ENJOY SAFER TECHNOLOGY™

GUIA DO

Empregado Seguro

Introdução

A cada ano, a Segurança da Informação em uma organização adquire cada vez mais relevância e, em condições ideais, é responsabilidade propriamente da área de Segurança - em empresas grandes -, ainda que, em função das características de cada organização, pode depender de outras áreas, como TI ou Operações.

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

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

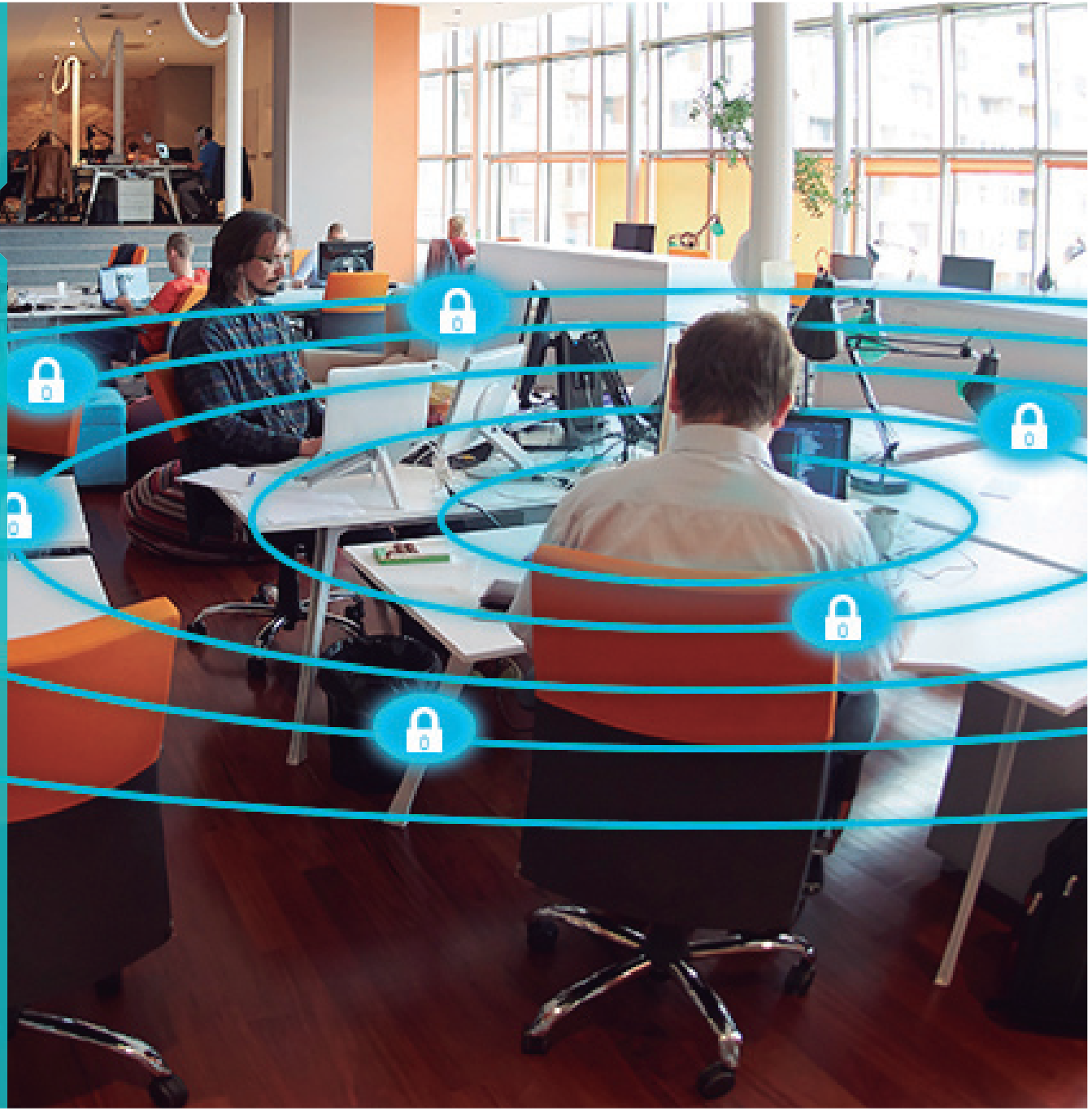
Índice

Empregado Seguro

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

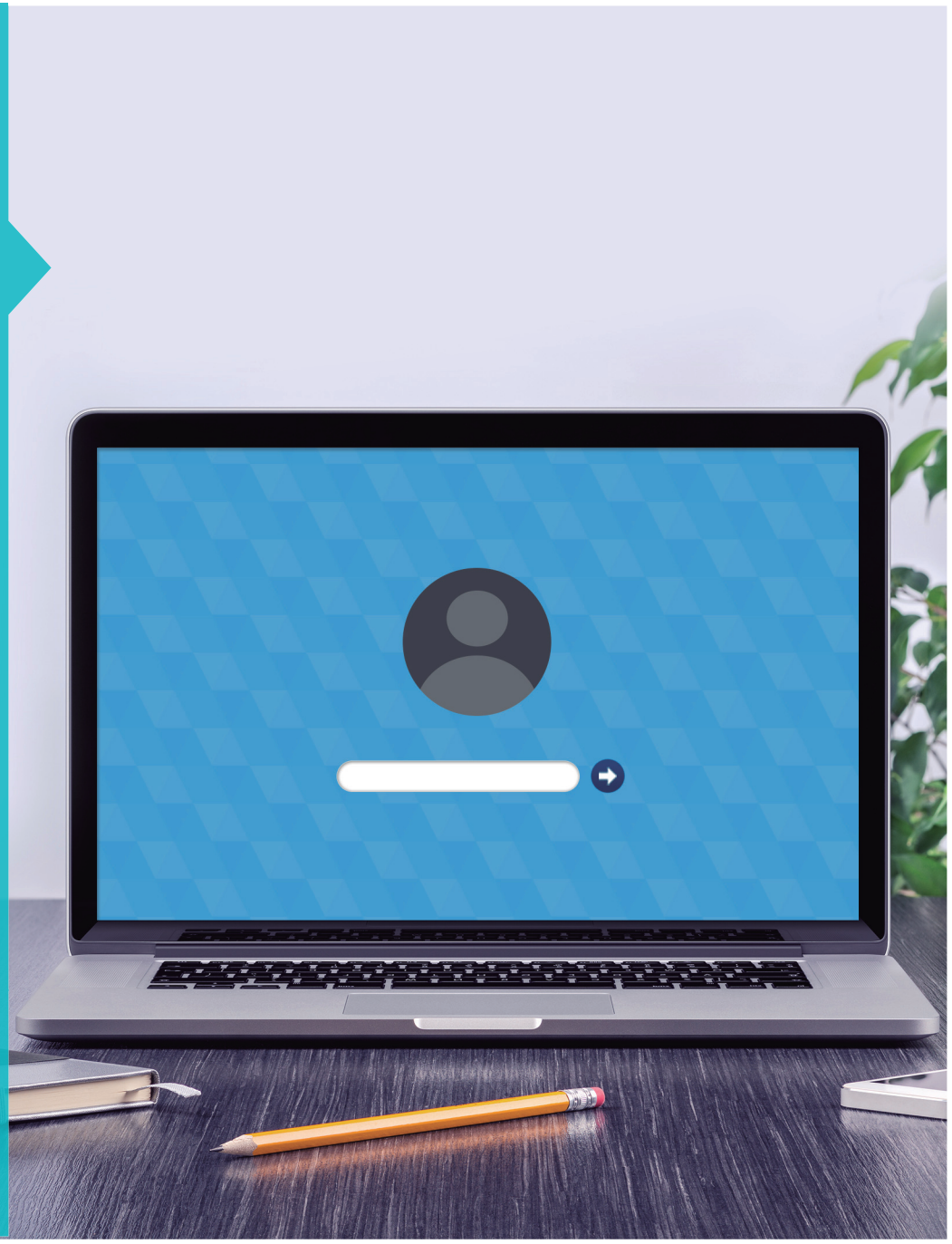
Por isso, este guia tem como propósito proporcionar a informação necessária para que cada integrante de uma organização possa se tornar um empregado seguro e atento às ameaças na área de informática para não colocar em risco o negócio.

Neste contexto, serão abordadas as problemáticas mais comuns, as principais ameaças e as melhores práticas para o manuseio da informação sensível nas 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 Aurélio, "segurança" se define como "estado, qualidade ou condição de quem ou do que está livre de perigos, incertezas, assegurado de danos e riscos eventuais". Entretanto, isso se trata de uma condição ideal, já que na realidade não é possível ter certeza de que se pode evitar todos os perigos.

Por esta razão, o propósito da segurança em todos os seus âmbitos de aplicação é reduzir riscos até um nivel que seja aceitável. Em um sentido mais amplo, a segurança também compreende todas as atividades que tenham como fim proteger uma coisa ou uma pessoa de algum tipo de perigo.

Informação

A informação é um ativo que, igual a outros ativos importantes, deve ser protegida. Nas empresas, é essencial para a tomada de decisões, o alcance de 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 as ideias ou o conhecimento das pessoas.

Para além do formato em que se encontra a informação, é necessário implementar medidas de segurança para protegê-la em função da 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 um propósito de maior alcance ainda: proteger o negócio.

As propriedades da informação

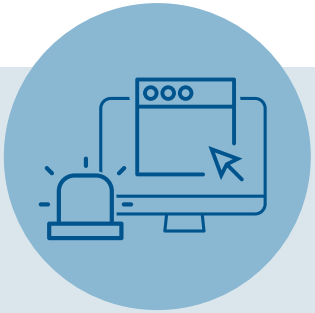
- **Confidencialidade**: que a informação seja acessível unicamente para os indivíduos, entidades ou processos que possuam os privilégios e a autorização para fazê-lo. *Por exemplo, que um usuário não possa acessar a base de dados de um servidor web.*

- **Integridade**: que a informação mantenha sua exatidão e completitude.
  Por exemplo, que um hacker não possa modificar os preços de venda de um site.

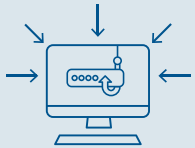
- **Disponibilidade**: que a informação seja acessível e utilizável quando uma entidade a requeira.
  Por exemplo, evitar problemas em um servidor que foi desligado.

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 freiam as organizações na busca e alcance de seus objetivos de negócio.
Portanto, o que se tenta minimizar o impacto que possa ser gerado com os incidentes de segurança relacionados com as vulnerabilidades (agentes internos) e ameaças (agentes externos). Estes riscos também podem materializar-se devido a situações intencionais ou acidentais.



INTERNO



EXTERNO

INTENCIONAL

Um empregado desgostoso destrói um documento e informações importantes.

Um hacker acessa uma base de dados do site da empresas de maneira externa.

ACIDENTAL

Um empregado perde um dispositivo USB onde transporta informação confidencial da empresa.

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

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

- Vulnerabilidade: debilidade 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 ou obter acesso não autorizado ou fazer uso indevido dos ativos.

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

A interceptação atenta contra a confidencialidade; a modificação o faz contra a integridade, enquanto que a interrupção se faz com a disponibilidade.

Os ataques de fabricação buscam atentar contra a autenticidade de quem interatua com a informação.

Risco, probabilidade e impacto

Através da aplicação de medidas de segurança se tenta mitigar riscos, de maneira que a realização de um ataque seja impraticável, inviável ou com as consequências mínimas aceitáveis.

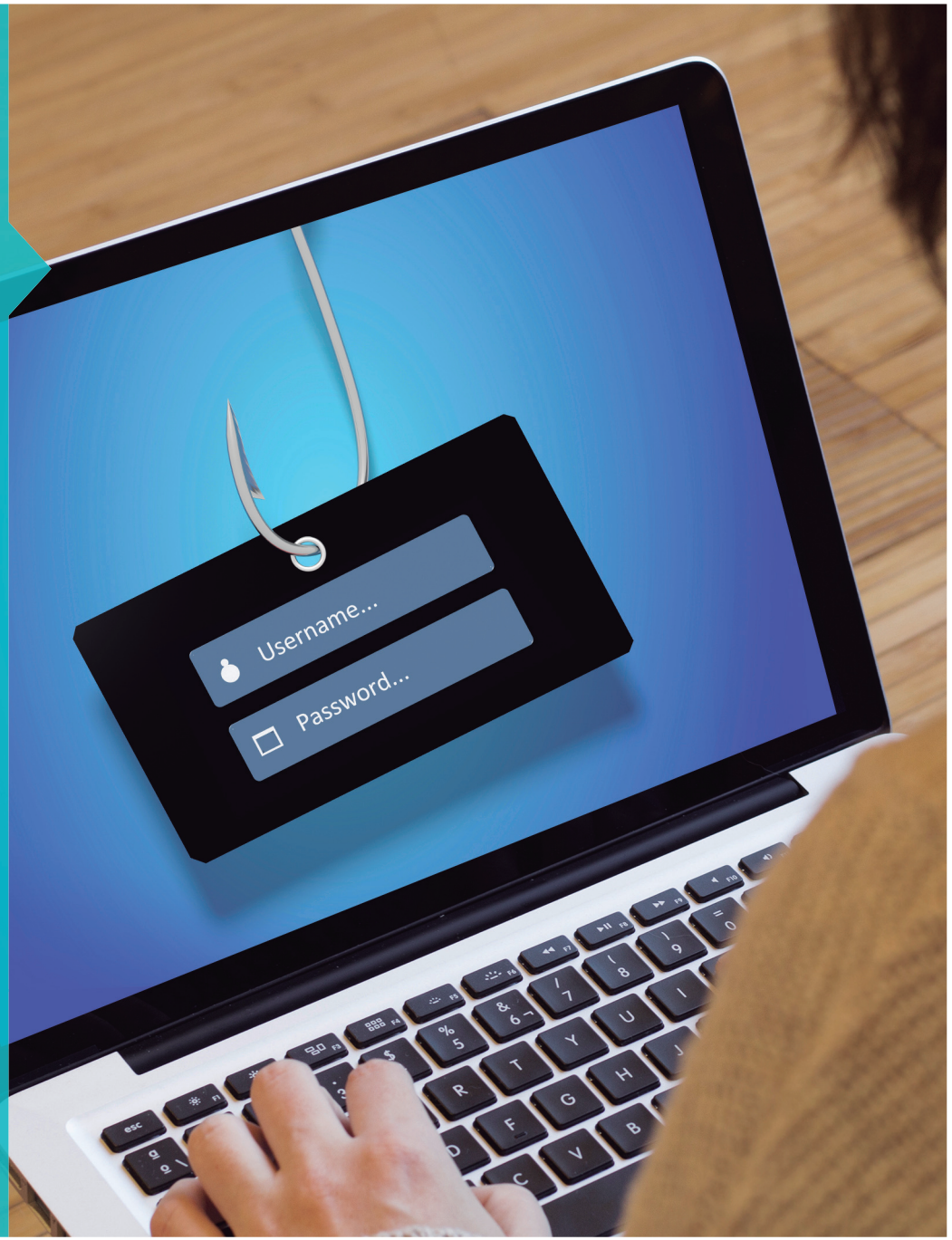
Portanto, a ideia inicial de segurança volta a tomar relevância pois, ainda que não possa ser garantida por completo, os riscos devem ser tratados e reduzidos até um nivel que não representem consequências consideráveis.

Para a Segurança da Informação, os riscos estão associados a causa potencial de que uma ameaça possa desencadear uma ou mais vulnerabilidades de um ativo ou grupo deles, tendo como consequência um dano para a organização.

Os riscos geralmente se expressam mediante a combinação da probabilidade de que um evento não desejado suceda e suas consequências ou impacto. Por este motivo, as medidas de segurança estão orientadas a reduzir uma dessas duas variáveis ou, no melhor dos casos, ambas.

Ameaças comuns que atentam contra a informação

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



Ameaças comuns que atentam contra a informação

Engenharia Social

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

Alguns exemplos são: e-mails fraudulentos que solicitam informação confidencial, falsas chamadas telefônicas ou propagação de códigos maliciosos nas redes sociais simulando ser aplicativos benignos. Também costumam utilizar temas da atualidade ou notícias falsas para aumentar a probabilidade de êxito destes ataques.

Recentemente, se viu um incremento de ataques dirigidos a organizações para se infiltrar na infraestrutura tecnológica e acessar a informação sensível que, em alguns casos, é exposta publicamente.

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

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

Malware

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

Estes 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 equipamento fosse sequestrada?, como isso afetaria a productividade?, quanto tempo se deveria dedicar a solucionar o inconveniente?, entre outras.

Sem dúvida, estas situações afetam diretamente o rendimento da empresa e, por fim, custam dinheiro.

Phishing

Se trata de um ataque que envolve técnicas de Engenharia Social para adquirir fraudulentamente informação pessoal e/ou confidencial, como senhas ou detalhes dos cartões de crédito das vitimas.

Dentro das organizações, costumam realizar-se ataques dirigidos através do denominado spear phishing, quer dizer, ataques desenhados especificamente para aumentar a probabilidade de infecção em uma empresa.

Para efetuar o engano, o phisher simula ser uma pessoa ou empresa de confiança (geralmente entidades bancárias) através de uma aparente comunicação legítima (como e-mails, sistemas de mensagem instantânea ou ainda chamadas telefônicas) e solicita da vitima informação sensível.

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

Um empregado seguro protege a informação armazenada, processada e transmitida para evitar o vazamento de informação.

Roubo e exposição de informação

Um dos piores cenários para uma empresa é o roubo de informação sensível cuja exposição possa afetar o negócio. Cabe destacar que o incidente pode ser tanto deliberado como acidental.

Assim mesmo, o roubo de informação não se aplica somente a meios digitais, mas também aos físicos (arquivistas, documentações, etc.).

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

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 respaldam os compromissos adquiridos pelos membros da organização, ou ainda, as normas que determinam sua conduta em relação à proteção da informação e outros ativos.

É ideal que toda empresa conte com uma política de segurança que seja conhecida por todos os empregados.

Quando este documento é assinado, a pessoa certifica que entende e acata os alinhamentos. Além disso, se compromete a cumprir todas as normas de segurança definidas pela organização.

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

Classificação da informação

Um aspecto relevante dentro das organizações se relaciona com a classificação da informação para definir qual resulta mais relevante para os fins que o negócio persegue.

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

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

Um empregado seguro identifica a informação sensível e, em consequência, a protege de acordo com os critérios definidos.

Ferramentas de segurança

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

- Antivírus: protege proativamente os equipamentos e sua informação contra distintos ataques de códigos maliciosos novos ou desconhecidos, desde vírus, worms e trojans até spyware, ransomware e botnets.
- Firewall: pode estar integrado com a solução antivírus e protege o equipamento das conexões de entrada e saída da Internet que se possam utilizar em ataque externos, como também as conexões que um equipamento infectado queira realizar no exterior.
- Antispam: software que também pode integrar-se 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, há outras ferramentas que se costuma implementar no perímetro da rede ou diretamente nos servidores, como soluções de backup, IDS, IPS, DLP, firewall perimetral, gestão 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 wireless

Boas práticas aplicadas ao uso da tecnologia

Senhas

Atualmente, as senhas continuam sendo o principal método para a autenticação dos usuários nos sistemas e plataformas, o que faz com que os integrantes de uma companhía tenham várias senhas para os sistemas internos que utilizam.

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

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

Um empregado seguro utiliza senhas diferentes 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 tornou um elemento utilizado pelos cibercriminosos com fins maliciosos, como hoax (notícias falsas), scams (fraudes), spam (e-mails massivos e indesejados), phishing ou a propagação de malware.

Existem situações onde, para registrar-se em algum serviço, incluindo Redes Sociais, se requer a colocação de um endereço de e-mail. Os endereços corporativos são utilizados como fonte de comunicação da empresa e, na medida do possível, debe-se evitar sua exposição na Internet.

Caso ele seja utilizado para registrar-se em um serviço, pode haver certa exposição desse endereço e, dessa maneira, aumentam as possibilidades de sofrer algum ataque.

Dispositivos móveis

A incorporação dos smartphones nas empresas permitem o acesso à informação em todo momento e de qualquer lugar. Não obstante, transportar informação sensível em dispositivos móveis implica um risco, já que pode se converter em uma via para o vazamento ou roubo de informação, assim como também sofrer infecções con malware para dispositivos móveis.

Para minimizar estes riscos, é possível utilizar ferramentas de controle de dispositivos MDM (Mobile Device Management) que evitem a instalação de aplicativos não permitidos, aplicar políticas de segurança ou apagar remotamente informações de maneira segura.

Ainda assim, as boas práticas incluem ações como o uso de um código de segurança para bloqueio, a criptografía da informação e a utilização de soluções antimalware.

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

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

Redes Sociais

As Redes Sociais são utilizadas pelos cibercriminosos como um vetor de propagação de ameaças de informática, especialmente através de links que se dirigem a sites desconhecidos, envio de arquivos maliciosos ou mensagens falsas.

Neste sentido, é recomendável que as organizações supervisionem o uso destes serviços em seus escritórios. Em algumas ocasiões, não podem ser bloqueados, já que são utilizados para tarefas específicas (como o Community Management), sendo necessário ter as medidas preventivas adequadas para evitar que ameaças se distribuam por estas vías.

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

Redes wireless

É comum utilizar equipamentos portáteis de trabalho para conectar-se a redes WiFi públicas, como por exemplo, redes em cafés ou aeroportos. Nestes casos, deve considerar-se que a segurança está ligada aos controles existentes na tal rede e que, muitas vezes, eles são inexistentes, tais como a ausência de uma senha para realizar a conexão ou o uso de protocolos seguros.

É por isso que não é recomendável realizar conexões sensíveis, como acessar o e-mail corporativo, já que a rede pode estar exposta e a informação sem nenhum tipo de criptografia, podendo muitos dados estarem visíveis para terceiros não autorizados conectados na mesma rede.

No caso de utilizar um equipamento público para conectar-se, não se deve acessar arquivos com informação confidencial de forma local, já que eles podem ficar acessíveis neste dispositivo e ser vistos por qualquer pessoa que o utilize no futuro.

Um empregado seguro usa conexões WiFi seguras. Quando não é possível, ele utiliza práticas como a criptografia de comunicações ou conexões VPN.

Práticas do empregado seguro em seu local de trabalho

Práticas do empregado seguro em seu local de trabalho

Segurança em seu local 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 se incluem:

- O empregado ter a responsabilidade de utilizar adequadamente todos os ativos da organização, como também de proteger aqueles que estejam sob sua responsabilidade.
- Se deve bloquear os equipamentos quando ficam sem supervisão, mesmo quando se deixa por poucos minutos o posto de trabalho, para evitar a extração ou leitura de informação por parte de terceiros não autorizados.
- Se deve manter a mesa de trabalho limpa, tanto na vida física como nos sistemas operacionais (área de trabalho do computador), para não divulgar informação sensível acidentalmente.
- Quando se suspeita que um sistema, ou ainda a rede completa da empresa, foi comprometida, se deve avisar o departamento de segurança ou de TI imediatamente.
- Incluso, quando um incidente efetivamente suceder, é indispensável avisar rapidamente o departamento pertinente.

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

11 Práticas do empregado seguro em seu local de trabalho

- **Políticas de segurança**: ler, entender e acatar as políticas de segurança da organização.
- **Classificação de informação:** identificar a informação sensível e aplicar a medida de proteção designada pela organização.
- **Ferramentas de segurança:** utilizar os controles de segurança tecnológicos, como antivírus, firewall ou antispam, de maneira adequada, para mitigar os riscos de incidentes.
- **Senhas**: utilizar senhas complexas e de mais de dez caracteres que sejam diferentes para distintos serviços ou sistemas da organização. Caso seja necessário, usar um gestor de senhas e mecanismos de autenticação dupla.
- **Informação pessoal**: evitar compartilhar informações com entidades que não estejam autorizadas a acessar a mesma.
- **Atualizações de segurança**: atualizar o software e aplicar patches de segurança para evitar a exploração de vulnerabilidades.
- **Eliminação segura de informação:** destruir documentos impressos com informação sensível antes de descartá-los e eliminar informação digital sensível com as ferramentas adequadas.
- **Bloqueio de sessão e mesa limpa**: bloquear o sistema quando se encontre sem supervisão e manter limpa a mesa física e do sistema operacional para não expor informação privada a terceiros não autorizados.
- **E-mail**: revisar o e-mail recebido e evitar acessar links suspeitos ou baixar arquivos anexos de remetentes desconhecidos.
- **Dispositivos móveis:** utilizar o dispositivo móvel corporativo somente para fins de trabalho e aplicando tecnologias MDM.
- **Incidentes de segurança**: reportar imediatamente eventos suspeitos ou incidentes de segurança que possam comprometer a informação sensível e outros ativos críticos da organização.

Práticas do empregado seguro em sua casa

Práticas do empregado seguro em sua casa

Do trabalho ao lar e vice-versa

Há anos, a portabilidade e os benefícios como o Home Office permitem aos empregados trabalhar em suas casas. Isso é muito cômodo e pode aumentar a produtividade, mas é necessário tomar precauções, dado que uma rede caseira pode não estar corretamente configurada e/ou controlada, como acontece no escritório, o que poderia decorrer em infecções e/ou vazamento de informação. Por isso, é necessário aplicar medidas adicionais:

- Contar com um software antivírus no computador pessoal para estar protegido contra potenciais ameaças.
- Ter o sistema operacional atualizado para contar com todos os patches de segurança. De igual maneira, se deve atualizar o resto do software e os aplicativos.
- Acatar as políticas de segurança da organização, mesmo quando o empregado se encontre fora do âmbito de trabalho.

Além disso, quando se leva informação e documentação importante para trabalhar fora da empresa, se deve ter cuidado especial no que diz respeito ao roubo, perda ou exposição dos dados em lugares públicos ou mesmo em casa. Tais documentos devem ser manipulados levando em conta o nível de confidencialidade que requerem.

No caso de se utilizar dispositivos de armazenamento USB, sempre é necessário realizar uma análise contra malware no momento de inseri-los no equipamento (tanto no corporativo como no pessoal), assim como utilizar medidas de segurança adicionais, como a criptografía de dados.

Um empregado seguro protege a informação da empresa, mesmo fora do âmbito organizacional.

Práticas do empregado seguro em seu lar

- **Políticas de segurança**: acatar as políticas de segurança da organização mesmo estando fora do escritório.
- **Dispositivos móveis**: proteger os dispositivos móveis utilizados em sua casa para acessar a rede ou informação corporativa.
- **Soluções contra malware**: se usar um computador pessoal, se deve utilizar, na medida do possível, os mesmos controles de segurança descritos nas políticas de segurança da organização.
- **Atualizações de segurança**: as atualizações não somente incluem melhorias nas funcionalidades, mas também patches de segurança que corrigem falhas nos programas.

Conclusões

Independentemente das tarefas dos integrantes da organização ou o nível hierárquico que possuam, proteger a informação sensível da empresa é uma tarefa fundamental que contribui para manter a continuidade das operações e alcançar os objetivos de negócio.

Qualquer divulgação, modificação ou interrupção de informação crítica devido a uma infecção com malware ou outras ameaças, impacta diretamente na imagen da empresa e na confiança dos clientes nela.

Entender a segurança corporativa, aplicar controles tecnológicos e de gestão, seguir as boas práticas, manter os usuários educados e conscientes em temas de Segurança da Informação, outorga um valor agregado à organização.

Todos estes elementos em conjunto contribuem para manter a confidencialidade, integridade e disponibilidade da informação, além de perseguir um propósito de maior alcance e importância: proteger o negócio.

www.eset.com.br

/EsetBrasil @ESET_Brasil /company/eset-brasil