

Sistemas de Informação

Aula 8

A Segurança da Tecnologia da Informação

Por que os Controles São Necessários



- Os controles são necessários para garantir a qualidade e segurança dos recursos de hardware, software, redes e dados dos sistemas de informação
- Os computadores provaram que podem processar grandes volumes de dados e executar cálculos complexos de modo mais preciso do que os sistemas manuais ou mecânicos

Por que os Controles São Necessários



- Os computadores estão sujeitos à:
 - Erros em seus sistemas
 - Utilização indevida para fins fraudulentos
 - Terem seus sistemas e/ou seus recursos de software e dados destruídos acidental ou deliberadamente

Por que os Controles São Necessários



- Os controles eficazes fornecem segurança dos sistemas de informação, ou seja:
 - A precisão, integridade e segurança das atividades e recursos dos sistemas de informação. Os controles podem minimizar erros, fraude e destruição nos sistemas de informação interconectados que hoje ligam entre si usuários finais e organizações

Por que os Controles São Necessários



- Fornecem garantia de qualidade para os sistemas de informação. Ou seja, eles podem deixar um sistema de informação computadorizado mais livre de erros e fraude e capaz de fornecer produtos de informação de qualidade mais alta do que os tipos manuais de processamento da informação
- Reduzem o impacto negativo potencial (e aumentam o impacto positivo) que a tecnologia da informação pode produzir na sobrevivência e sucesso das empresas e na qualidade de vida na sociedade

Por que os Controles São Necessários



- Três tipos principais de controle devem ser desenvolvidos para garantir a qualidade e segurança dos sistemas de informação.
- Essas categorias de controle incluem:
 - Controles de sistemas de informação
 - Controles de procedimentos
 - Controles de instalações

Controles dos Sistemas de Informação



- Os controles dos sistemas de informação são métodos e dispositivos que procuram garantir a precisão, validade e propriedade das atividades dos sistemas de informação
- Os controles devem ser desenvolvidos para garantir a forma correta de:
 - Entrada de dados
 - Técnicas de processamento
 - Métodos de armazenamento
 - Saída de informações

Controles dos Sistemas de Informação



- Os controles dos sistemas de informação são projetados para monitorar e manter a qualidade e segurança das atividades de entrada, processamento, saída e armazenamento de um sistema de informação.

Controles de Entrada



- A expressão GIGO (garbage in, garbage out, ou “entra lixo, sai lixo”) explica a necessidade de controles de entrada
- Esses controles incluem:
 - Senhas e outros códigos de segurança
 - Telas formatadas para entrada de dados
 - Sinais audíveis de erro
 - Máscaras para as teclas de dispositivos de entrada acionados por teclas
 - Formulários pré-gravados e pré-numerados.

Controles de Entrada



- Sistemas de tempo real que podem registrar todas as entradas no sistema em registros de controle em fita magnética que preservam evidência de todas as entradas no sistema. Isto pode incluir a realização de “checagens de razoabilidade” para determinar se os dados introduzidos excedem certos limites especificados ou estão fora de ordem. Isto inclui o cálculo e monitoração de totais de controle (contagem de registros, totais de lotes [batch totals] e totais parciais [hash totals])

Controles de Processamento



- Uma vez que os dados tenham sido registrados corretamente em um sistema, eles devem ser corretamente processados
- Os controles de processamento identificam erros em cálculos aritméticos e operações lógicas
- Eles também são utilizados para garantir que os dados não se percam ou fiquem sem processamento
- Os controles de processamento podem incluir controles de hardware e controles de software

Controles de Hardware



- Os controles de hardware são verificações especiais embutidas no hardware para verificar a precisão do processamento do computador
- Exemplos de controles de hardware incluem:
 - Circuitos de Detecção de Falhas
 - Componentes Redundantes
 - Microprocessadores de Finalidades Especiais e Circuitos Associados

Controles de Hardware



- **Circuitos de Detecção de Falhas**
São os circuitos encontrados dentro do computador utilizados para monitorar suas operações – por exemplo, verificações de paridade, verificações pelo eco, verificações de circuitos redundantes, verificações de sinais aritméticos e verificações de sincronização e voltagem da CPU
- **Componentes Redundantes**
São dispositivos que verificam e promovem a exatidão de atividades de leitura e gravação – por exemplo, múltiplas cabeças de leitura e gravação em unidades de fita e disco magnético

Controles de Hardware



- **Microprocessadores de Finalidades Especiais e Circuitos Associados**
São dispositivos como chaves que podem ser utilizados para apoiar diagnósticos e manutenção à distância. Estes permitem aos técnicos o diagnóstico e correção de alguns problemas via links de rede com o computador

Controles de Software



- Os controles de software têm o objetivo de garantir que os dados corretos estão sendo processados
- Exemplos de controles de software incluem
 - Rótulos de arquivos internos que permitem que o computador garanta que o arquivo correto de armazenamento está sendo utilizado e que os dados corretos no arquivo foram processados.

Controles de Software



- O estabelecimento de pontos de verificação durante o processamento de um programa. Os pontos de verificação são pontos intermediários dentro de um programa que está sendo processado, onde os resultados intermediários são gravados em fita ou disco magnético ou listados em uma impressora. Os pontos de verificação minimizam o efeito de erros de processamento e também ajudam a construir uma trilha de auditoria [audit trail], que permite que as transações em processamento sejam acompanhadas ao longo de todas as etapas de processamento

Controles de Software



- Pacotes de software de sistemas especializados conhecidos como monitores de segurança de sistemas são programas que monitoram o uso de um sistema de computador e protegem seus recursos contra uso não autorizado, fraude e destruição

Controles de Saída



- Os controles de saída são desenvolvidos para garantir que os produtos de informação estejam corretos e completos e estejam disponíveis de maneira oportuna a usuários autorizados. Exemplos de controles de saída são:
 - Documentos e relatórios de saída que são freqüentemente registrados, identificados com revisões de rota e visualmente checados pelo pessoal de entrada/saída

Controles de Saída



- Totais de controle sobre a saída que normalmente são comparados com os totais de controle gerados durante as etapas de entrada e processamento
- Listagens de controle que podem ser produzidas fornecendo evidência em papel para toda saída produzida
- Formulários de saída pré-numerados que podem ser usados para controlar a perda de documentos importantes

Controles de Saída



- Listas de distribuição que garantem que apenas os usuários autorizados recebem saída
- Acesso à saída que pode ser controlado por códigos de segurança que identificam os usuários que podem receber saída e o tipo de saída que eles estão autorizados a receber
- Usuários finais que recebem saída que devem ser incentivados a fornecer feedback sobre a qualidade da saída

Controles de Armazenamento



- Os recursos de armazenamento de dados são uma importante consideração
- As responsabilidades de controle para arquivos de programas de computador e bancos de dados organizacionais podem envolver:
 - Atribuir as responsabilidades de controle a especialistas de centros de dados e administradores de bancos de dados

Controles de Armazenamento



- Garantir a proteção contra uso não autorizado ou acidental utilizando programas de segurança que exigem identificação apropriada antes de poderem ser utilizados.
- Utilizar códigos de contas, senhas e outros códigos de segurança para permitir acesso apenas a usuários autorizados
- Outros controles de armazenamento que podem utilizar tecnologias de criptografia e cartão inteligente

Controles de Armazenamento



- Estabelecer um catálogo de usuários autorizados para permitir ao sistema de computador identificar usuários qualificados e determinar que tipos de informação eles estão autorizados a receber
- Ter arquivos de reserva, que são arquivos duplicados que podem ser armazenados em um local distante do centro de computação
- Proteger arquivos utilizando medidas de retenção de arquivo que envolvem cópias de armazenamento de arquivos mestre e arquivos de transações de períodos anteriores

Controles de Armazenamento



- Manter diversas gerações de arquivos para fins de controle (arquivos filho, pai, avô, etc.)

Controles de Instalações



- Controles de instalações são métodos que protegem as instalações de computação e redes de uma organização e seu conteúdo contra a perda ou destruição
- As redes e centros de computação estão sujeitos a casualidades como: acidentes, desastres naturais, sabotagem, vandalismo, uso não autorizado, espionagem industrial, destruição e roubo de recursos

Segurança de Rede



- A segurança de uma rede pode ser fornecida por pacotes de software de sistemas especializados conhecidos como monitores de segurança de sistemas
- Os monitores de segurança de sistemas são programas que monitoram o uso de sistemas e redes de computadores e os protegem do uso não autorizado, fraude e destruição. Esses programas fornecem:

Segurança de Rede



- As medidas de segurança necessárias para permitir que apenas usuários autorizados acessem as redes
- Os monitores de segurança também controlam o uso dos recursos de hardware, software e dados de um sistema de computador
- Os programas de segurança monitoram o uso de redes de computadores e coletam estatísticas sobre quaisquer tentativas de uso impróprio. Em seguida, produzem relatórios para ajudar na manutenção da segurança da rede

Criptografia



- A criptografia de dados tornou-se uma maneira importante de proteger dados e outros recursos de rede de computadores, principalmente na Internet, intranets e extranets
- Características da criptografia incluem:
 - Senhas, mensagens, arquivos e outros dados que podem ser transmitidos de forma embaralhada e desembaralhados pelos sistemas de computadores apenas para usuários autorizados

Criptografia



- O uso de algoritmos matemáticos especiais, ou chaves, para transformar dados digitais em um código embaralhado antes que esses dados sejam transmitidos e para decodificá-los quando forem recebidos
- O método mais amplamente utilizado de criptografia que utiliza um par de chaves públicas e privadas exclusivas de cada indivíduo. Um e-mail, por exemplo, poderia ser embaralhado e codificado utilizando uma única chave pública para o destinatário, que é conhecida pelo remetente. Após a transmissão do e-mail, apenas a chave privada secreta do destinatário poderia desembaralhar a mensagem

Criptografia



- Os programas de criptografia que são vendidos como produtos independentes ou embutidos em outro software utilizado para o processo de criptografia.

Firewall



- Outro método importante para controle e segurança na Internet e outras redes é o uso de computadores e software
- Características de computadores e software Firewall incluem:
 - Um Firewall de rede é um sistema de computador “guardião” que protege as intranets e outras redes de computadores de uma empresa contra a invasão, funcionando como um filtro e ponto seguro de transferência para acesso à e da Internet e outras redes

Firewall



- Um computador de rede Firewall filtra todo o tráfego de rede em busca de senhas corretas ou outros códigos de segurança e somente permite transmissões autorizadas para dentro e para fora da rede
- Os Firewalls se tornaram um componente essencial de organizações que se conectam com a Internet, em virtude da vulnerabilidade e falta de segurança da Internet

Firewall



- Os Firewalls podem deter, mas não evitar inteiramente, o acesso não autorizado (hacking) às redes de computadores. Em alguns casos, um Firewall pode permitir acesso apenas a partir de locais credenciados na Internet para determinados computadores dentro do Firewall. Ou pode permitir que apenas informações “seguras” sejam transmitidas

Firewall



- Em alguns casos, é impossível saber se o uso de um determinado serviço de rede é seguro ou inseguro e, por isso, todos os pedidos devem ser bloqueados. O Firewall pode então fornecer substitutos para alguns serviços de rede que desempenham a maioria das mesmas funções mas que são menos vulneráveis a invasão

Controles de Proteção Física



- Fornecer segurança máxima e proteção contra desastres para os recursos de computação de uma organização exige diversos tipos de controle
- O acesso a centros de computação e áreas de trabalho do usuário final, por exemplo, é permitido apenas ao pessoal autorizado por técnicas como:
 - Símbolos de identificação
 - Fechaduras eletrônicas
 - Alarmes contra roubo
 - Polícia de segurança
 - Circuito fechado de TV e outros sistemas de detecção

Controles de Procedimentos



- Os centros de computação podem ser protegidos de desastres por salvaguardas como:
 - Sistemas de detecção e extinção de incêndio
 - Caixas fortes de armazenamento à prova de incêndio para a proteção de arquivos
 - Sistemas de energia elétrica de emergência
 - Escudos eletromagnéticos
 - Controles de temperatura, umidade e poeira.

Controles Biométricos



- Os controles biométricos são medidas de segurança fornecidas por dispositivos de computador que medem características físicas que tornam cada indivíduo único. Isto inclui:
 - Verificação de voz
 - Análise de digitação
 - Impressões digitais
 - Escaneamento de retina

Controles Biométricos



- Geometria de mão
- Reconhecimento facial
- Dinâmica de assinatura
- Análise de padrões genéticos

Controles de Falhas no Computador



- Uma série de controles é necessária para evitar falhas de computador ou minimizar seus efeitos
- Os de computadores podem falhar em virtude de:
 - Queda de energia
 - Defeitos nos circuitos eletrônicos
 - Problemas na rede de telecomunicações

Controles de Falhas no Computador



- Erros de programação ocultos
- Erros do operador do computador
- Vandalismo eletrônico

Controles de Falhas no Computador



- O departamento de serviços de informação normalmente toma medidas para evitar a falha no equipamento e minimizar seus efeitos prejudiciais. Por exemplo:
 - Programas de manutenção preventiva de hardware e administração de atualizações de software são comuns.
 - Utilizar computadores dotados de capacidades de manutenção automática e à distância.

Controles de Falhas no Computador



- Estabelecer padrões para fornecimento de energia elétrica, ar condicionado, controle de umidade e padrões de prevenção de incêndio
- Obter uma capacidade de backup de um sistema de computador com organizações de recuperação de desastres.
- Programar e implementar principais mudanças de hardware ou software para evitar problemas.
- Treinamento e supervisão de operadores de computadores.
- Utilizar sistemas de computação tolerantes a falhas (capacidades à prova de falhas e tolerante a falhas)

Tolerância a Falhas



- Esses sistemas evitam a falha do computador utilizando múltiplas CPUs, periféricos e software de sistemas
 - Sistemas à Prova de Falhas: se refere a sistemas de computador que continuam a operar no mesmo nível de desempenho depois de uma falha maior
 - Sistemas Tolerantes a Falhas: se refere a sistemas de computador que continuam a operar em um nível reduzido, porém aceitável, depois de uma falha do sistema.

Controles de Procedimentos



- Controles de procedimentos são métodos que especificam como os recursos de computadores e redes de uma organização devem ser operados para a segurança máxima
- Eles facilitam a precisão e integridade das operações dos computadores e das atividades de desenvolvimento de sistemas. Isto inclui:
 - Padrões de procedimento e documentação
 - Requisitos de Autorização
 - Recuperação de Desastres
 - Controles para a Computação pelo Usuário Final

Procedimentos-padrão



- Normalmente, uma organização de SI desenvolve e adota procedimentos padrão para a operação de sistemas de informação
- Os procedimentos padrão promovem a qualidade e minimizam as chances de erros e fraude
- Eles ajudam usuários finais e especialistas de SI a saberem o que se espera deles em termos de procedimentos operacionais e qualidade de sistemas

Procedimentos-padrão



- Além disso, a documentação do projeto de software e dos sistemas e a operação do sistema devem ser desenvolvidas e mantidas atualizadas
- A documentação também é inestimável na manutenção de um sistema à medida que são feitos os melhoramentos necessários

Requisitos de Autorização



- Os pedidos de desenvolvimento de sistemas, alterações de programas ou processamento de computação normalmente são submetidos a uma revisão formal pela administração antes de ser dada a autorização
- A autorização minimiza os efeitos prejudiciais sobre a precisão e integridade das operações em curso de sistemas e redes

Recuperação de Desastres



- Furacões, terremotos, incêndios, enchentes, atos terroristas e criminosos e falha humana podem danificar seriamente os recursos de computação de uma organização
- Muitas organizações como companhias aéreas e bancos, por exemplo, são incapacitadas até pela perda de algumas horas de poder de computação
- É por isso que é importante que as organizações desenvolvam procedimentos de recuperação de desastres e os formalizem em um plano de recuperação de desastres

Recuperação de Desastres



- Esse plano especifica quais funcionários participarão na recuperação do desastre e quais serão suas obrigações; que hardware, software e instalações serão utilizados e a prioridade das aplicações que serão processadas
- Acordos com outras empresas para o uso de instalações alternativas como local de recuperação de desastres e armazenamento externo dos bancos de dados de uma organização também fazem parte de um esforço eficaz de recuperação de desastres

Controles para a Computação pelo Usuário Final



- Muitas aplicações desenvolvidas pelo usuário final estão desempenhando funções organizacionais extremamente importantes que são decisivas para o sucesso e sobrevivência da empresa
- Elas podem muitas vezes ser chamadas de aplicações do usuário final críticas à empresa
- Os controles envolvidos nas aplicações dos usuários finais devem ser os mesmos que aqueles que constituem prática padrão no desenvolvimento de aplicações por departamentos de profissionais de SI

Auditoria de Sistemas de Informação



- Um departamento de serviços de informação deve ser periodicamente examinado pelo pessoal de auditoria interna da empresa
- Auditorias periódicas realizadas por auditores externos de firmas de contabilidade profissional constituem uma boa prática de negócios
- Tais auditorias devem revisar e avaliar se foram desenvolvidos e implementados controles corretos e adequados dos sistemas de informação, controles de procedimento, controles de instalações e outros controles administrativos

Auditoria de Sistemas de Informação



- Existem duas abordagens básicas para auditoria de sistemas de informação – ou seja, a realização de auditoria das atividades de processamento de informações dos sistemas de informação computadorizados
- Essas abordagens são conhecidas como:
 - Auditoria em torno do computador
 - Auditoria por meio do computador

Auditoria em torno do computador



- A auditoria em torno do computador envolve a verificação da precisão e propriedade de entrada e saída do computador produzida sem avaliação do software que processou os dados
- Vantagens desse método:
 - Método simples e fácil que não exige auditores com experiência em programação.
- Desvantagens deste método:
 - Não acompanha uma transação ao longo de todas as suas etapas de processamento
 - Não testa a precisão e integridade do software utilizado

Auditoria por meio do computador



- A auditoria por meio do computador envolve a verificação da precisão e integridade do software que processa os dados, bem como da entrada de dados e saída produzidos pelos sistemas e redes de computadores
- Vantagens deste método:
 - Testa a precisão e integridade dos programas de computador.
 - Testa a entrada e saída do sistema de computador.

Auditoria por meio do computador



- Desvantagens deste método:
 - Exige um conhecimento do sistema de computador e operações de rede e desenvolvimento de software
 - Dispendioso para algumas aplicações de computador

Auditoria de Sistemas de Informação



- Um dos objetivos importantes desses procedimentos de auditoria é testar a integridade da trilha de auditoria de uma aplicação
- Uma trilha de auditoria pode ser definida como a presença de documentação que permite que uma transação seja rastreada ao longo de todas as etapas de seu processamento de informações

Auditoria de Sistemas de Informação



- A trilha de auditoria dos sistemas de informação manuais são bastante visíveis e fáceis de rastrear, entretanto, os sistemas de informação baseados em computador alteraram a forma da trilha de auditoria.

Bibliografia



- Sistemas de Informação e as Decisões Gerenciais na Era da Internet - James A. O'Brien - Editora: Saraiva