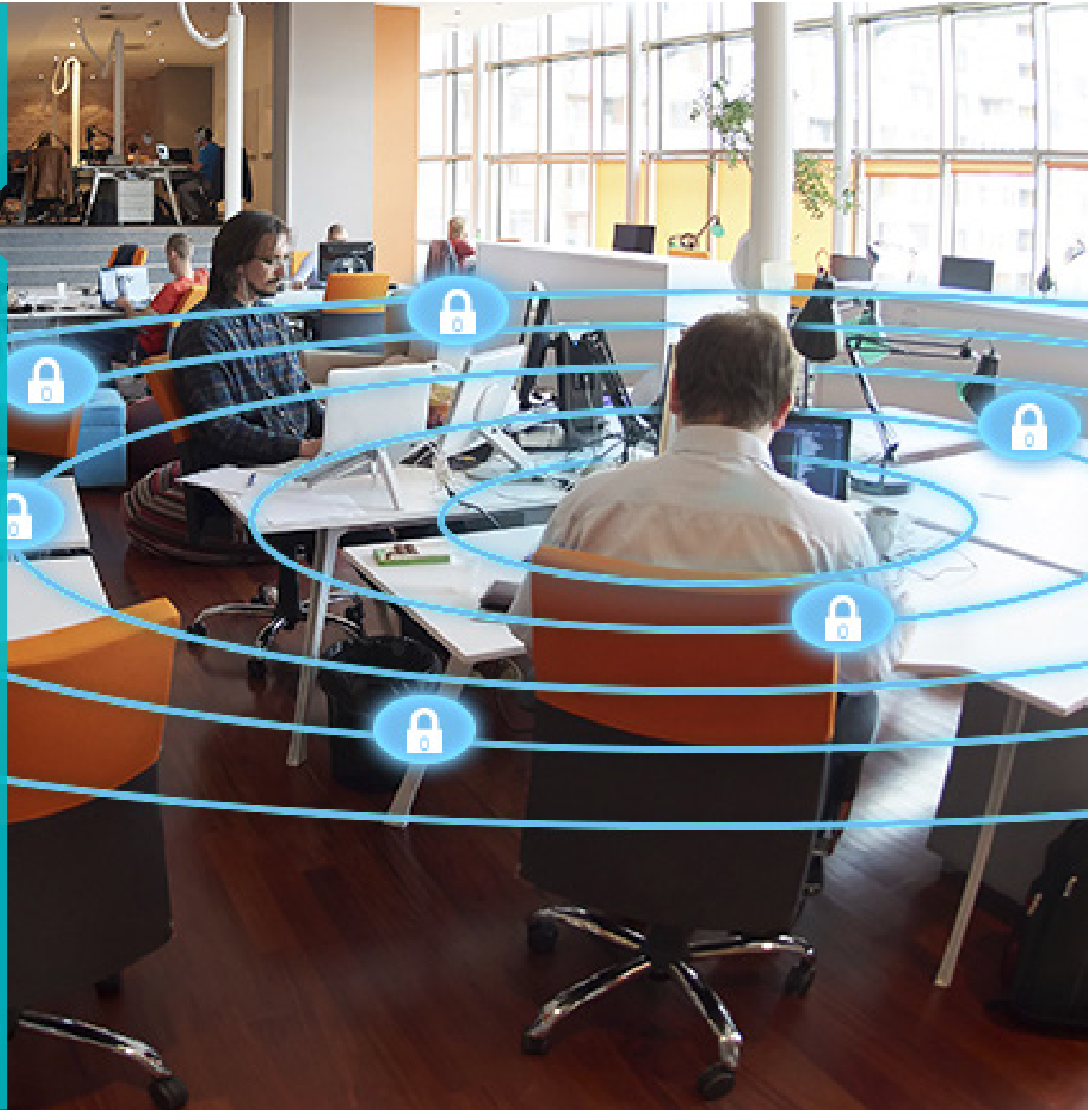
Índice

Funcionário Seguro

Um empregado seguro é aqueleque sabe administrar e utilizar os recursos da empresa de maneira consciente e responsável.

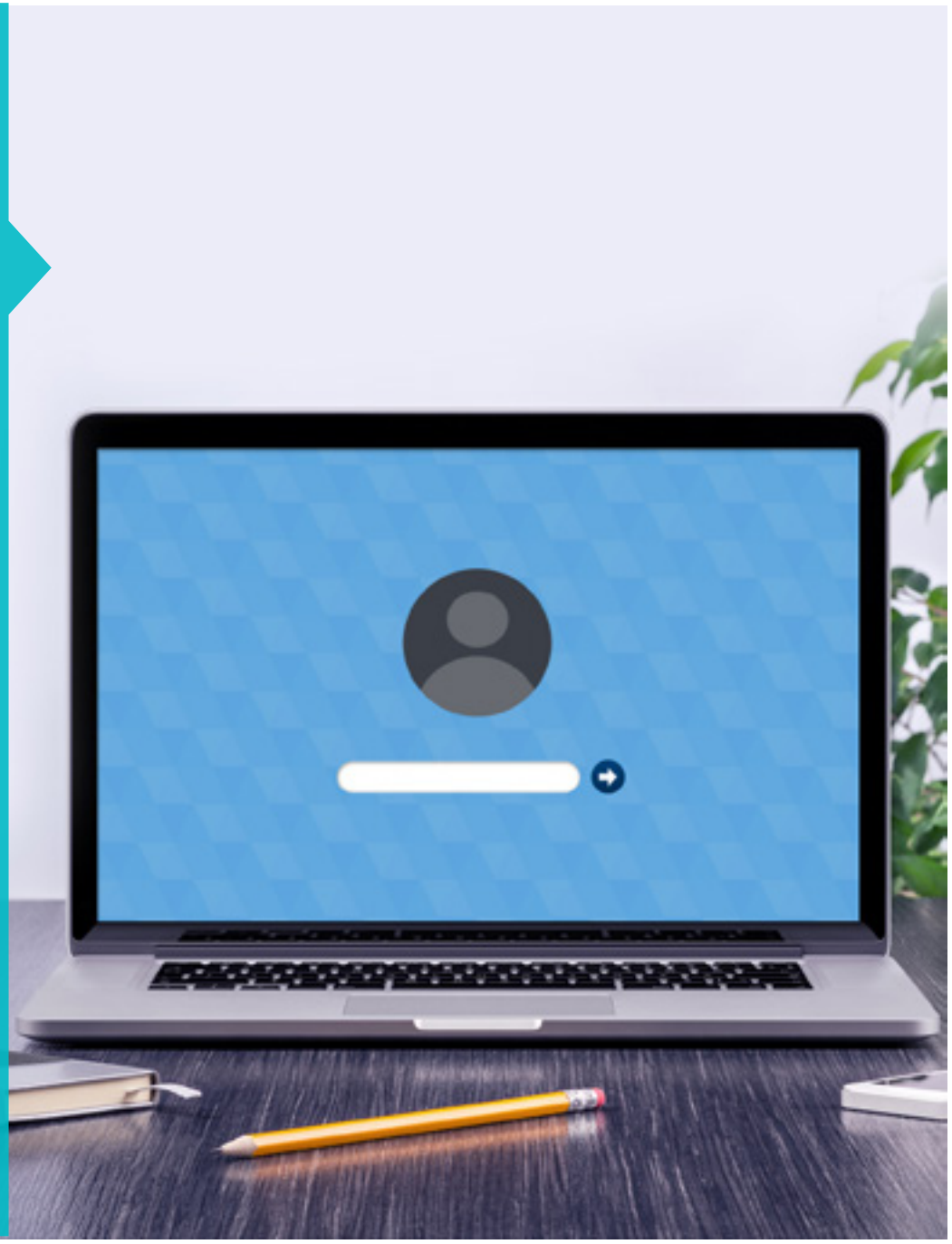
Por isso, este guia possui o objetivo de proporcionar a informação necessária para que cada integrante de uma organização possa se tornar um funcionário seguro e atento sobre o panorama de ameaças para não colocar o negócio em risco.

Neste contexto, serão abordadas as problemáticas mais comuns, as principais ameaças e as melhores práticas para administrar informações sensíveis para as empresas.



Segurança da informação: definições e problemáticas

- Segurança
- Informação
- Segurança da Informação
- As propriedades da informação
- Vulnerabilidade, ameaça e ataque
- Risco, probabilidade e impacto



Segurança da informação: definições e problemáticas

Segurança

De acordo com o dicionário da língua portuguesa, "segurança" se define como "condição de estado que está livre de danos ou riscos", no entanto, trata-se de uma condição idealizada, já que não é possível ter a certeza de que todos os perigos foram evitados.

Por esse motivo, o propósito da segurança em todos os seus âmbitos de aplicação é reduzir riscos até um nível considerado aceitável. Em um sentido mais amplo, a segurança também compreende todas as atividades que possuem o objetivo de proteger uma pessoa ou objeto de algum tipo de perigo.

Informação

A informação é um **ativo** que, igual outros ativos importantes, deve ser protegida. Nas empresas é essencial no momento de tomar decisões, conquistar objetivos e o cumprimento de sua missão.

A informação pode ser encontrada de diferentes maneiras e formatos: digital, escrita, impressa e/ou não representada, como podem ser ideias ou o conhecimento das pessoas. Além do formato em que se encontra a informação, é necessário implementar medidas de segurança para protegê-la em função de sua criticidade, sensibilidade e importância.

Segurança da Informação

Através da combinação dos conceitos anteriores, surge a Segurança da Informação, uma disciplina que se sustenta com metodologias, normas, técnicas, ferramentas, estruturas organizacionais, tecnologia e outros elementos, com a ideia de proteger a informação em todos os seus formatos.

A segurança busca preservar a integridade, disponibilidade e confidencialidade da informação da empresa, com o objetivo de, primordialmente, proteger o negócio.

As propriedades da informação

Confidencialidade: que a informação seja acessível unicamente pelo indivíduos ou processos que possuem os privilégios de autorização para isso.
Por exemplo, que um usuário não possa acessar a base de dados de um servidor.

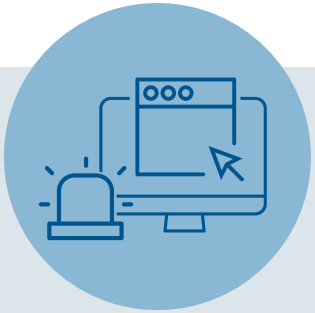
Integridade: que a informação mantenha sua exatidão e completude.
Por exemplo, que um atacante não possa modificar preços de venda de um site.

Disponibilidade: que a informação seja acessível e utilizável quando alguém autorizado necessite.
Por exemplo, evitar problemas em um servidor que causem a exclusão de informações.

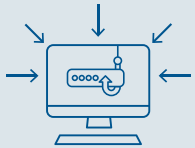
Vulnerabilidade, ameaça e ataque

A Segurança da Informação também implica a consideração de uma ampla gama de riscos, já que continuamente são os obstáculos que bloqueiam as organizações na busca e alcance dos objetivos do negócio.

Portanto, existe uma tentativa de minimizar o impacto causado por incidentes de segurança relacionados com as vulnerabilidades (agentes internos) e ameaças (agentes externos). Esses riscos também podem surgir a partir de situações intencionais ou acidentais.



INTERNO



EXTERNO

INTENCIONAL

Um funcionário descontente destrói um documento e informações importantes.

Um atacante acessa a base de dados do site de empresas de forma externa.

ACIDENTAL

Um funcionário perde um dispositivo USB em que se transportava informação confidencial da empresa.

O aumento nas visitas a um site excede a capacidade de processamento do servidor e se bloqueia.

Como foi visto anteriormente, os problemas de segurança se relacionam com os conceitos de vulnerabilidade, ameaça e ataque:

- **Vulnerabilidade:** fragilidade em um ativo ou controle que pode ser aproveitado por um ou mais agentes externos.
- **Ameaça:** causa potencial de um incidente não desejado que pode resultar em danos a um sistema ou organização.
- **Ataque:** tentativa de destruir, expor, alterar, inutilizar, roubar, obter acesso não autorizado ou fazer uso da fragilidade dos ativos.

Os ataques que buscam comprometer um sistema de informação e os ativos se classificam em quatro categorias segundo sua manifestação: intercepção, modificação, interrupção e fabricação.

A intercepção ameaça a confidencialidade; a modificação atenta contra a integridade; enquanto que a interrupção faz o mesmo com a disponibilidade.

Os ataques de fabricação buscam causar danos à autenticidade daqueles que interatuam com a informação.

Risco, probabilidade e impacto

Através da aplicação de medidas de segurança tentamos mitigar riscos, de maneira que a realização de um ataque seja imprática, não viável ou com as consequências mínimas aceitáveis.

Portanto, a ideia inicial da segurança volta a ter relevância dado que, ainda que não se possa garantir por completo, os riscos devem ser tratados e reduzidos até um nível que não representem consequências consideráveis.

Para a Segurança da Informação, os riscos estão associados à possibilidade de uma ameaça que seja capaz de explorar uma ou mais vulnerabilidades de um ativo ou grupo deles, tendo como consequência um dano à organização.

Os riscos geralmente são expressados mediante a combinação de **probabilidade** de que um evento não desejado aconteça e suas consequências ou **impacto**. Por esse motivo, as medidas de segurança visam reduzir algumas dessas variáveis ou, no melhor dos casos, ambas.

Ameaças comuns contra a informação

- Engenharia Social
- Malware
- Phishing
- Roubo e exposição de informação

Ameaças comuns contra a informação

Engenharia Social

É a utilização de habilidades sociais para manipular ações de uma pessoa. A partir dessas técnicas, os cibercriminosos enganam usuários para comprometer a segurança de uma empresa.

Alguns exemplos são: e-mails falsos que solicitam informação confidencial, chamadas de telefone falsas, ou propagação de códigos maliciosos nas redes sociais simulando ser de aplicativos que não apresentam ameaças. Também costumam fazer uso de temas atuais ou notícias falsas para aumentar a probabilidade de êxito desses ataques.

Recentemente, os ataques direcionados a organizações aumentaram com o objetivo de se infiltrar na infraestutura tecnológica e acessar a informação sensível que, em alguns casos, é exposta publicamente.

Um empregado seguro identifica os principais ataques relacionados com Técnicas de Engenharia Social.

Um empregado seguro conhece os diferentes tipos de códigos maliciosos e aplica boas práticas para evitar infecções.

Malware

O malware (acrônimo de malicious software) é um dos ataques mais comuns da atualidade. Basicamente, se trata de arquivos com fins danosos que, ao infectar um computador, podem realizar diversas ações como roubar informação, controlar o sistema e/ou sequestrar dados, ou, ainda, sistemas por completo.

Esses códigos maliciosos fazem com que as equipes de segurança se perguntem coisas como: o que aconteceria se toda a informação que se armazena em um dispositivo é sequestrada? Como afetaria a produtividade? Quanto tempo deve demorar para solucionar o incoveniente?

Sem dúvida, essas situações afetam diretamente o rendimento da empresa, e em consequência, possuem custos financeiros.

Phishing

Trata-se de um ataque que envolve técnicas de Engenharia Social para adquirir informações pessoais e/ou confidenciais de forma fraudulenta, como senhas ou detalhes de cartões de crédito das vítimas.

Dentro das organizações, costumam ser realizados o que chamamos de spear phishing, ou seja, ataques direcionados especificamente para aumentar a probabilidade de infecção em uma empresa.

Para realizar esse truque, o atacante (phisher) simula ser uma pessoa ou empresa de confiança (geralmente organizações bancárias) através de uma comunicação que parece legítima (como e-mails, sistemas de mensagens instantâneas ou ainda chamadas telefônicas) e solicita informações sensíveis da vítima.

Um funcionário seguro reconhece os e-mails e mensagens fraudulentas que buscam roubar informação sensível.

Um funcionário seguro protege a informação armazenada, processada e transmitida para evitar a fuga de informação.

Roubo e exposição de informação

Um dos piores cenários para uma empresa é o roubo de informação sensível cuja exposição pode afetar o negócio. Cabe destacar que o incidente pode ser tanto deliberado como acidental. Da mesma forma, o roubo de informação não aplica somente a meios digitais, mas também os físicos (arquiveiros, pastas, etc.).

O impacto do roubo de informação aumenta se os dados são expostos, já que não afeta somente a organização, mas também os usuários que possuem seus dados conhecidos publicamente. Por isso, todos os integrantes da empresa devem cuidar da informação e aplicar as medidas de proteção necessárias.

Práticas de gestão e controles tecnológicos

- Políticas de segurança
- Classificação da informação
- Ferramentas de segurança

Práticas de gestão e controles tecnológicos

Políticas de segurança

As políticas de segurança são os documentos que protegem os compromissos adquiridos pelos membros da organização, ou ainda as normas que determinam sua conduta em relação à proteção dos dados e outros ativos.

É ideal que toda empresa possua uma política de segurança, que seja conhecida por todos os funcionários.

Quando esse documento é assinado, a pessoa certifica que entende e acata os alinhamentos; além disso, se responsabiliza em cumprir todas as normas de segurança definidas pelas organização.

Um empregado seguro lê, entende e acata as políticas de segurança da organização.

Classificação da informação

Um aspecto relevante dentro das organizações é a classificação da informação, para definir qual se mostra mais importante para os objetivos do negócio.

Nesse sentido, as medidas de proteção se aplicam em função da importância e criticidade dos dados.

Quando o custo dos controles de segurança sobrepassa o valor designado para a informação e outros recursos críticos, resulta mais conveniente repensar se esses controles são adequados.

Um funcionário seguro identifica a informação sensível e, por isso, a protege de acordo com os critérios definidos.

Ferramentas de segurança

Os controles tecnológicos são parte de um elemento básico de Segurança da Informação nas empresas. Os mais comuns são:

- **Antivírus:** protege proativamente os equipamentos e sua informação contra ataques de códigos maliciosos novos ou desconhecidos, desde vírus, worm e trojans até spyware, ransomware e botnets.
- **Firewall:** pode estar integrado com a solução antivírus e protege o equipamento de conexões que entram e saem da Internet, utilizadas em ataques externos, como também conexões em que um dispositivo infectado busca realizar com outro.
- **Antispam:** software que também pode ser integrado com um antivírus ou com o cliente de e-mail e que permite filtrar e-mails em massa e indesejados em sua caixa de entrada corporativa.

Não obstante, existem outras ferramentas que costumam ser implementadas no perímetro da rede ou diretamente nos servidores, como soluções de backup, IDS, IPS, DLP, firewall de perímetro, gerenciador de patches, entre outras.

Um empregado seguro conhece e utiliza de maneira adequada as soluções tecnológicas de segurança da empresa.

Boas práticas aplicadas ao uso da tecnologia

- Senhas
- E-mail
- Dispositivos móveis
- Redes Sociais
- Redes sem fio

Boas práticas aplicadas ao uso da tecnologia

Senhas

Hoje em dia, as senhas continuam sendo o principal pelo método para a autenticação dos usuários nos sistemas e plataformas, por isso, os funcionários costumam ter várias senhas para os sistemas internos que utilizam.

Por isso, uma senha forte pode evitar o acesso à informação confidencial ou a um sistema por parte de um atacante ou um código malicioso. Com isso em mente, é importante que as senhas sejam fáceis de lembrar e difíceis de advinhar.

Nesse sentido, é recomendável a utilização de um software para gerenciamento de senhas, assim como o uso de diferentes chaves para serviços corporativos diferentes. Do mesmo modo, soluções de dupla autenticação reduzem de maneira considerável os riscos de segurança associados à forma de verificar a identidade dos usuários.

Um empregado seguro utiliza senhas distintas e fortes para serviços diferentes, e utiliza 2FA.

Um empregado seguro evita acessar links suspeitos ou baixar arquivos anexos de remetentes desconhecidos.

E-mail

O uso massivo do e-mail o transformou em um elemento utilizado pelos cibercriminosos com fins maliciosos, como hoax (notícias falsas), scams (enganos), spam (correios em massa e indesejados), phishing ou a propagação de malware.

Existem situações em que, para se registrar em algum serviço, ou ainda Redes Sociais, se requer um endereço de e-mail. Os endereços corporativos utilizam como fonte de comunicação da empresa e na medida do possível deve-se evitar sua exposição na Internet.

Caso utilize esse endereço de e-mail para se registrar em um serviço, pode existir certa exposição desse contato e, dessa forma, aumentar as possibilidades de sofrer um ataque.

Dispositivos móveis

O uso massivo de smartphones nas empresas permitem o acesso à informação a todo momento e a partir de qualquer lugar. Não obstante, transportar informação sensível em dispositivos móveis implica um risco, já que se tornar em uma forma de roubo ou perda de informação, assim como também sofrer infecções com malware nesses equipamentos.

Para minimizar esses riscos, é possível utilizar ferramentas de controle de dispositivos MDM (Mobile Device Management) que evitam a instalação de aplicativos não autorizados, aplicar políticas de segurança ou exlcuir a informação de forma segura e remota.

Do mesmo modo, as boas práticas incluem ações como o uso de um código de segurança para o bloqueio, criptografia da informação e utilização de soluções antimalware.

Um empregado seguro utiliza seu dispositivo móvel de maneira responsável e segura para os fins da empresa.

Um funcionário seguro utiliza as Redes Sociais e ferramentas de comunicação de maneira responsável e com filtros de privacidade.

Redes Sociais

As Redes Sociais são utilizadas pelos cibercriminosos com oum vetor de propagação de ameaças à informação, especialmente através de links que redirecionam a sites desconhecidos, envio de arquivos maliciosos ou mensagens falsas.

Nesse sentido, é recomendável que as organizações supervisionem o use desses serviços em seus escritórios. Em ocasiões não podem ser bloqueados, já que existem cargos específicos (como Community Mangement), para ter medidas preventivas necessárias visando evitar que ameaças à informação sejam distribuídas por esses meios.

As configurações adequadas de segurança e privacidade dos perfis também são práticas que evitam a exposição da informação.

Redes sem fio

É comum utilizar equipamentos portáteis de trabalho para conectar-se a redes WiFi públicas, como por exemplo, redes em cafés ou aeroportos. Nesses casos, é preciso lembrar que a segurança está ligada aos controles existentes em tal rede e que, muitas vezes, são inexistentes, tais como a ausência de uma senha para realizar a conexão ou o uso de protocolos seguros. É por isso que não recomendamos realizar conexões sensíveis, como acessar o e-mail corporativo, já que a rede pode estar exposta e a informação sem nenhum tipo de criptografia, sendo assim, muitos dados podem ser visíveis por terceiros não autorizados conectados nessa mesma rede.

Caso você utilize um equipamento público para se conectar, não acessar arquivos com informação confidencial de forma local, já que podem ficar acessíveis nesse dispositivo e serem vistos por qualquer pessoa que venha usá-lo futuramente.

Um empregado seguro utiliza conexões WiFi protegidas. Quando não é possível, utiliza práticas como criptografia de comunicações ou conexões VPN.

Práticas do funcionário seguro em seu ambiente de trabalho

Práticas do funcionário seguro em seu ambiente de trabalho

Segurança em seu lugar de trabalho

Além das políticas de segurança que os membros da organização devem cumprir, existem outras práticas que contribuem para aumentar a segurança.

Entre elas podemos citar:

- O funcionário tem a responsabilidade de utilizar adequadamente todos os ativos da organização, como também de proteger os que estão sob sua proteção.
- É necessário bloquear o dispositivo ao deixar de usá-lo, inclusive ao sair de seu lugar de trabalho por apenas poucos minutos, para evitar a leitura de informações por parte de terceiros não autorizados.
- Deve-se manter a área de trabalho limpa, tanto na vida física como nos sistemas operacionais, para não divulgar informações sensível por acidente.
- Quando se suspeita que um sistema, ou ainda uma rede completa da empresa, foi comprometida, deve-se avisar o departamento de segurança ou de TI imediatamente.
- Mais ainda, quando realmente houver um incidente, deve-se avisar de maneira rápida o departamento responsável.

Um empregado seguro aplica boas práticas em seu ambiente de trabalho e notifica imediatamente qualquer suspeita de incidente de segurança.

11 práticas do funcionário seguro em seu ambiente de trabalho

- **Políticas de segurança:** ler, entender e acatar as políticas de segurança da empresa.
- **Classificação da informação:** identificar a informação sensível e aplicar medidas de proteção criadas pela empresa.
- **Ferramentas de segurança:** utilizar os controles de segurança tecnológicos, como antivírus, firewall ou antispam, de maneira adequada para mitigar os riscos de incidentes.
- **Sehnas:** utilizar senhas complexas com mais de dez caracteres e que sejam diferentes para cada serviço ou sistemas da organização. Caso seja necessário, é possível implementar um gerenciador de senhas e mecanismos de dupla autenticação.
- **Informação pessoal:** evitar compartilhar informações com pessoas que não possuem acesso a elas.
- **Atualizações de segurança:** atualizar o software e aplicar patches de segurança para evitar exploração de vulnerabilidades.
- **Eliminar informações de forma segura:** destruir documentos impressos com informações sensíveis antes de jogá-los fora e excluir informação digital sensível com as ferramentas adequadas.
- **Bloqueio de sessão e área de trabalho limpa:** bloquear o sistema quando está fora de uso e manter tanto o a área de trabalho fisica como a do sistema operacional limpa para não expor informações privadas a terceiros não autorizados.
- **E-mail:** revisar o e-mail recebido e evitar acessar links suspeitos ou fazer o downloads de arquivos anexas provenientes de remetentes desconhecidos.
- **Dispositivos móveis:** utilizar o dispositivo móvel corporativo somente para trabalho e aplicando tecnologias MDM.
- **Incidentes de segurança:** reportar imediatamente eventos suspeitos ou incidentes de segurança que possam comprometer a informação sensíve, e outros ativos críticos da organização.

Práticas do funcionário seguro em seu ambiente pessoal

Práticas do funcionário seguro em seu ambiente pessoal

Do trabalho para casa e vice-versa

Há anos, a portabilidade e os benefícios como o Home Office permitem que os funcionários possam trabalhar a partir de suas casa. Mesmo isso sendo muito cômodo e capaz de aumentar a produtividade, é necessário tomar cuidados já que uma rede doméstica pode estar configurada de forma errada e/ou contorlada, como acontece nos escritórios, o que poderia causar infecções e/ou fugas de dados. Por isso, é necessário aplicar medidas adicionais:

- Contar com um software antivírus no computador pessoal para estar protegido contra possíveis ameaças.
- Atualizar o sistema operacional para contar com todos os patches de segurança. Da mesma forma, é necessário atualizar todos os aplicativos e software.
- Acatar políticas de segurança da organização, mesmo quando o funcionário encontra-se fora do ambiente corporativo.

Além disso, quando se leva informações e documentos de extrema importância para trabalhar fora da empresa, deve-se ter um cuidado especial quanto a roubos, perda ou exposição dos dados em lugares públicos ou até mesmo em casa. Esses documentos devem ser tratados levando em conta o nível de confidencialidade que requerem.

Caso utilizem dispositivos de armazenameno USB, sempre é necessário realizar uma análise contra malware ao inserir o dispositivo no equipamento (tanto o corporativo como o pessoal), assim como utilizar medidas de segurança adicionais, como a criptografia de dados.

Um funcionário seguro protege a informação da empresa até mesmo fora do ambiente de trabalho.

Práticas do funcionário seguro em seu ambiente pessoal

- **Políticas de segurança:** acatar as políticas de segurança da empresa mesmo estando fora dela.
- **Dispositivos móveis:** proteger os dispositivos móveis utilizados em casa para acessar a rede ou informação corporativa.
- **Soluções contra malware:** se utiliza um computador pessoal é necessário, na medida do possível, implementar os mesmos controles de segurança presentes nas políticas da organização.
- **Atualizações de segurança:** as atualizações não só incluem melhorias nas funcionalidades, mas também patches de segurança que corrigem falhas nos programas.

Conclusões

Independente das tarefas dos integrantes da organização ou o nível hierárquico que possuem, proteger a informação sensível da empresa é uma responsabilidade fundamental que contribui na manutenção e continuidade das operações e conquista dos objetivos do negócio.

Qualquer divulgação, modificação ou interrupção de informações críticas devido a uma infecção com malware ou outras ameaças à informação, impacta diretamente na imagem da empresa e na confiança dos clientes em relação a ela.

Entender a segurança corporativa, aplicar controles tecnológicos e de gestão, seguir boas práticas, manter os usuário educados e conscientes sobre temas que cercam a Segurança da Informação, atribui um valor agregado à organização.

Todos esses elementos em conjunto contribuem para a garantia da confidencialidade, integridade e disponibilidade da informação, além de buscar um propósito maior e mais importante: proteger o negócio.

www.eset.com/br

/EsetBrasil @ESET_Brasil /company/eset-brasil