Tópicos Especiais - Segurança da Informação

Segurança dos Ativos

O que é um ativo ?

Em segurança da informação, o termo “ativo” se refere a tudo o que é importante e tem valor para uma empresa. Os ativos podem ser divididos em duas categorias: tangíveis e intangíveis.

temos basicamente dois ativos: **tangíveis** e **intangíveis**:

Ativos Tangíveis são os elementos físicos que compõem a infraestrutura de TI da empresa, como computadores, servidores, cabos, roteadores, switches etc. Também incluem os espaços físicos onde esses elementos estão localizados, como prédios, salas ou armários. Esses ativos são vulneráveis a riscos como roubo, furto, incêndio, inundação ou sabotagem.

Ativos Intangíveis são os elementos lógicos que contêm as informações da empresa, como dados, arquivos, documentos, contratos, planos, projetos etc. Também incluem o conhecimento que os funcionários possuem sobre os processos e as tecnologias da empresa. Esses ativos são vulneráveis a riscos como invasão, vazamento, corrupção ou perda.

Proteger esses ativos é essencial para a continuidade e a competitividade do negócio. Se algo der errado, a empresa pode sofrer prejuízos financeiros, danos à sua reputação ou sanções legais.. É como garantir que tudo o que é valioso para a empresa esteja seguro e em bom estado.

2.1 Precisamos entender agora a classificação da informação, isso implica como os dados serão manipulados e processados conforme sua classificação.

Abaixo temos os níveis de classificação da informação:

- **Informação Pública -** é aquela que pode ser divulgada livremente para qualquer pessoa ou entidade, sem que isso cause prejuízo à organização. Exemplos: Nome da empresa, o endereço do site, relatório anual, missão e valores, evite ao máximo sobrecarga na efetividade dessas informações.

- **Informação Internas (Sensíveis) -** é aquela que deve ser restrita aos membros da organização ou a terceiros autorizados. São exemplos de informação interna: os procedimentos operacionais, as políticas internas, os dados dos funcionários, os planos de marketing.
  A divulgação não autorizada desta informação pode causar danos moderados à organização, afetando a sua competitividade ou reputação.

- **Informações Confidenciais** - é aquela que deve ser protegida com o mais alto grau de segurança, pois a sua divulgação não autorizada pode causar danos graves à organização. São exemplos de informação confidencial: os dados dos clientes, os contratos comerciais, as informações financeiras, as estratégias de negócio.

- **Informações Confidenciais** - A informação confidencial deve ser acessada apenas por pessoas que tenham uma necessidade legítima e que estejam sujeitas a acordos de confidencialidade. Além disso, deve-se utilizar mecanismos de segurança como criptografia, autenticação e controle de acesso para garantir a confidencialidade e a integridade dessa informação.

- **Informações Restritas (Privada/Confidencial)** - é aquela que deve ser protegida com o mais alto nível de segurança possível, pois a sua divulgação não autorizada pode causar danos catastróficos à organização. São exemplos de informações restritas: os segredos comerciais, as patentes, as informações sensíveis do governo.

- **Informações Restritas (Privada/Confidencial)** - informação restrita deve ser acessada apenas por um número muito limitado de pessoas que tenham uma autorização especial e que estejam sujeitas a rigorosas medidas de segurança. Essas pessoas devem assinar termos de responsabilidade e compromisso para evitar qualquer vazamento ou uso indevido dessa informação.

Para classificar as informações de forma adequada, é preciso levar em conta alguns fatores que determinam o seu nível de proteção necessário. Os principais critérios de classificação são:

Valor:

Requisitos Legais:

Sensibilidade:

Criticidade:

Valor: É o grau de importância da informação para a organização e para os seus objetivos. Quanto maior o valor, maior o nível de proteção necessário. O valor pode ser avaliado considerando, por exemplo, a contribuição da informação para a receita, a competitividade ou a reputação da organização.

Requisitos legais: São as obrigações impostas por leis, normas ou contratos que regulam o tratamento das informações. Algumas informações podem ter um nível de confidencialidade definido por lei, como é o caso dos dados pessoais sensíveis previstos na LGPD.

Sensibilidade: É o grau de exposição da informação a riscos internos ou externos. Quanto maior a sensibilidade, maior o nível de proteção necessário. A sensibilidade pode ser medida considerando, por exemplo, o impacto potencial da divulgação não autorizada, da modificação ou da destruição da informação.

Criticidade: É o grau de essencialidade da informação para as operações contínuas da organização. Quanto maior a criticidade, maior o nível de proteção necessário. A criticidade pode ser avaliada considerando, por exemplo, o tempo máximo tolerável de indisponibilidade ou perda da informação.

Responsabilidades do Proprietário dos Dados

O papel do proprietário dos dados é crucial para garantir a conformidade e a proteção adequada dos dados pessoais. De acordo com a LGPD, o proprietário é a figura central que detém a autoridade para decidir sobre o tratamento dos dados.

Classificação dos Dados:
Monitoramento e Atualização:
Implementação de Controles de Segurança:
Gestão de Acesso:
Proteção dos Direitos dos Titulares:

Tão importante quanto as práticas e políticas formais é a promoção de uma cultura de conscientização sobre a segurança da informação. Todos os colaboradores, independentemente do nível hierárquico, devem entender a importância de proteger os ativos de informação.

Algumas estratégias para cultivar essa cultura incluem:

Treinamentos Regulares

Simulações

Reconhecimento e Recompensas

Feedback Contínuo

2.2 Propriedade e Responsabilidade

No mundo digital atual, é fundamental compreender quem possui e quem cuida dos dados. Esse aspecto é essencial para a segurança da informação, pois define as responsabilidades e os direitos dos agentes envolvidos no tratamento dos dados.

Propriedade dos Dados

A propriedade dos dados é um conceito que define quem tem o direito legal e a responsabilidade de gerenciar uma informação. Existem dois atores principais: o **titular dos dados**, que é a pessoa física a quem os dados se referem, e o **controlador dos dados**, que é a entidade ou organização que coleta e processa esses dados.

Titular dos Dados: É quem fornece os dados, seja de forma voluntária ou como requisito para acessar determinado serviço ou produto.

O titular dos dados tem os seguintes direitos:

Acesso

Correção

Exclusão

Informação

Portabilidade

Controlador dos Dados: É quem reúne e processa os dados fornecidos pelo titular, para uma finalidade específica e legítima. O controlador dos dados tem os seguintes direitos:

Uso

Armazenamento

Transferência

Proteção

Conformidade

Custodiante dos Dados

O custodiante dos dados é um profissional que atua como um guardião, encarregado de zelar pela integridade e segurança das informações que não são de sua propriedade, mas que estão sob sua responsabilidade.

Deveres do Custodiante dos Dados:

Proteção - Implementar e manter atualizadas medidas de segurança para defender os dados.

Manutenção - Garantir o armazenamento correto dos dados, realizar backups e assegurar a recuperação da informação.

Conformidade - Trabalhar em alinhamento com políticas internas e externas como leis e normas.

Usuário dos Dados

Os usuários dos dados são aqueles que interagem diretamente com as informações, seja para consulta, edição ou outros fins operacionais. Embora não sejam os guardiões primários dos dados, têm um papel crucial no ecossistema de segurança da informação.

Deveres do Usuário de Dados:

Uso adequado desses dados
Adesão às Normas
Comunicação Proativa

Exemplo Prática:

Titular dos Dados: João Silva, Cliente da Loja Virtual ABC.
Forneceu seus dados como endereço, nome e informações de cartão de crédito.
João pode a qualquer momento e alterar esse dados caso seja necessário.

Exemplo Prática:

Controlador dos Dados: Loja Virtual ABC.

Eles coletaram e processaram os dados do João para enviar por exemplo um produto que ele comprou.

A loja usa esses dados para enviar o produto ao endereço correto e processar o pagamento. Armazenando esses dados de forma segura e só compartilha dados necessários.

Custodiante dos Dados.

A Equipe de Ti da Loja Virtual ABC.

Eles garantem que o site esteja seguro e que os dados dos clientes, como joão, estejam protegidos de qualquer ataque.

Eles fazem backups regulares para evitar perda de informação e estão sempre atualizando o sistema para proteger contra qualquer tipo de ameaça.

2.3 Ciclo de Vida dos Dados

O Ciclo de Vida dos Dados é um processo que inclui várias fases, tais como criação, **processamento**, **armazenamento**, **uso**, **compartilhamento**, **arquivamento** e **descarte de dados**. Cada fase tem suas próprias práticas e considerações de segurança, que são fundamentais para proteger as informações contra acessos não autorizados, perdas ou vazamentos.

Criação de Dados:

A fase inicial do ciclo de vida dos dados é a sua criação. Aqui, os dados podem ser gerados internamente, como documentos, planilhas, ou através de transações online, bem como podem ser obtidos de fontes externas.

Coleta e Processamento:

Nesta etapa, os dados são coletados para serem processados conforme as necessidades operacionais. Durante o processamento, os dados são transformados, organizados ou analisados para extrair informações úteis.

Durante estas fases, deve-se garantir que os dados sejam manipulados e armazenados de forma segura, mantendo sua precisão e confiabilidade através de controles e políticas de segurança rigorosos.

Armazenamento:

O armazenamento refere-se à manutenção segura dos dados em diversos meios, como servidores, nuvens ou bases de dados. Durante esta fase, é crucial assegurar que os dados estejam protegidos contra acessos não autorizados e ameaças, como vazamentos ou ataques cibernéticos.

Transmissão:

Na fase de transmissão, os dados são transferidos entre locais, sistemas ou partes interessadas. Aqui, a integridade e a confidencialidade dos dados devem ser rigorosamente mantidas, utilizando protocolos de transmissão seguros, como HTTPS, e métodos de encriptação robustos para evitar interceptações maliciosas ou perda de dados.

Uso:

Durante o uso, os dados são acessados e manipulados por usuários autorizados. Políticas de controle de acesso e monitoramento contínuo são essenciais para garantir que os dados sejam utilizados de maneira apropriada e eticamente responsável, e para evitar o uso indevido ou o acesso não autorizado às informações.