PROTEÇÃO DE DADOS

Série temas pertinentes à proteção de dados pessoais

Janne Melo

SUMÁRIO

Introdução

A nossa sociedade é praticamente dependente das tecnologias da informação e das telecomunicações, pois são de fundamental importância para o desenvolvimento de diversas atividades, em que diversos dados são produzidos ao mesmo tempo em que possuímos inúmeros dados, como por exemplo dados de cadastros, biográficos, profissionais, financeiros e de navegação referentes aos titulares que, diariamente, circulam por diversas redes e são armazenados em diferentes sistemas, dispositivos e mídias.

Infelizmente, há situações em que dados podem ser perdidos, indevidamente acessados ou até mesmo coletados e vendidos sem que o titular tenha ciência disso. Alguns exemplos dessas situações incluem:

- Perda do celular, computador ou mídia removível;
- Interceptação de dados ao trafegarem nas redes;
- Há um vazamento envolvendo os dados;
- Contas de usuário e sistemas onde seus dados estão armazenados são invadidos;
- Dados de navegação são coletados de forma não transparente e compartilhados sem consentimento, etc.

Por isso, adotar uma postura preventiva, tentando reduzir a quantidade de dados fornecida e/ou tratadas por você, é essencial. Para coibir abusos, garantir seus direitos e deveres, agindo adequadamente quando necessário é importante também que a Lei Geral de Proteção de Dados veio para auxiliar na proteção dos dados pessoais.

Assim como o titular de dados, as empresas também podem sofrer acessos indevidos, coletados. A proteção de dados, vai muito além do que proteger apenas os seus dados, ou seja, no seu dia a dia, na sua organização, você trata dados pessoais o tempo todo e a sua colaboração com a Unimed em termos de segurança das informações irá incrementar e muito os níveis de segurança não apenas dos seus dados, mas também os dados de outros titulares para que sejam tratados de forma adequada com uso de mecanismos de segurança.

Como ocorre o tratamento indevido dos dados?

O tratamento indevido pode gerar além de prejuízos financeiros, restrição a direitos ou benefícios e invasão de sua privacidade. Podendo ocorrer da seguinte forma:

a) Acesso Indevido

- Por aplicativos e sites que processem seus dados além das finalidades informadas;
- Por atacantes ou códigos maliciosos que consigam acesso às suas contas, aos seus equipamentos ou mídias;
- Em casos de vazamentos de dados.

b) Coleta Excessiva

- Muitos aplicativos e sites coletam dados extras sem o seu conhecimento e os utilizam para a elaboração de perfis de comportamento (profiling);
- Seu perfil pode, então, ser usado, sem o seu consentimento, de forma discriminatória ou para fins como propagandas.

c) Perda de Dados

- Pela ação de códigos maliciosos, como ransomware;
- Pela ação de atacantes que consigam invadir seus equipamentos e mídias e venham a apagá-los

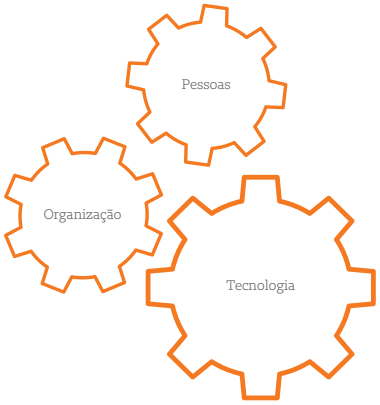
b) Invasão de Contas e Golpes

- Para tentar adivinhar suas senhas e responder perguntas de segurança;
- Em tentativas de golpes, como extorsão, furto de identidade e phishing direcionado e personalizado (spear phishing).

Segurança da Informação

Segundo Laudon e Laudon (2014), um sistema de informação pode ser definido "como um conjunto de componentes inter-relacionados que coletam (ou recuperam), processam, armazenam e distribuem informações destinadas a apoiar a tomada de decisões, coordenação e o controle em uma organização".

Ou seja, os sistemas de informação só obtêm sucesso quando as dimensões tecnológica, organizacional e humana se inter-relacionam de forma harmônica, como em uma engrenagem.



Logo, Sistemas de Informação não é Tecnologia da Informação! A tecnologia da informação é utilizada para armazenar, transferir, processar, coletar, como por exemplo: computadores, telecomunicações, aplicativos outros softwares.

Importância da Segurança da Informação

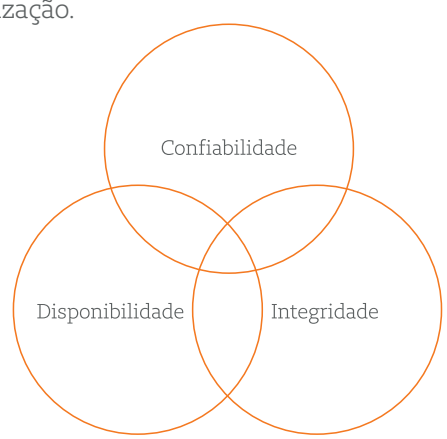
Em um mundo interconectado, a informação e os processos relacionados, sistemas, redes e pessoas envolvidas nas suas operações são informações, que como outros ativos importantes, têm valor para o negócio da organização e, consequentemente, requerem proteção contra vários riscos.

Os sistemas de informação e a tecnologia são os meios que habilitam a vantagem competitiva das organizações. Entretanto, violações da segurança podem trazer prejuízos. A segurança da informação é fundamental para:

- Prevenir de perda de dados;
- Assegurar a privacidade;
- Proteger a propriedade intelectual da organização;
- Minimizar perdas financeiras a partir de incidentes de segurança;
- Garantir a continuidade do negócio durante um desastre;
- Maximizar o retorno de investimentos em novos projetos e oportunidades de negócios.

Princípios da Segurança da Informação

A proteção de dados (e mais amplamente, segurança da informação), abrange todos os controles técnicos, administrativos, lógicos e técnicos necessários para proteger informações. A tríade abaixo é geralmente usada para guiar o desenvolvimento e implementação de uma estrutura para gerenciar segurança da informação dentro de uma organização.



Confidencialidade

Existe uma certa atração do ser humano a tudo que é secreto ou sigiloso. E que, quando ocorre um compartilhamento de uma informação sigilosa a outra pessoa que não está autorizada para tê-la, ocorre uma quebra do princípio da confidencialidade.

A confidencialidade é a propriedade que a informação não é disponibilizada ou divulgada a indivíduos, entidades ou processos não autorizados. São características relacionadas à confidencialidade:

Exclusividade – Dados disponíveis exclusivamente para os usuários autorizados a acessá-los.
Privacidade – Consiste em limitar o acesso às informações pessoais

Para proteger a confidencialidade de dados sensíveis, várias políticas de empregabilidade, segurança e privacidade geralmente definem quem tem acesso a certos dados dentro de uma organização, por quais propósitos e o que são autorizados a fazer com esses dados. Os controles técnicos para garantir confidencialidade podem incluir criptografia de gestão de acesso e identidade e soluções de prevenção de perda de dados.

Integridade

Tem propriedade da exatidão e completeza da informação, prevenindo a modificação inadequada ou não autorizada de dados. São características relacionadas à integridade:

• Completeza: os dados estão completos, inteiros.
• Correção: garante que os dados são verdadeiros e exatos.
• Precisão: as saídas de dados podem ser reproduzidas de forma consistente.
• Validade: os dados atendem aos critérios de aceitação (exatidão, precisão, tempo de vida, etc.).
• Verificação: é possível verificar que os dados foram cadastrados, armazenados, recuperados, transferidos e exibidos corretamente.

Para proteger a integridade de dados, várias soluções técnicas como validação de inserção de dados em formulários e bases de dados podem ser implementados., assim como a adoção de assinaturas digitais e tecnologias de criptografia com uso de hash para provar a autenticidade dos dados ou para verificar que os dados não foram alterados. Finalmente, soluções antimalware protegem a integridade dos dados (e potencialmente a confidencialidade e disponibilidade dos dados).

Disponibilidade

Propriedade de ser acessível e utilizável sob demanda por uma entidade autorizada. Garante que usuários autorizados tenham acesso confiável e pontual aos dados, e previne a interrupção ou destruição de dados não autorizados. São características:

Prontidão
Os sistemas de informação precisam estar disponíveis quando necessários.
Continuidade
O pessoal precisa continuar a trabalhar no caso de uma falha.
Robustez
Necessário ter capacidade suficiente para permitir que todo o pessoal no sistema possa trabalhar.

Para proteger a disponibilidade dos dados de destruição acidental (por exemplo, exclusão) ou intencional (por exemplo, um ataque de ransomware), sistemas de recuperação e backup, além de políticas de retenção e de backup, são implementados.

Dicas de Prevenção

Há diversas normas e regulações setoriais que versam sobre privacidade e proteção de dados no Brasil, como o Código de Defesa do Consumidor, a Lei de Acesso à Informação, a Lei Geral de Telecomunicações, o Marco Civil da Internet, a própria Constituição Federal Brasileira e, no caso da saúde, as diversas normas setoriais da Agência Nacional de Saúde Suplementar (ANS), do Conselho Federal de Medicina (CFM), da Agência Nacional de Vigilância Sanitária (Anvisa), do Conselho Nacional de Saúde (CNS), entre outras.

a) Cópia de Segurança (Backups)

- Protegem seus dados em caso de mau funcionamento de equipamentos, da perda de dispositivos e da ação de códigos maliciosos, especialmente ransomware.

b) Contas e Senhas

- Crie senhas fortes e não repita senhas.
- Tenha certeza de sair de suas contas (logout) ao usar equipamentos compartilhados.
- Habilite a verificação em duas etapas em todas as suas contas, quando disponível.

c) Criptografia

- A criptografia ajuda a tornar as transmissões de dados mais seguras, detectar alterações em seus dados e impedir que sejam lidos indevidamente. Utilize sempre conexões seguras.

d) Arquivos

- Evite colocar na nuvem arquivos contendo dados confidenciais ou que considere privados.
- Seja cuidadoso(a) ao abrir arquivos da organização e enviados por terceiros.

e) Aplicativos

o Instale aplicativos somente de fontes e lojas oficiais em seus dispositivos pessoais, em caso de dispositivos corporativos, entre em contato com o suporte técnico para receber as orientações corretamente.

f) Equipamentos e Mídias

- Utilize sempre mecanismos de segurança em especial os disponibilizados pela Unimed.
- Cuidado para não perder pen drives e discos externos, caso ocorra alguma perda destes equipamentos da organização, deverá realizar o reporte de incidente nos canais oficiais.
- Seja cuidadoso(a) ao usar equipamentos de terceiros, respeite sempre as políticas de segurança da sua organização.

g) E-mails e Mensagens Eletrônicas

- Desconfie de links ou pedidos de pagamentos recebidos via mensagens eletrônicas, mesmo que vindos de pessoas conhecidas.
- Seja cuidadoso ao acessar seu webmail: digite a URL diretamente no navegador.

A Unimed Maceió usa abordagem baseada em risco, irá implementar controles apropriados para abordar vulnerabilidades e atingir um nível aceitável de risco aos dados contra ameaças específicas. Quanto maior o risco para os dados, maior devem ser as medidas que devem ser implementadas.

A Informação como um Ativo Organizacional

Em contabilidade, o termo ativo são todos os bens e direitos de propriedade da empresa, expressos em moeda, e que representam benefícios presentes ou futuros para a empresa. Os patrimônios físicos podem ser considerados ativos empresariais. Entretanto, há também ativos intangíveis que trazem retorno para as empresas.

A informação deve ser tratada como um ativo pelas organizações, visto que possui valor e representa benefícios presentes ou futuros para a empresa, conforme entendimento da NBR 27.002 (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2013).

Localização da Informação

A informação pode estar em vários meios eletrônicos: computadores; notebooks; servidores; discos; fitas; CDs; DVDs. Mas não se pode esquecer que a informação também pode estar: na mente das pessoas; em fotografias; em filmes; em papel, etc.

Benefícios e Direitos Trazidos pela LGPD

A LGPD dá ao titular o direito de saber exatamente como seus dados são tratados, quais dados são coletados e o porquê e com quem eles são compartilhados.

Organizações públicas e privadas, como a Unimed Maceió, devem disponibilizar informações claras que o ajudem a compreender os termos de consentimento e as bases legais que apoiam o tratamento dos seus dados.

A LGPD traz maior segurança jurídica, ao fornecer mecanismos para que o titular tenha controle sobre quais dados seus são coletados e como são usados. É por isto que a Unimed Maceió tem como prioridade realizar a adequação institucional à LGPD garantindo a Proteção de Dados Pessoais, seja dos seus colaboradores, prestadores, beneficiários e/ou fornecedores.

Conseguir atingir níveis adequados de segurança só é possível com a construção de um consenso e com a participação de todas as pessoas envolvidas no trato da informação.

Localização da Informação

https://cartilha.cert.br/fasciculos/protecao-de-dados/fasciculo-protecao-de-dados.pdf

LAUDON, K.C. e LAUDON, J. P. (2014) Sistemas de Informação Gerenciais. 11a. Edição. Pearson

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR 27002: Tecnologia da informação: Técnicas de segurança: Código de prática para controles de segurança da informação. Rio de Janeiro, 2013

SUPREMO TRIBUNAL FEDERAL. Curso a distância: Segurança da informação. Brasília: Coordenadoria de Desenvolvimento de Pessoas, 2018. Disponível em: https://ead.stf.jus.br/. Acesso restrito com login e senha.

MARQUES, W. L. Contabilidade gerencial. 2011.