

1.Posse ou controle

Suponha que um ladrão roube um envelope lacrado contendo um cartão bancário de débito e a senha associada ao cartão. Mesmo que o ladrão não abra esse envelope, a vítima do roubo ficaria legitimamente preocupada com a possibilidade do ladrão usar o cartão de forma fraudulenta e a qualquer momento sem o controle do proprietário. Essa situação ilustra uma perda de controle ou posse de informações, mas não envolve a quebra de sigilo.

2.Autenticidade

Autenticidade se refere à veracidade da alegação de origem ou a auditoria das informações. Por exemplo, um método de verificação da auditoria de um documento escrito à mão é comparar as características de escrita do documento com uma amostra de outros que já tenham sido verificados. Para informações eletrônicas, uma assinatura digital pode ser usada para verificar a autoria de um documento digital usando criptografia de chave pública.

3.Utilidade

Utilidade significa capacidade de uso. Suponha que alguém criptografar dados em um disco para prevenir o acesso não autorizado ou modificações indesejadas - e depois perdeu a chave criptográfica: isso seria uma quebra de utilidade. Os dados seriam confidenciais, controlados, integrais, autênticos e disponíveis - eles não seriam úteis dessa forma. Similarmente, a conversão de dados salariais de uma moeda para outra inadequada também seria uma quebra de utilidade, assim como seria o armazenamento de dados em um formato impróprio para uma determinada arquitetura de computador. A substituição de uma tabela de dados por um gráfico poderia ser descrita como uma quebra de utilidade se a substituição tornar mais difícil a interpretação dos dados. A utilidade é muitas vezes confundida com disponibilidade, pois as falhas, também podem requerer tempo para solucionar as alterações de formato ou de apresentação dos dados. Entretanto, o conceito de capacidade de uso é diferente do de disponibilidade.

4.Devida diligência e devido cuidado

Hoje, as devidas diligências e devidos cuidados estão se tornando questões sérias nas operações de computadores. De fato, o sistema legal começou a responsabilizar importantes parceiros pela ausência dos devidos cuidados no caso de uma grave falha de segurança. Violações de segurança e privacidade são questões quentes que confrontam a comunidade da Internet, e são necessárias normas que abranjam as melhores práticas de devidos cuidados para a proteção de uma organização.

Privacidade e Criptografia no Nível de Transporte	Confidencialidade e Integridade
Controle de Autenticação	Confidencialidade, Integridade e Disponibilidade
Controle de Autorização	Confidencialidade, Integridade e Disponibilidade

Devida diligência consiste em compreender as ameaças e os riscos atuais, e devido cuidado diz respeito à implementação de contramedidas para prover proteção contra essas ameaças. Se uma empresa não pratica o devido cuidado e a devida diligência em relação à segurança de seus ativos, ela pode ser legalmente acusada de negligência e responsabilidade por quaisquer implicações dessa negligência de acordo com as leis de cada país em que opera, se for um negócio.

5. Devida diligência e devido cuidado

5.1 Diferença entre dado e informação

É essencial compreender a diferença entre dado e informação. O dado pode ser processado pela tecnologia da informação, mas ele se torna informação após adquirir certo significado. Quando se trata de segurança da informação, você deve levar em conta as diversas formas nas quais a informação pode essencialmente se concentrar. Isso envolve, afinal de contas, a segurança da própria informação e independe da forma em que ela é apresentada. No entanto, isso impõe algumas restrições acerca das medidas necessárias para proteger essa informação.

5.2 Análise da informação

A análise da informação fornece uma imagem clara de como uma organização lida com a informação. Por exemplo, um hóspede se registra em um hotel através do site. Essa informação é passada para o sistema de reservas on-line, que, em serviços domésticos, sabe que o quarto deve estar limpo para a chegada do hóspede. Em todos esses passos, é importante que a informação seja confiável.

5.3 Informática

Informática é converter dados em informação. A informática desenvolve novos usos para a tecnologia da informação, está interessada em como as pessoas transformam a tecnologia e em como a tecnologia nos transforma.

5.4 O valor do dado

O dado pode ter grande importância, mesmo se ele não estiver no formato de “informação”, como definido anteriormente. Não haveria a necessidade da “proteção dos dados” e, portanto, da “segurança de computadores” se dados, por definição, não tivessem importância. O valor do dado é determinado principalmente pelo usuário.

5.5 O valor da informação

Informação é conhecimento que alguém tenha adquirido. Enquanto algumas pessoas podem considerar um determinado conjunto de dados desinteressante, outros podem ser capazes de extrair informações valiosas a partir dele. O valor da informação é, portanto, determinado pelo valor que o beneficiário lhe atribui.

5.6 Informação como um fator de produção

Os fatores de produção normais de uma empresa ou organização são o capital, o trabalho (manual) e as matérias-primas. Em tecnologia da informação, é comum também considerar a informação como fator de produção. Empresas não podem existir sem informação. Um armazém que perde suas informações de estoque e clientes normalmente não seria capaz de operar sem elas. Para algumas empresas, tais como o escritório de um contador, a informação é, na verdade, o seu único produto.

6. Sistemas de Informação

A transferência e o processamento de informações ocorrem através de uma infraestrutura de sistema de informação. O termo sistema de informação é frequentemente usado para se referir à interação entre pessoas, processos, dados e tecnologia. Nesse sentido, o termo é usado para se referir não só à tecnologia da informação e da comunicação (TIC) que uma organização usa, mas também à forma como as pessoas interagem com essa tecnologia em apoio aos processos de negócio. Exemplos de sistemas de informação são documentos em armários de arquivos, arquivos de computador e bases de dados, telefones celulares e impressoras. No contexto da segurança da informação, um sistema de informação é toda a combinação de meios, procedimentos, regras e pessoas que asseguram o fornecimento de informações para um processo operacional.

Componentes de TIC incluem:

1. Estações de trabalho, que consistem em um PC com um sistema operacional e outros softwares.
2. Transporte de dados através de uma rede, cabeada ou sem fio
3. Servidores, que consistem no servidor com um sistema operacional e softwares
4. Armazenamento de dados, como em disco, e-mail e bancos de dados
5. Telefones móveis que evoluem cada vez mais para pequenos dispositivos computacionais com grande armazenamento removível.
6. A capacidade e a possibilidade de trocar informações pela rede móvel e/ou bluetooth.
7. Conexões

Um armário de arquivos é uma peça do mobiliário de escritório normalmente usado para armazenar documentos de papel em pastas.