Segurança da Informação

CONCEITOS BÁSICOS DE SEGURANÇA DA INFORMAÇÃO

Uma definição para Segurança da Informação:

"Segurança da Informação: A proteção conferida a um sistema de informação automatizado para atingir os objetivos aplicáveis de preservação da integridade, disponibilidade e confidencialidade dos recursos do sistema de informação (inclui hardware, software, firmware, informações/dados e telecomunicações)."

Fonte: Manual de Segurança de Computadores do NIST [NIST 95]

Esta definição apresenta três objetivos principais que estão no centro da segurança da informação:

- **Confidencialidade**: Este termo abrange dois conceitos relacionados:

Confidencialidade dos dados: 1 Garante que informações privadas ou confidenciais não sejam disponibilizadas ou divulgadas a pessoas não autorizadas.

Privacidade: Garante que os indivíduos controlem ou influenciem quais informações relacionadas a eles podem ser coletadas e armazenadas e por quem e para quem essas informações podem ser divulgadas.

- **Integridade**: Este termo abrange dois conceitos relacionados:

Integridade dos dados: Garante que as informações e os programas sejam alterados apenas de maneira especificada e autorizada.

Integridade do sistema: Garante que um sistema desempenhe sua função pretendida de maneira intacta, livre de manipulação não autorizada deliberada ou inadvertida do sistema.

- **Disponibilidade**: Garante que os sistemas funcionem prontamente e o serviço não seja negado a usuários autorizados

Os três conceitos incorporam os objetivos fundamentais de segurança tanto para dados quanto para serviços de informação e computação.

- **Confidencialidade**: Preservar as restrições autorizadas de acesso e divulgação de informações, incluindo meios para proteger a privacidade pessoal e informações proprietárias. Uma perda de confidencialidade é a divulgação não autorizada de informações.

- **Integridade**: Proteção contra modificação ou destruição imprópria de informações, incluindo a garantia de não repúdio e autenticidade das informações. Uma perda de integridade é a modificação ou destruição não autorizada de informações.

- **Disponibilidade**: Garantir o acesso e o uso oportuno e confiável da informação. Uma perda de disponibilidade é a interrupção do acesso ou uso da informação ou de um sistema de informação.

Embora o uso desses três conceitos para definir os objetivos de segurança esteja bem estabelecido, alguns no campo da segurança sentem que são necessários conceitos adicionais para apresentar um quadro completo. Dois dos mais comumente mencionados são os seguintes:

- **Autenticidade**: A propriedade de ser genuíno e poder ser verificado e confiável; confiança na validade de uma transmissão, uma mensagem ou mensagem

originador. Isso significa verificar se os usuários são quem dizem ser e se cada entrada que chega ao sistema veio de uma fonte confiável.

- **Responsabilidade:** O objetivo de segurança que gera o requisito para que as ações de uma entidade sejam rastreadas exclusivamente para essa entidade. Isso oferece suporte ao não repúdio, dissuasão, isolamento de falhas, detecção e prevenção de intrusão e recuperação pós-ação e ação legal. Como os sistemas realmente seguros ainda não são uma meta alcançável, devemos ser capazes de rastrear uma violação de segurança até uma parte responsável. Os sistemas devem manter registros de suas atividades para permitir análises forenses posteriores para rastrear violações de segurança ou para auxiliar em disputas de transações.

Os Desafios da Segurança da Informação:

A segurança do computador é fascinante e complexa. Seguem alguns dos motivos:

- A segurança do computador não é tão simples como pode parecer ao iniciante. Os requisitos parecem ser diretos; na verdade, a maioria dos principais requisitos para serviços de segurança pode receber rótulos autoexplicativos de uma palavra: confidencialidade, autenticação, não repúdio, integridade. Mas os mecanismos usados para atender a esses requisitos podem ser bastante complexos, e entendê-los pode envolver um raciocínio bastante sutil.

- Ao desenvolver um mecanismo ou algoritmo de segurança específico, deve-se sempre considerar possíveis ataques a esses recursos de segurança. Em muitos casos, os ataques bem-sucedidos são projetados analisando o problema de uma maneira completamente diferente, explorando, portanto, uma fraqueza inesperada no mecanismo.

- Por causa do ponto 2, os procedimentos usados para fornecer serviços específicos são muitas vezes contraintuitivos. Normalmente, um mecanismo de

segurança é complexo e não é óbvio a partir da declaração de um requisito específico que tais medidas elaboradas sejam necessárias. É somente quando os vários aspectos da ameaça são considerados que mecanismos de segurança elaborados fazem sentido.

- Tendo projetado vários mecanismos de segurança, é necessário decidir onde usá-los. Isso é verdade tanto em termos de posicionamento físico (por exemplo, em que pontos de uma rede são necessários certos mecanismos de segurança) quanto em um sentido lógico [por exemplo, em qual camada ou camadas de uma arquitetura como TCP/IP (*Transmission Control Protocol/ Internet Protocol*) devem ser colocados mecanismos].

- Os mecanismos de segurança geralmente envolvem mais do que um algoritmo ou protocolo específico. Eles também exigem que os participantes possuam algumas informações secretas (por exemplo, uma chave de criptografia), o que levanta questões sobre a criação, distribuição e proteção dessas informações secretas. Também pode haver dependência de protocolos de comunicação cujo comportamento pode complicar a tarefa de desenvolver o mecanismo de segurança. Por exemplo, se o funcionamento adequado do mecanismo de segurança requer a definição de limites de tempo no tempo de trânsito de uma mensagem do emissor para o receptor, qualquer protocolo ou rede que introduza atrasos variáveis e imprevisíveis pode tornar esses limites de tempo sem sentido.

- A segurança do computador é essencialmente uma batalha de inteligência entre um criminoso que tenta encontrar brechas e o projetista ou administrador que tenta fechá-las. A grande vantagem que o invasor tem é que ele precisa apenas encontrar uma única fraqueza, enquanto o projetista deve encontrar e eliminar todas as fraquezas para obter a segurança perfeita.

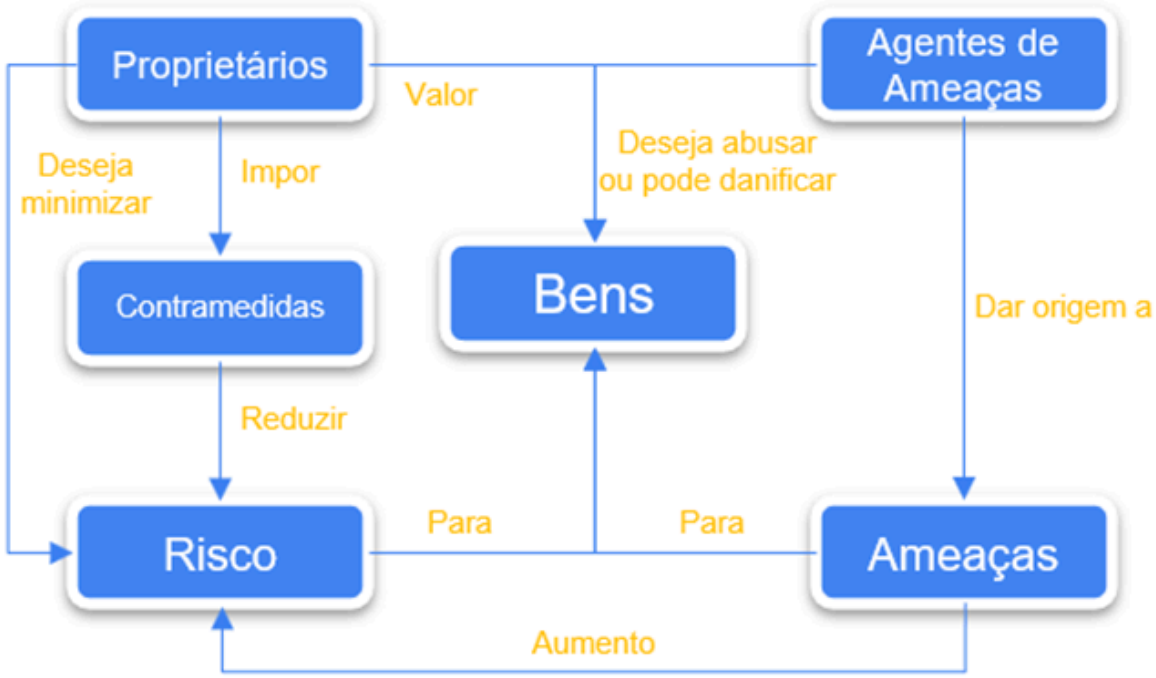
- Existe uma tendência natural por parte dos usuários e gerentes de sistema de perceber pouco benefício do investimento em segurança até que ocorra uma falha de segurança.

- A segurança requer monitoramento regular, até mesmo constante, e isso é difícil no ambiente sobrecarregado de curto prazo de hoje.

- A segurança ainda é muitas vezes uma reflexão tardia para ser incorporada a um sistema após a conclusão do projeto, em vez de ser parte integrante do processo de projeto.

- Muitos usuários e até mesmo administradores de segurança veem a segurança forte como um impedimento para a operação eficiente e amigável de um sistema de informação ou uso de informações.

Um modelo para segurança de computadores



Os ativos de um sistema de computador podem ser categorizados da seguinte forma:

- **Hardware:** Incluindo sistemas de computador e outros dispositivos de processamento de dados, armazenamento de dados e comunicação de dados

- **Software**: Incluindo o sistema operacional, utilitários do sistema e aplicativos.

- **Dados**: Incluindo arquivos e bancos de dados, bem como dados relacionados à segurança, como arquivos de senha.

- **Instalações e redes de comunicação**: links de comunicação de rede local e de longa distância, pontes, roteadores e assim por diante.

No contexto da segurança, a preocupação deve ser com as vulnerabilidades dos recursos do sistema. Observe a lista das seguintes categorias gerais de vulnerabilidades de um sistema de computador ou ativo de rede:

- Ele pode ser corrompido, de modo que faça a coisa errada ou dê respostas erradas. Por exemplo, os valores de dados armazenados podem diferir do que deveriam ser porque foram modificados incorretamente.

- Pode tornar-se vazado. Por exemplo, alguém que não deveria ter acesso a algumas ou todas as informações disponíveis na rede obtém tal acesso.

- Pode ficar indisponível ou muito lento. Ou seja, o uso do sistema ou rede torna-se impossível ou impraticável.

Esses três tipos gerais de vulnerabilidade correspondem aos conceitos de integridade, confidencialidade e disponibilidade, enumerados anteriormente.

Correspondendo aos vários tipos de vulnerabilidades de um recurso do sistema estão as ameaças que são capazes de explorar essas vulnerabilidades. Uma ameaça representa um dano potencial à segurança de um ativo. Um ataque é uma ameaça

que é executada (ameaça ação) e, se bem-sucedido, leva a uma violação indesejável de segurança ou consequência de ameaça.

O agente que executa o ataque é referido como um atacante, ou agente de ameaça. Podemos distinguir dois tipos de ataques:

- **Ataque ativo**: Uma tentativa de alterar os recursos do sistema ou afetar sua operação.

- **Ataque passivo**: uma tentativa de aprender ou fazer uso de informações do sistema que não afetam os recursos do sistema

Também podemos classificar os ataques com base na origem do ataque:

- **Ataque interno**: Iniciado por uma entidade dentro do perímetro de segurança (um "insider"). O insider está autorizado a acessar os recursos do sistema, mas os usa de uma maneira não aprovada por quem concedeu a autorização.

- **Ataque externo**: Iniciado de fora do perímetro, por uma pessoa não autorizada ou usuário ilegítimo do sistema (um "estranho"). Na Internet, o potencial os atacantes externos variam de brincalhões amadores a criminosos organizados, terroristas internacionais e governos hostis.

Finalmente, uma contramedida é qualquer meio utilizado para lidar com um ataque de segurança. Idealmente, uma contramedida pode ser planejada para evitar que um determinado tipo de ataque seja bem-sucedido. Quando a prevenção não é possível, ou falha em alguma instância, o objetivo é detectar o ataque e então se recuperar dos efeitos do ataque. Uma contramedida pode, por si só, introduzir novas vulnerabilidades. Em qualquer caso, vulnerabilidades residuais podem permanecer após a imposição de contramedidas. Essas vulnerabilidades podem ser exploradas por agentes de ameaças que representam um nível residual de risco para os ativos. Os proprietários deverão minimizar esse risco dadas outras restrições.

Ameaças, Ataques e Ativos

Passamos agora a uma análise mais detalhada de ameaças, ataques e ativos. Primeiro, examinamos os tipos de ameaças à segurança que devem ser tratadas e, em seguida, damos alguns exemplos dos tipos de ameaças que se aplicam a diferentes categorias de ativos.

Ameaças e Ataques

A **divulgação não autorizada** é uma ameaça à **confidencialidade**. Os seguintes tipos de ataques podem resultar nessa consequência de ameaça:

- **Exposição:** Isso pode ser deliberado, como quando um insider libera intencionalmente informações confidenciais, como números de cartão de crédito, para um outsider. Também pode ser o resultado de um erro humano, de hardware ou de software, que resulta em uma entidade obter conhecimento não autorizado de dados confidenciais. Tem havido vários casos disso, como universidades que publicam acidentalmente informações confidenciais de alunos na Web.

- **Interceptação:** A interceptação é um ataque comum no contexto das comunicações. Em uma rede local (LAN) compartilhada, como uma LAN sem fio ou uma Ethernet de transmissão, qualquer dispositivo conectado à LAN pode receber uma cópia dos pacotes destinados a outro dispositivo. Na Internet, um determinado hacker pode ter acesso ao tráfego de e-mail e outras transferências de dados. Todas essas situações criam o potencial de acesso não autorizado aos dados.

- **Inferência:** Um exemplo de inferência é conhecido como análise de tráfego, na qual um adversário é capaz de obter informações observando o padrão de tráfego em uma rede, como a quantidade de tráfego entre pares específicos de hosts na rede. Outro exemplo é a inferência de informações detalhadas de um

banco de dados por um usuário que tem acesso limitado; isso é realizado por consultas repetidas cujos resultados combinados permitem inferência.

- **Intrusão:** Um exemplo de intrusão é um adversário que obtém acesso não autorizado a dados confidenciais ao superar as proteções de controle de acesso do sistema.

O **engano** é uma ameaça à **integridade** do sistema ou à integridade dos dados. Os seguintes tipos de ataques podem resultar nessa consequência de ameaça:

- **Máscara:** Um exemplo de máscara é uma tentativa de um usuário não autorizado de obter acesso a um sistema fazendo-se passar por um usuário autorizado; isso pode acontecer se o usuário não autorizado tiver descoberto o ID de logon e a senha de outro usuário. Outro exemplo é a lógica maliciosa, como um cavalo de Tróia, que parece executar uma função útil ou desejável, mas na verdade obtém acesso não autorizado aos recursos do sistema ou enganar um usuário para que execute outra lógica maliciosa.

- **Falsificação:** Refere-se à alteração ou substituição de dados válidos ou à introdução de dados falsos em um arquivo ou banco de dados. Por exemplo, um aluno pode alterar suas notas em um banco de dados da escola.

- **Repúdio:** Neste caso, o usuário nega o envio de dados ou nega o recebimento ou a posse dos dados.

A **interrupção** é uma ameaça à **disponibilidade** ou **integridade** do sistema. Os seguintes tipos de ataques podem resultar nessa consequência de ameaça:

- **Incapacitação:** Trata-se de um ataque à **disponibilidade** do sistema. Isso pode ocorrer como resultado da destruição física ou dano ao hardware do sistema. Mais comumente, softwares mal-intencionados, como cavalos de Tróia, vírus ou

worms, podem operar de forma a desabilitar um sistema ou alguns de seus serviços.

- **Corrupção**: Este é um ataque à **integridade** do sistema. O software malicioso neste contexto pode operar de forma que os recursos ou serviços do sistema funcionem de maneira não intencional. Ou um usuário pode obter acesso não autorizado a um sistema e modificar algumas de suas funções. Um exemplo deste último é um usuário colocando lógica de backdoor no sistema para fornecer acesso subsequente a um sistema e seus recursos por um procedimento diferente do usual.

- **Obstrução**: Uma maneira de obstruir a operação do sistema é interferir nas comunicações, desabilitando os links de comunicação ou alterando as informações de controle de comunicação. Outra maneira é sobrecarregar o sistema, sobrecarregando o tráfego de comunicação ou os recursos de processamento.

A **usurpação** é uma ameaça à **integridade** do sistema. Os seguintes tipos de ataques podem resultar nessa consequência de ameaça:

- **Apropriação indevida**: Isso pode incluir roubo de serviço. Um exemplo é um ataque distribuído de negação de serviço, quando um software malicioso é instalado em vários hosts para serem usados como plataformas para iniciar o tráfego em um host de destino. Nesse caso, o software malicioso faz uso não autorizado dos recursos do processador e do sistema operacional.

- **Uso indevido**: O uso indevido pode ocorrer por meio de lógica maliciosa ou de um hacker que obteve acesso não autorizado a um sistema. Em ambos os casos, as funções de segurança podem ser desativadas ou impedidas.

Ameaças e Ativos

Os ativos de um sistema de computador podem ser categorizados como hardware, software, dados e linhas e redes de comunicação.

Hardware: Uma grande ameaça ao hardware do sistema de computador é a ameaça à disponibilidade. O hardware é o mais vulnerável a ataques e o menos suscetível a controles automatizados. As ameaças incluem danos acidentais e deliberados ao equipamento, bem como roubo. A proliferação de computadores pessoais e estações de trabalho e o uso generalizado de LANs aumentam o potencial de perdas nessa área. O roubo de CD-ROMs e DVDs pode levar à perda de confidencialidade. Medidas de segurança física e administrativa são necessárias para lidar com essas ameaças.

Software: Software inclui o sistema operacional, utilitários e programas de aplicativos. Uma das principais ameaças ao software é um ataque à disponibilidade. O software, especialmente o software de aplicativo, geralmente é fácil de excluir. O software também pode ser alterado ou danificado para torná-lo inútil. O gerenciamento cuidadoso da configuração de software, que inclui fazer backups da versão mais recente do software, pode manter alta disponibilidade. Um problema mais difícil de lidar é a modificação de software que resulta em um programa que ainda funciona, mas que se comporta de forma diferente de antes, o que é uma ameaça à integridade/autenticidade. Vírus de computador e ataques relacionados caem nesta categoria. Um problema final é a proteção contra a pirataria de software. Apesar de certas contramedidas estarem disponíveis, em geral o problema de cópia não autorizada de software não foi resolvido.

Dados: A segurança de hardware e software normalmente são preocupações de profissionais de centros de computação ou preocupações individuais de usuários de computadores pessoais. Um problema muito mais difundido é a segurança de dados, que envolve arquivos e outras formas de dados controlados por indivíduos, grupos e organizações empresariais.

As preocupações de segurança com relação aos dados são amplas, abrangendo disponibilidade, sigilo e integridade. No caso da disponibilidade, a preocupação é com a destruição dos arquivos de dados, que pode ocorrer de forma acidental ou maliciosa.

Linhas e redes de comunicação: Os ataques de segurança de rede podem ser classificados como ataques passivos e ataques ativos. Um ataque passivo tenta aprender ou usar informações do sistema, mas não afeta os recursos do sistema. Um ataque ativo tenta alterar os recursos do sistema ou afetar sua operação.

- Os **ataques passivos** são da natureza de espionagem ou monitoramento de transmissões. O objetivo do invasor é obter informações que estão sendo transmitidas.

- Os **ataques ativos** envolvem alguma modificação do fluxo de dados ou a criação de um fluxo falso e podem ser subdivididos em quatro categorias: repetição, mascaramento, modificação de mensagens e negação de serviço.

Requisitos Funcionais de Segurança

- **Controle de acesso**: Limitar o acesso ao sistema de informação a usuários autorizados, processos que agem em nome de usuários autorizados ou dispositivos (incluindo outros sistemas de informação) e aos tipos de transações e funções que os usuários autorizados têm permissão para exercer.

- **Conscientização e Treinamento**: Assegurar que os gestores e usuários dos sistemas de informação organizacionais estejam cientes dos riscos de segurança associados às suas atividades e das leis, regulamentos e políticas aplicáveis relacionadas à segurança dos sistemas de informação organizacionais; e garantir que o pessoal seja adequadamente treinados para desempenhar suas funções e responsabilidades relacionadas à segurança da informação.

- **Auditoria e Responsabilidade:** Criar, proteger e reter registros de auditoria do sistema de informação na medida necessária para permitir o monitoramento, análise, investigação e comunicação de informações ilegais, não autorizadas, ou atividade inadequada do sistema de informação; e garantir que as ações de usuários individuais do sistema de informação possam ser rastreadas exclusivamente para esses usuários para que possam ser responsabilizados por suas ações.

- **Certificação, Acreditação e Avaliações de Segurança:** Avaliar periodicamente os controles de segurança nos sistemas de informação organizacionais para determinar se os controles são eficazes em sua aplicação; desenvolver e implementar planos de ação destinados a corrigir deficiências e reduzir ou eliminar vulnerabilidades nos sistemas de informação organizacionais; autorizar a operação de sistemas de informação organizacional e quaisquer conexões de sistemas de informação associados; e monitorar continuamente os controles de segurança do sistema de informação para assegurar a continuidade da eficácia dos controles.

- **Gerenciamento de Configuração:** Estabelecer e manter configurações básicas e inventários de sistemas de informações organizacionais (incluindo hardware, software, firmware e documentação) ao longo dos respectivos ciclos de vida de desenvolvimento do sistema; e estabelecer e aplicar configurações de segurança para produtos de tecnologia da informação empregados em sistemas de informações organizacionais.

- **Planejamento de Contingência:** Estabelecer, manter e implementar planos de resposta a emergências, operações de backup e recuperação pós-desastre para sistemas de informação organizacionais para garantir a disponibilidade de recursos de informação críticos e continuidade das operações em situações de emergência.

- **Identificação e autenticação:** Identifique usuários do sistema de informação, processos que agem em nome de usuários ou dispositivos e autentique (ou verifique) as identidades desses usuários, processos ou dispositivos, como pré-requisito para permitir o acesso aos sistemas de informações organizacionais.

- **Resposta a Incidentes:** Estabelecer uma capacidade operacional de tratamento de incidentes para sistemas de informações organizacionais que inclua atividades adequadas de preparação, detecção, análise, contenção, recuperação e resposta ao usuário; e rastrear, documentar e relatar incidentes aos funcionários e/ou autoridades organizacionais apropriados.

- **Manutenção**: Realizar manutenções periódicas e pontuais nos sistemas de informação organizacionais; e fornecer controles eficazes sobre as ferramentas, técnicas, mecanismos e pessoal usado para realizar a manutenção do sistema de informação.

- **Proteção de Mídia:** Proteger a mídia do sistema de informação, tanto em papel quanto digital; limitar o acesso às informações na mídia do sistema de informação a usuários autorizados; e higienizar ou destruir a mídia do sistema de informação antes do descarte ou liberação para reutilização.

- **Proteção Física e Ambiental:** Limitar o acesso físico aos sistemas de informação, equipamentos e respectivos ambientes operacionais a pessoas autorizadas; proteger a planta física e a infraestrutura de suporte aos sistemas de informação; fornecer utilitários de suporte para sistemas de informação; proteger os sistemas de informação contra os riscos ambientais; e fornecer controles ambientais apropriados em instalações que contenham sistemas de informação.

- **Planejamento:** Desenvolver, documentar, atualizar periodicamente e implementar planos de segurança para sistemas de informação organizacionais que descrevam os controles de segurança em vigor ou planejados para os

sistemas de informação e as regras de comportamento para os indivíduos que acessam os sistemas de informação.

- **Segurança do Pessoal:** Garantir que os indivíduos que ocupem cargos de responsabilidade nas organizações (incluindo prestadores de serviços terceirizados) sejam confiáveis e atendam aos critérios de segurança estabelecidos para esses cargos; garantir que as informações organizacionais e os sistemas de informação sejam protegidos durante e após as ações de pessoal, como rescisões e transferências; e aplicar sanções formais para o pessoal que não cumprir as políticas e procedimentos de segurança organizacional.

- **Avaliação de Riscos:** Avalie periodicamente o risco para as operações organizacionais (incluindo missão, funções, imagem ou reputação), ativos organizacionais e indivíduos, resultantes da operação de sistemas de informações organizacionais e do processamento, armazenamento ou transmissão de informações organizacionais associados.

- **Aquisição de Sistemas e Serviços:** Alocar recursos suficientes para proteger adequadamente os sistemas de informação organizacional; empregar processos de ciclo de vida de desenvolvimento de sistemas que incorporem considerações de segurança da informação; empregar restrições de uso e instalação de software; e garantir que os provedores terceirizados empreguem medidas de segurança adequadas para proteger informações, aplicativos e/ou serviços terceirizados da organização.

- **Proteção do Sistema e das Comunicações:** Monitorar, controlar e proteger as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informação organizacionais) nos limites externos e nos limites internos principais dos sistemas de informação; e empregar projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de

engenharia de sistemas que promovam a segurança da informação efetiva dentro dos sistemas de informação organizacionais.

- **Integridade do Sistema e da Informação:** Identificar, reportar e corrigir informações e falhas do sistema de informação em tempo hábil; fornecer proteção contra códigos maliciosos em locais apropriados nos sistemas de informações organizacionais; e monitorar alertas e avisos de segurança do sistema de informação e tomar medidas apropriadas em resposta.

Metodologias de Segurança da Informação

Apesar de anos de pesquisa e desenvolvimento, não foi possível desenvolver técnicas de projeto e implementação de segurança que excluam sistematicamente falhas de segurança e impeçam todas as ações não autorizadas. Na ausência de tais técnicas infalíveis, é útil ter um conjunto de princípios de projeto amplamente aceitos que possam orientar o desenvolvimento de mecanismos de proteção. Vejamos alguns dos métodos mais utilizados:

- Economia de mecanismo
- Padrões à prova de falhas
- Mediação completa
- Design aberto
- Separação de privilégio
- Último privilégio
- Mecanismo menos comum

- Aceitabilidade psicológica
- Isolamento
- Encapsulamento
- Modularidade
- Camadas

Vejamos cada um desses princípios agora:

Economia de mecanismo significa que o projeto de medidas de segurança incorporadas em hardware e software deve ser o mais simples e pequeno possível. A motivação para este princípio é que o design relativamente simples e pequeno é mais fácil de testar e verificar minuciosamente. Com um design complexo, há muito mais oportunidades para um adversário descobrir fraquezas sutis para explorar que podem ser difíceis de detectar com antecedência. Quanto mais complexo o mecanismo, maior a probabilidade de possuir falhas exploráveis. Mecanismos simples tendem a ter menos falhas exploráveis e requerem menos manutenção.

O **padrão à prova de falhas** significa que as decisões de acesso devem ser baseadas na permissão e não na exclusão. Ou seja, a situação padrão é a falta de acesso, e o esquema de proteção identifica as condições sob as quais o acesso é permitido. Essa abordagem exibe um modo de falha melhor do que a abordagem alternativa, em que o padrão permite o acesso. Um erro de projeto ou implementação em um mecanismo que dá permissão explícita tende a falhar ao recusar a permissão, uma situação segura que pode ser detectada rapidamente.

A **mediação completa** significa que cada acesso deve ser verificado em relação ao mecanismo de controle de acesso. Os sistemas não devem depender de decisões

de acesso recuperadas de um cache. Em um sistema projetado para operar continuamente, esse princípio exige que, se as decisões de acesso forem lembradas para uso futuro, seja dada uma consideração cuidadosa sobre como as mudanças na autoridade são propagadas em tais memórias locais. Os sistemas de acesso a arquivos parecem fornecer um exemplo de sistema que atende a esse princípio.

Design aberto significa que o design de um mecanismo de segurança deve ser aberto e não secreto. Por exemplo, embora as chaves de criptografia devam ser secretas, os algoritmos de criptografia devem ser abertos ao escrutínio público. Os algoritmos podem ser revisados por muitos especialistas e, portanto, os usuários podem ter alta confiança neles.

A **separação de privilégio** é definida como uma prática em que vários atributos de privilégio são necessários para obter acesso a um recurso restrito. Um bom exemplo disso é a autenticação de usuário multifatorial, que requer o uso de várias técnicas, como senha e cartão inteligente, para autorizar um usuário. O termo agora também é aplicado a qualquer técnica na qual um programa é dividido em partes que são limitadas aos privilégios específicos de que necessitam para executar uma tarefa específica. Isso é usado para mitigar o dano potencial de um ataque à segurança do computador.

Privilégio mínimo significa que cada processo e cada usuário do sistema deve operar usando o menor conjunto de privilégios necessários para executar a tarefa. Um bom exemplo do uso desse princípio é o controle de acesso baseado em função. A política de segurança do sistema pode identificar e definir as várias funções de usuários ou processos. Cada função recebe apenas as permissões necessárias para executar suas funções. Cada permissão especifica um acesso permitido a um recurso específico (como acesso de leitura e gravação a um arquivo ou diretório especificado e acesso de conexão a um determinado host e porta). A menos que a permissão seja concedida explicitamente, o usuário ou processo não poderá acessar o recurso protegido. De maneira mais geral, qualquer sistema de

controle de acesso deve permitir a cada usuário apenas os privilégios autorizados para esse usuário.

Mecanismo menos comum significa que o design deve minimizar as funções compartilhadas por diferentes usuários, proporcionando segurança mútua. Esse princípio ajuda a reduzir o número de caminhos de comunicação não intencionais e reduz a quantidade de hardware e software dos quais todos os usuários dependem, tornando mais fácil verificar se existem implicações de segurança indesejáveis.

A **aceitabilidade psicológica** implica que os mecanismos de segurança não interfiram indevidamente no trabalho dos usuários, ao mesmo tempo em que atendem às necessidades de quem autoriza o acesso. Se os mecanismos de segurança dificultam a usabilidade ou acessibilidade dos recursos, os usuários podem optar por desativá-los. Sempre que possível, os mecanismos de segurança devem ser transparentes para os usuários do sistema ou, no máximo, apresentar uma obstrução mínima. Além de não serem intrusivos ou onerosos, os procedimentos de segurança devem refletir o modelo mental de proteção do usuário. Se os procedimentos de proteção não fizerem sentido para o usuário ou se o usuário precisar traduzir sua imagem de proteção em um protocolo substancialmente diferente, o usuário provavelmente cometerá erros.

O **isolamento** é um princípio que se aplica em três contextos. Primeiro, os sistemas de acesso público devem ser isolados de recursos críticos (dados, processos, etc.) para evitar divulgação ou adulteração. Nos casos em que a sensibilidade ou a criticidade das informações é alta, as organizações podem querer limitar o número de sistemas nos quais esses dados são armazenados e isolá-los, física ou logicamente. O isolamento físico pode incluir a garantia de que não existe conexão física entre os recursos de informação de acesso público de uma organização e as informações críticas de uma organização. Ao implementar soluções de isolamento lógico, devem ser estabelecidas camadas de serviços e mecanismos de segurança entre sistemas públicos e sistemas seguros responsáveis pela proteção de recursos críticos. Em segundo lugar, os processos e arquivos de usuários individuais devem

ser isolados uns dos outros, exceto onde for explicitamente desejado. Todos os sistemas operacionais modernos oferecem recursos para esse isolamento, de modo que os usuários individuais tenham espaço de processo, espaço de memória e espaço de arquivo separados e isolados, com proteções para impedir o acesso não autorizado. E, finalmente, os mecanismos de segurança devem ser isolados no sentido de impedir o acesso a esses mecanismos.

O **encapsulamento** pode ser visto como uma forma específica de isolamento com base na funcionalidade orientada a objetos. A proteção é fornecida pelo encapsulamento de uma coleção de procedimentos e objetos de dados em um domínio próprio, de modo que a estrutura interna de um objeto de dados seja acessível apenas aos procedimentos do subsistema protegido e os procedimentos possam ser chamados apenas em pontos de entrada de domínio designados.

A **modularidade** no contexto da segurança refere-se tanto ao desenvolvimento de funções de segurança como módulos separados e protegidos quanto ao uso de uma arquitetura modular para projeto e implementação de mecanismos. Com relação ao uso de módulos de segurança separados, o objetivo do projeto aqui é fornecer funções e serviços de segurança comuns, como funções criptográficas, como módulos comuns. Por exemplo, vários protocolos e aplicativos fazem uso de funções criptográficas. Em vez de implementar essas funções em cada protocolo ou aplicativo, um design mais seguro é fornecido pelo desenvolvimento de um módulo criptográfico comum que pode ser invocado por vários protocolos e aplicativos. O esforço de projeto e implementação pode então se concentrar no projeto seguro e na implementação de um único módulo criptográfico, incluindo mecanismos para proteger o módulo contra adulteração. Com relação ao uso de uma arquitetura modular, cada mecanismo de segurança deve ser capaz de suportar a migração para uma nova tecnologia ou atualização de novos recursos sem exigir um redesenho completo do sistema. O projeto de segurança deve ser modular para que partes individuais do projeto de segurança possam ser atualizadas sem a necessidade de modificar todo o sistema.

Camadas refere-se ao uso de várias abordagens de proteção sobrepostas que abordam as pessoas, a tecnologia e os aspectos operacionais dos sistemas de informação. Ao usar várias abordagens de proteção sobrepostas, a falha ou a evasão de qualquer abordagem de proteção individual não deixará o sistema desprotegido. Veremos que uma abordagem de camadas é frequentemente usada para fornecer várias barreiras entre um adversário e informações ou serviços protegidos. Esta técnica é muitas vezes referida como defesa em profundidade.

Menor susto significa que um programa ou interface de usuário deve sempre responder da maneira que menos provavelmente surpreenderá o usuário. Por exemplo, o mecanismo de autorização deve ser transparente o suficiente para que o usuário tenha uma boa compreensão intuitiva de como as metas de segurança são mapeadas para o mecanismo de segurança fornecido.

Superfícies de Ataque

Uma superfície de ataque consiste nas vulnerabilidades alcançáveis e exploráveis em um sistema. Exemplos de superfícies de ataque são os seguintes:

- Portas abertas na Web e outros servidores voltados para o exterior e escuta de código nessas portas
- Serviços disponíveis no interior de um firewall
- Código que processa dados de entrada, e-mail, XML, documentos diversos e formatos de troca de dados personalizados específicos do setor
- Interfaces, SQL e formulários da Web
- Um funcionário com acesso a informações confidenciais vulneráveis a um ataque de engenharia social

As superfícies de ataque podem ser categorizadas da seguinte maneira:

- **Superfície de ataque de rede:** esta categoria refere-se a vulnerabilidades em uma rede corporativa, rede de longa distância ou Internet. Incluídas nesta categoria estão vulnerabilidades de protocolo de rede, como aquelas usadas para um ataque de negação de serviço, interrupção de links de comunicação e várias formas de ataques de intrusos.

- **Superfície de ataque de software:** Refere-se a vulnerabilidades no código do aplicativo, utilitário ou sistema operacional. Um foco particular nesta categoria é o software de servidor Web.

- **Superfície de ataque humano:** esta categoria refere-se a vulnerabilidades criadas por pessoal ou pessoas de fora, como engenharia social, erro humano e insiders confiáveis.

Estratégia de Segurança da Informação

Uma estratégia de segurança abrangente envolve três aspectos:

- Especificação/política: O que o esquema de segurança deve fazer?

- Implementação/mecanismos: Como faz?

- Correção/garantia: Isso realmente funciona?

Política de segurança

O primeiro passo na criação de serviços e mecanismos de segurança é desenvolver uma política de segurança. Os envolvidos com segurança de computadores usam o termo política de segurança de várias maneiras. No mínimo, uma política de segurança é uma descrição informal do comportamento desejado do sistema. Essas políticas informais podem fazer referência a requisitos de segurança, integridade e disponibilidade. Mais útil, uma política de segurança é uma

declaração formal de regras e práticas que especificam ou regulam como um sistema ou organização fornece serviços de segurança para proteger recursos de sistemas sensíveis e críticos. Essa política de segurança formal se presta a ser aplicada pelos controles técnicos do sistema, bem como por seus controles operacionais e gerenciais.

Ao desenvolver uma política de segurança, um gerente de segurança precisa considerar os seguintes fatores:

- O valor dos ativos protegidos
- As vulnerabilidades do sistema
- Ameaças potenciais e a probabilidade de ataques

Implementação de segurança

A implementação de segurança envolve quatro cursos de ação complementares:

- **Prevenção:** Um esquema de segurança ideal é aquele em que nenhum ataque é bem-sucedido. Embora isso não seja prático em todos os casos, há uma ampla gama de ameaças nas quais a prevenção é um objetivo razoável. Por exemplo, considere a transmissão de dados criptografados. Se um algoritmo de criptografia seguro for usado e se houver medidas para impedir o acesso não autorizado às chaves de criptografia, os ataques à confidencialidade dos dados transmitidos serão evitados.
- **Detecção:** Em vários casos, a proteção absoluta não é viável, mas é prático detectar ataques de segurança. Por exemplo, existem sistemas de detecção de intrusão projetados para detectar a presença de indivíduos não autorizados conectados a um sistema. Outro exemplo é a detecção de um ataque de negação de serviço, em que recursos de comunicação ou processamento são consumidos para que fiquem indisponíveis para usuários legítimos.

- **Resposta:** Se os mecanismos de segurança detectarem um ataque em andamento, como um ataque de negação de serviço, o sistema poderá responder de forma a interromper o ataque e evitar mais danos.

- **Recuperação:** Um exemplo de recuperação é o uso de sistemas de backup, para que, caso a integridade dos dados seja comprometida, uma cópia anterior e correta dos dados possa ser recarregada.

Criptografia

Um elemento importante em muitos serviços e aplicativos de segurança de computadores é o uso de algoritmos criptográficos. Teremos aqui uma visão geral dos vários tipos de algoritmos, juntamente com uma discussão de sua aplicabilidade. Para cada tipo de algoritmo, apresentamos os algoritmos padronizados mais importantes de uso comum.

Confidencialidade com Criptografia Simétrica

A técnica universal para fornecer confidencialidade para dados transmitidos ou armazenados é a criptografia simétrica. Esta seção apresenta o conceito básico de criptografia simétrica. Isso é seguido por uma visão geral dos dois algoritmos de criptografia simétrica mais importantes: o Data Encryption Standard (DES) e o Advanced Encryption Standard (AES), que são algoritmos de criptografia de bloco.

Criptografia Simétrica

A criptografia simétrica, também conhecida como criptografia convencional ou criptografia de chave única, era o único tipo de criptografia em uso antes da introdução da criptografia de chave pública no final da década de 1970. Incontáveis indivíduos e grupos, de Júlio César à força alemã de submarinos até os atuais usuários diplomáticos, militares e comerciais, criptografia simétrica usada para comunicação secreta. Resta o mais amplamente utilizado dos dois tipos de criptografia.

Um esquema de criptografia simétrica tem cinco componentes:

- **Texto simples:** Esta é a mensagem original ou dados que são alimentados no algoritmo como entrada.

- **Algoritmo de criptografia:** O algoritmo de criptografia realiza várias substituições e transformações no texto simples.

- **Chave secreta:** A chave secreta também é inserida no algoritmo de criptografia. As substituições e transformações exatas realizadas pelo algoritmo dependem da chave.

- **Texto cifrado:** Esta é a mensagem codificada produzida como saída. Depende do texto simples e da chave secreta. Para uma determinada mensagem, duas chaves diferentes produzirão dois textos cifrados diferentes.

- **Algoritmo de descriptografia:** Este é essencialmente o algoritmo de criptografia executado em sentido inverso. Ele pega o texto cifrado e a chave secreta e produz o texto simples original.

Existem dois requisitos para o uso seguro da criptografia simétrica:

- Precisamos de um **algoritmo de criptografia forte.** No mínimo, gostaríamos que o algoritmo fosse tal que um oponente que conhecesse o algoritmo e tivesse acesso a um ou mais textos cifrados fosse incapaz de decifrar o texto cifrado ou descobrir a chave. Esse requisito geralmente é declarado de forma mais forte: o oponente deve ser incapaz de decifrar o texto cifrado ou descobrir a chave, mesmo que possua vários textos cifrados juntamente com o texto simples que produziu cada texto cifrado.

- O remetente e o destinatário devem ter obtido **cópias da chave secreta** de forma segura e devem manter a chave segura. Se alguém puder descobrir a

chave e conhecer o algoritmo, toda a comunicação usando essa chave será legível.

Existem duas abordagens gerais para atacar um esquema de criptografia simétrica. O primeiro ataque é conhecido como criptoanálise. Os **ataques criptanalíticos** dependem da natureza do algoritmo, mais talvez algum conhecimento das características gerais do texto simples ou mesmo alguns pares de amostra de texto simples-texto cifrado. Este tipo de ataque explora as características do algoritmo para tentar deduzir um texto simples ou para deduzir a chave que está sendo usada. Se o ataque conseguir deduzir a chave, o efeito é catastrófico: todas as mensagens futuras e passadas criptografadas com essa chave são comprometidas.

O segundo método, conhecido como **ataque de força bruta**, é tentar todas as chaves possíveis em um pedaço de texto cifrado até que uma tradução inteligível em texto simples seja obtida. Em média, metade de todas as chaves possíveis devem ser tentadas para alcançar o sucesso. Ou seja, se houver x chaves diferentes, em média, um invasor descobrirá a chave real após x/2 tentativas.

Algoritmos de criptografia de bloco simétrico

Os algoritmos de criptografia simétrica mais usados são as cifras de bloco. Uma cifra de bloco processa a entrada de texto simples em blocos de tamanho fixo e produz um bloco de texto cifrado de tamanho igual para cada bloco de texto simples. O algoritmo processa quantidades de texto simples mais longas como uma série de blocos de tamanho fixo.

Data Encryption Standard

Até recentemente, o esquema de criptografia mais utilizado era baseado no **Data Encryption Standard (DES)** adotado em 1977 pelo National Bureau of Standards, agora National Institute of Standards and Technology (NIST). O algoritmo em si é referido como o **Algoritmo de Criptografia de Dados (DEA).** O DES usa um bloco

de texto simples de 64 bits e uma chave de 56 bits para produzir um bloco de texto cifrado de 64 bits.

DES triplo

A vida do DES foi estendida pelo uso do **DES triplo (3DES)**, que envolve a repetição do algoritmo DES básico três vezes, usando duas ou três chaves exclusivas, para um tamanho de chave de 112 ou 168 bits. O 3DES foi padronizado pela primeira vez para uso em aplicações financeiras no padrão ANSI X9.17 em 1985.

Padrão de criptografia avançada Por causa de suas desvantagens, o 3DES não é um candidato razoável para uso a longo prazo. Como substituto, o NIST em 1997 lançou uma chamada para propostas para um novo **Padrão de Criptografia Avançada (AES)**, que deveria ter uma força de segurança igual ou melhor que 3DES e eficiência significativamente melhorada. Além desses requisitos gerais, o NIST especificou que o AES deve ser uma cifra de bloco simétrica com um comprimento de bloco de 128 bits e suporte para comprimentos de chave de 128, 192 e 256 bits.

Autenticação de Mensagens e Funções Hash.

A criptografia protege contra ataques passivos (escutas). Um requisito diferente é proteger contra ataques ativos (falsificação de dados e transações). A proteção contra tais ataques é conhecida como autenticação de mensagens ou dados.

Uma mensagem, arquivo, documento ou outra coleção de dados é considerada autêntica quando é genuína e veio de sua suposta fonte. A autenticação de mensagens ou dados é um procedimento que permite que as partes comunicantes verifiquem se as mensagens recebidas ou armazenadas são autênticas. Os dois aspectos importantes são verificar se o conteúdo da mensagem não foi alterado e se a fonte é autêntica. Também podemos verificar a pontualidade de uma mensagem (ela não foi atrasada e reproduzida artificialmente) e a sequência em relação a outras mensagens que fluem entre duas partes.

Autenticação usando criptografia simétrica

Parece possível realizar a autenticação simplesmente pelo uso de criptografia simétrica.

Se presumirmos que apenas o remetente e o destinatário compartilham uma chave (como deveria ser), apenas o remetente genuíno poderá criptografar uma mensagem com sucesso para o outro participante, desde que o destinatário possa reconhecer uma mensagem válida.

Além disso, se a mensagem incluir um código de detecção de erro e um número de sequência, o receptor tem a garantia de que nenhuma alteração foi feita e que a sequência é adequada. Se a mensagem também incluir um carimbo de data/hora, o receptor terá a garantia de que a mensagem não foi atrasada além do normalmente esperado para o trânsito da rede.

Autenticação de mensagem sem criptografia de mensagem

Examinamos algumas abordagens para autenticação de mensagens que não dependem de criptografia de mensagens. Em todas essas abordagens, uma etiqueta de autenticação é gerada e anexada a cada mensagem para transmissão. A mensagem em si não é criptografada e pode ser lida no destino independentemente da função de autenticação no destino.

Como as abordagens vistas até aqui não criptografam a mensagem, a confidencialidade da mensagem não é fornecida. Como foi mencionado, a criptografia de mensagens por si só não fornece uma forma segura de autenticação. No entanto, é possível combinar autenticação e confidencialidade em um único algoritmo criptografando uma mensagem mais sua tag de autenticação.

Criptografia de Chave Pública

Estrutura de criptografia de chave pública

A criptografia de chave pública, proposta publicamente pela primeira vez por Diffie e Hellman em 1976, é o primeiro avanço verdadeiramente revolucionário na criptografia em literalmente milhares de anos.

Os algoritmos de chave pública são baseados em funções matemáticas e não em operações simples em padrões de bits, como os usados em algoritmos de criptografia simétrica. Mais importante, a criptografia de chave pública é assimétrica, envolvendo o uso de duas chaves separadas, em contraste com a criptografia simétrica, que usa apenas uma chave. O uso de duas chaves tem consequências profundas nas áreas de confidencialidade, distribuição de chaves e autenticação.

Um esquema de criptografia de chave pública tem seis componentes:

- **Texto simples:** Esta é a mensagem ou dados legíveis que são alimentados no algoritmo como entrada.

- **Algoritmo de criptografia:** O algoritmo de criptografia realiza várias transformações no texto simples.

- **Chave pública e privada:** Este é um par de chaves que foram selecionadas para que, se uma for usada para criptografia, a outra será usada para descriptografar. As transformações exatas realizadas pelo algoritmo de criptografia dependem da chave pública ou privada fornecida como entrada.7

- **Texto cifrado:** Esta é a mensagem codificada produzida como saída. Depende do texto simples e da chave. Para uma determinada mensagem, duas chaves diferentes produzirão dois textos cifrados diferentes.

- **Algoritmo de descriptografia:** Este algoritmo aceita o texto cifrado e a chave correspondente e produz o texto simples original.

Aplicações para Criptossistemas de Chave Pública

Os sistemas de chave pública são caracterizados pelo uso de um tipo de algoritmo criptográfico com duas chaves, uma privada e outra disponível publicamente. Dependendo da aplicação, o remetente usa a chave privada do remetente ou a chave pública do destinatário, ou ambas, para realizar algum tipo de função criptográfica. Em termos gerais, podemos classificar o uso de criptossistemas de chave pública em três categorias: **assinatura digital**, **distribuição de chaves simétricas** e **criptografia de chaves secretas**.

Lei Geral de Proteção de Dados – LGPD

LEI Nº 13.709, DE 14 DE AGOSTO DE 2018

A Lei Geral de Proteção de Dados Pessoais (LGPD) vem para proteger os direitos fundamentais de liberdade e de privacidade e a livre formação da personalidade de cada indivíduo. A lei dispõe sobre o tratamento de dados feito por pessoa física ou jurídica de direito público ou privado e engloba um amplo conjunto de operações efetuadas em meios manuais ou digitais.

Vale para: dados relacionados à pessoa (brasileira ou não) que esteja no Brasil, no momento da coleta; dados tratados dentro do território nacional, independentemente do meio aplicado, do país-sede do operador ou do país onde se localizam os dados; dados usados para fornecimento de bens ou serviços.

Não se aplica para fins exclusivamente: jornalísticos e artísticos; de segurança pública; de defesa nacional; de segurança do Estado; de investigação e repressão de infrações penais; particulares (ou seja, a lei só se aplica para pessoa física ou jurídica que gerencie bases com fins ditos econômicos). E não se aplica a dados de fora do Brasil e que não sejam objeto de transferência internacional.

Atores envolvidos

A LGPD prevê algumas definições e papéis que você deve compreender:

- O **titular de dados:** é a pessoa a quem se referem os dados pessoais;

- **Controlador:** uma empresa pode ser considerada controladora quando toma as decisões em relação ao uso dos dados pessoais que possui (obs: utilizamos o termo "empresa", como um exemplo. A LGPD determina que o controlador pode ser uma pessoa natural ou jurídica, de direito público ou privado. Além de empresas, estão submetidos à LGPD: organizações, ONGs, órgãos da administração pública etc.);

- **Operador:** é a empresa que apenas irá realizar o processamento de dados de acordo com as ordens do controlador, sem poder de decisão sobre o uso dos dados;

- **Encarregado (DPO):** é um novo cargo previsto na lei. O encarregado (ou Data Protection Officer) é a pessoa nomeada pelo controlador para coordenar as ações de adequação interna da empresa, além de atuar como canal de comunicação com o titular e com a Autoridade Nacional de Proteção de Dados (ANPD).

Fundamentos da LGPD

O tema proteção de dados pessoais, na LGPD, tem como fundamentos:

- o respeito à privacidade, ao assegurar os direitos fundamentais de inviolabilidade da intimidade, da honra, da imagem e da vida privada

- a autodeterminação informativa, ao expressar o direito do cidadão ao controle, e assim, à proteção de seus dados pessoais e íntimos

- a liberdade de expressão, de informação, de comunicação e de opinião, que são direitos previstos na Constituição brasileira

- o desenvolvimento econômico e tecnológico e a inovação, a partir da criação de um cenário de segurança jurídica em todo o país

- a livre iniciativa, a livre concorrência e a defesa do consumidor, por meio de regras claras e válidas para todo o setor privado

- os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas

Itens abordados pela LGPD

Dados Pessoais: O dado pessoal é aquele que permite, sozinho ou em conjunto com outros, a identificação de seu titular. Por meio dele, é possível descobrir nome, apelido, endereço de residência, e-mail, endereço IP, números de cartões e cookies. São dados que as empresas devem garantir proteção, sendo utilizados somente para os fins autorizados pelo dono desses dados.

Dados Sensíveis: A lei também visa à proteção dos dados sensíveis, que contêm características ainda mais reveladoras sobre uma pessoa. Alguns exemplos de dados sensíveis são: religião, etnia, sexo, posicionamento político, biometria, dados bancários e outras que permitam que um sistema ou ferramenta faça segmentação de grupos. Essas informações exigem um cuidado ainda maior da empresa que se dispõe a armazenar e fazer o tratamento.

Tratamento de Dados: O tratamento de dados faz referência à utilização dos dados do usuário. Ou seja: o que a empresa faz ou pretende fazer com as informações coletadas? Essas intenções devem estar claras para o usuário, que deverá consentir o uso dos dados para estes fins. Um exemplo é a comunicação entre bancos. Sem a

LGPD, os bancos interligam os dados dos seus clientes. Dessa forma, os dados bancários e financeiros do cliente de um banco podem ser consultados por outro banco, ainda que isso não seja uma prática ética ou legal. Com a LGPD, o usuário terá garantida sua proteção ao crédito, já que ele terá que dar permissão para que seus dados possam ser comunicados entre bancos. É importante reforçar que todas as autorizações devem estar explícitas e claras, ou seja, não serão válidos os consentimentos que forem dados a partir de letras miúdas ou textos muito longos e complexos, que possam confundir o usuário. Esse consentimento, transparente e direto, é o que garante às empresas o direito de tratar os dados coletados, de acordo com os termos acordados.

Titular dos Dados: Titular dos dados é qualquer pessoa física que tenha passado dados e informações pessoais, de maneira virtual ou não. O titular dos dados tem direitos sobre os seus dados, incluindo o direito ao esquecimento. Se a pessoa estiver com dados sendo expostos em algum site, por exemplo, ainda que ela tenha autorizado a exposição no passado, se quiser retirar, ela tem direito à remoção imediata do conteúdo.

Outros direitos fundamentais da LGPD ao usuário são o direito ao acesso e o direito da informação, que permitem que ele saiba quais dados estão sendo armazenados pela empresa e o porquê. O artigo 18 da LGPD prevê que o titular dos dados pode solicitar, a qualquer momento e sem necessidade de justificativas:

- Confirmação da existência de tratamento dos seus dados;

- O acesso aos seus dados;

Correção de dados incompletos, inexatos ou desatualizados:

- Anonimização, bloqueio ou eliminação de dados tratados em desconformidade com a LGPD;

- Portabilidade dos dados a outro fornecedor de serviço ou produto;
- Eliminação dos dados pessoais tratados;
- Informações das entidades públicas e privadas com as quais o controlador compartilhou os dados do usuário;
- Informações sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;
- Revogação do consentimento;
- Revisão por pessoa natural de decisões automatizadas.

O objetivo de dar ao titular os dados o controle total sobre suas informações é evitar que empresas se utilizem de brechas legais (ou desconhecimento dos usuários) para utilizar os dados a seu favor, como aconteceu no famoso caso da Cambridge Analytica.

Consentimento aos Dados: Quando falamos em dados, não temos como fugir do setor de TI. Afinal, é nessa área que as informações são processadas, armazenadas e tratadas. Portanto, a responsabilidade de seus profissionais aumenta a partir da lei.

Um dos fatores primordiais será a adoção do Privacy by Design. Ou seja: a privacidade passa a ser incorporada à arquitetura dos sistemas, dando acesso ao titular dos dados e permitindo o gerenciamento, a coleta e o tratamento de modo autônomo. Caberá ao setor de TI disponibilizar e incorporar esse novo modelo aos negócios.

Penalidades por Descumprir a LGPD

Um ponto que é importante trazer é que qualquer empresa que tenha contato ou relação com brasileiros devem se adequar à LGPD.

Isso significa que empresas do exterior, ainda que de países sem legislação específica sobre o assunto, também devem respeitar e cumprir os termos da lei brasileira.

No caso da empresa descumprir a LGPD, poderá ter suas atividades relacionadas a tratamento de dados interrompidas ou completamente proibidas.

O descumprimento parcial, ou seja, as não conformidades, também trazem prejuízos. As multas podem corresponder a 2% do faturamento da empresa ou limitadas a R$ 50 milhões por infração.

No art. 52 da LGPD, constam todas as sanções para caso de descumprimento. Confira:

I – advertência, com indicação de prazo para adoção de medidas corretivas;

II – multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;

III – multa diária, observado o limite total a que se refere o inciso II;

IV – publicização da infração após devidamente apurada e confirmada a sua ocorrência;

V – bloqueio dos dados pessoais a que se refere a infração até a sua regularização;

VI – eliminação dos dados pessoais a que se refere a infração.

Não existe, ainda, um órgão específico para regular a lei e as penalidades para as empresas. Dessa forma, as partes ambíguas da lei que dependem de interpretação podem acabar custando muito dinheiro à empresa.

Portanto, é fundamental que as empresas providenciem todas as adequações necessárias e esperadas com a entrada da LGPD em vigor, revendo processos, planos de contingência e sistemas, se necessário.

Referência Bibliográfica

TANENBAUM, Andrew S. **Redes de Computadores**. Trad. 4. ed. Rio de Janeiro: Campus, 2003.

Ir para exercício