Segurança da Informação

A segurança da informação diz respeito à proteção de determinados dados, com a intenção de preservar seus respectivos valores para uma organização (empresa) ou um indivíduo. Podemos entender como informação todo o conteúdo ou dado valioso para um indivíduo/organização, que consiste em qualquer conteúdo com capacidade de armazenamento ou transferência, que serve a determinado propósito e que é de utilidade do ser humano.

Atualmente, a informação digital é um dos principais produtos de nossa era e necessita ser convenientemente protegida. A segurança de determinadas informações pode ser afetadas por vários fatores, como os comportamentais e do usuário, pelo ambiente/infraestrutura em que ela se encontra e por pessoas que têm o objetivo de roubar, destruir ou modificar essas informações.

Confidencialidade, disponibilidade e integridade são algumas das características básicas da segurança da informação, e podem ser consideradas até mesmo atributos.

• Confidencialidade – Diz respeito à inacessibilidade da informação, que não pode ser divulgada para um usuário, entidade ou processo não autorizado;

• Integridade – A informação não deve ser alterada ou excluída sem autorização;

• Disponibilidade – Acesso aos serviços do sistema/máquina para usuários ou entidades autorizadas.

Toda vulnerabilidade de um sistema ou computador pode representar possibilidades de ponto de ataque de terceiros.

Esse tipo de segurança não é somente para sistemas computacionais, como imaginamos. Além de também envolver informações eletrônicas e sistemas de armazenamento, esse tipo de segurança também se aplica a vários outros aspectos e formas de proteger, monitorar e cuidar de dados.

Segurança da Informação está relacionada com proteção de um conjunto de dados, no sentido de preservar o valor que possuem para um indivíduo ou uma organização. São características básicas da segurança da informação os atributos de confidencialidade, integridade e disponibilidade, não estando esta segurança restrita somente a sistemas computacionais, informações eletrônicas ou sistemas de armazenamento. O conceito se aplica a todos os aspectos de proteção de informações e dados. O conceito de Segurança Informática ou Segurança de Computadores está intimamente relacionado com o de Segurança da Informação, incluindo não apenas a segurança dos dados/informação, mas também a dos sistemas em si.

Atualmente o conceito de Segurança da Informação está padronizado pela norma ISO/IEC 17799:2005, influenciada pelo padrão inglês (British Standard) BS 7799. A série de normas ISO/IEC 27000 foram reservadas para tratar de padrões de Segurança da Informação, incluindo a complementação ao trabalho original do padrão inglês. A ISO/IEC 27002:2005 continua sendo considerada formalmente como 17799:2005 para fins históricos.

Conceitos

A Segurança da Informação se refere à proteção existente sobre as informações de uma determinada empresa ou pessoa, isto é, aplica-se tanto as informações corporativas quanto às pessoais. Entende-se por informação todo e qualquer conteúdo ou dado que tenha valor para alguma organização ou pessoa. Ela pode estar guardada para uso restrito ou exposta ao público para consulta ou aquisição.

Podem ser estabelecidas métricas (com o uso ou não de ferramentas) para a definição do nível de segurança existente e, com isto, serem estabelecidas as bases para análise da melhoria ou piora da situação de segurança existente. A segurança de uma determinada informação pode ser afetada por fatores comportamentais e de uso de quem se utiliza dela, pelo ambiente ou infra-estrutura que a cerca ou por pessoas mal intencionadas que têm o objetivo de furtar, destruir ou modificar tal informação.

A tríade CIA (Confidentiality, Integrity and Availability) -- Confidencialidade, Integridade e Disponibilidade -- representa os principais atributos que, atualmente, orientam a análise, o planejamento e a implementação da segurança para um determinado grupo de informações que se deseja proteger. 0

Outros atributos importantes são a irretratabilidade e a autenticidade. Com o evoluir do comércio electrónico e da sociedade da informação, a privacidade é também uma grande preocupação.

Os atributos básicos (segundo os padrões internacionais) são os seguintes:

• **Confidencialidade** - propriedade que limita o acesso a informação tão somente às entidades legítimas, ou seja, àquelas autorizadas pelo proprietário da informação.

• **Integridade** - propriedade que garante que a informação manipulada mantenha todas as características originais estabelecidas pelo proprietário da informação, incluindo controle de mudanças e garantia do seu ciclo de vida (nascimento,manutenção e destruição).

• **Disponibilidade** - propriedade que garante que a informação esteja sempre disponível para o uso legítimo, ou seja, por aqueles usuários autorizados pelo proprietário da informação.

O nível de segurança desejado, pode se consubstanciar em uma "política de segurança" que é seguida pela organização ou pessoa, para garantir que uma vez estabelecidos os princípios, aquele nível desejado seja perseguido e mantido.

Para a montagem desta política, deve-se levar em conta:

• Riscos associados à falta de segurança;

• Benefícios;

• Custos de implementação dos mecanismos.

Mecanismos de Segurança

O suporte para as recomendações de segurança pode ser encontrado em:

• Controles físicos: são barreiras que limitam o contato ou acesso direto a informação ou a infra-estrutura (que garante a existência da informação)que a suporta. Existem mecanismos de segurança que apóiam os controles físicos: Portas / trancas / paredes / blindagem / guardas / etc...

• Controles lógicos: são barreiras que impedem ou limitam o acesso a informação, que está em ambiente controlado, geralmente eletrônico, e que, de outro modo, ficaria exposta a alteração não autorizada por elemento mal intencionado.

• Existem mecanismos de segurança que apóiam os controles lógicos:

• Mecanismos de criptografia. Permitem a transformação reversível da informação de forma a torná-la ininteligível a terceiros.

• Utiliza-se para tal, algoritmos determinados e uma chave secreta para, a partir de um conjunto de dados não criptografados, produzir uma sequência de dados criptografados. A operação inversa é a decifração.

• Assinatura digital. Um conjunto de dados criptografados, associados a um documento do qual são função, garantindo a integridade do documento associado, mas não a sua confidencialidade.

• Mecanismos de garantia da integridade da informação. Usando funções de "Hashing" ou de checagem, consistindo na adição.

• Mecanismos de controle de acesso. Palavras-chave, sistemas biométricos, firewalls, cartões inteligentes.

• Mecanismos de certificação. Atesta a validade de um documento.

• Integridade. Medida em que um serviço/informação é genuino, isto é, esta protegido contra a personificação por intrusos.

• Honeypot: É o nome dado a um software, cuja função é detectar ou de impedir a ação de um cracker, de um spammer, ou de qualquer agente externo estranho ao sistema, enganando-o, fazendo-o pensar que esteja de fato explorando uma vulnerabilidade daquele sistema.

Existe hoje em dia um elevado número de ferramentas e sistemas que pretendem fornecer segurança. Alguns exemplos são os detectores de intrusões, os anti-vírus, firewalls, firewalls locais, filtros anti-spam, fuzzers, analisadores de código, etc.

O tema Segurança da Informação desperta muito interesse em várias audiências desde executivos e gerentes até técnicos. Isto ocorre, principalmente, porque a segurança cobre diversas áreas, tais como: segurança física, infraestrutura tecnológica, aplicações e conscientização organizacional, cada uma delas com seus próprios riscos, ameaças potenciais, controles aplicáveis e soluções de segurança que podem minimizar o nível de exposição ao qual a empresa está exposta, com o objetivo de garantir segurança para o seu principal patrimônio: a informação.

Normalmente, quando o assunto segurança é discutido, as pessoas associam o tema a hackers e vulnerabilidades em sistemas, onde o principal entendimento é de que a empresa precisa de um bom antivírus, um firewall e ter todos os seus “patches” aplicados no ambiente tecnológico. Não há dúvida de que são questões importantes, porém a Segurança da Informação não está limitada a somente esses pontos.

Um Gestor de Segurança da Informação (Security Officer), deve estar atento a itens como: ambiente, tecnologia, processos e pessoas. Em cada uma dessas vertentes surgem diversas iniciativas, por exemplo, Políticas, Normas e Procedimentos, Controle de Acesso (Físico e Lógico), Auditoria, Questões Legais, Continuidade de Negócios, Criptografia, Gerenciamento de Incidentes, Segurança da Rede, Conscientização dos Usuários, dentre outros.

Fundamentos e Conceitos da Segurança da Informação

Fundamentalmente a Segurança da Informação está calcada em três princípios básicos: Confidencialidade, Integridade e Disponibilidade.

Confidencialidade, diferente de ser um segredo ou algo inacessível, é um conceito no qual o acesso à informação deve ser concedido a quem de direito, ou seja, apenas para as entidades autorizadas pelo proprietário ou dono da informação.

Já o conceito de Integridade está ligado à propriedade de manter a informação armazenada com todas as suas características originais estabelecidas pelo dono da informação, tendo atenção com o seu ciclo de vida (criação, manutenção e descarte).

E por fim, o conceito de Disponibilidade deve garantir que a informação esteja sempre disponível para uso quando usuários autorizados necessitarem.

O estabelecimento de um Programa de Segurança da Informação em sua empresa deve passar sempre por ações que norteiem esses princípios. Tal modelo deve estar amparado por um Sistema de Gestão de Segurança da Informação que precisa ser planejado e organizado, implementado, mantido e monitorado.

Muitas organizações não seguem esta abordagem no desenvolvimento, implementação e manutenção de seu programa de gestão de segurança. Isso é porque talvez não conheçam, ou entendam que essa abordagem é de difícil implementação ou uma perda de tempo.

A política de segurança da informação nada mais é que um conjunto de práticas e controles adequados, formada por diretrizes, normas e procedimentos, com objetivo de minimizar os riscos com perdas e violações de qualquer bem. Se aplicada de forma correta ajudam a proteger as informações que são consideradas como um ativo importante dentro da organização.

Informação

Informação é um conjunto de dados, que processados ganham significado e tornam possível sua compreensão e interpretação. As informações constituem um dos objetos de grande valor para as empresas.

A ISO/IEC 13335-1/2004 caracteriza como ativo qualquer coisa que tenha valor para a organização. É considerado como ativo de informação todo bem da empresa que se relaciona com informação e que tenha valor para a organização, pode ser um componente humano, tecnológico, físico ou lógico que realize processos de negócio dentro da empresa.

Classificação da Informação

A classificação das informações norteia-se mediante ao impacto que causaria a sua perda, alteração ou uso sem permissão. Ferreira afirma que “quanto mais estratégica e decisiva para a manutenção ou sucesso da organização maior será sua importância”. (FERREIRA, 2008, p. 78)

Entre os níveis mais utilizados na classificação de informação estão: informação pública, informação interna e informação confidencial.

Segurança da Informação

Os princípios da segurança da informação abrangem basicamente os seguintes aspectos: confidencialidade, integridade e disponibilidade (CID), toda ação que possa comprometer um desses princípios pode ser tratada como atentado a sua segurança.

• Confidencialidade: É a garantia de que a informação é acessível somente por pessoas autorizadas a terem acesso.

• Integridade: É a preservação da exatidão da informação e dos métodos de processamento

• Disponibilidade: É a Garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

As informações estão sujeitas a ameaças e riscos devido suas vulnerabilidades. A ABNT ISSO/IEC 27002,2005 define risco como a combinação da probabilidade de um evento e de suas consequências.

Moreira (2001) aponta a vulnerabilidade como sendo o ponto onde qualquer sistema é suscetível a um ataque, condição causada muitas vezes pela ausência ou ineficiência das medidas de proteção.

Adachi (2004), que estudou a gestão da segurança em Internet Banking, agrupou os aspectos envolvidos na segurança da informação em três camadas: física, lógica e humana. Logo, se torna essencial que haja segurança em cada uma das três camadas.

A segurança física tem como objetivo proteger equipamentos e informações contra usuários não autorizados e prevenção de danos por causas naturais.

A segurança lógica aplica-se em casos onde um usuário ou processo da rede tenta obter acesso a um objeto que pode ser um arquivo ou outro recurso de rede (estação de trabalho, impressora, etc.), sendo assim, um conjunto de medida e procedimentos, adotados com objetivo de proteger os dados, programas e sistemas contra tentativas de acessos não autorizados, feitas por usuários ou outros programas.

Todos colaboradores da empresa fazem parte do fator humano, principalmente os que têm acesso direto aos recursos de T.I. Trata-se do fator mais difícil de se gerenciar e avaliar riscos.

Políticas de Segurança da Informação

A política de segurança define normas, procedimentos, ferramentas e responsabilidades às pessoas que lidam com essa informação, para garantir o controle e a segurança da informação na empresa. É formalmente o documento que dita quais são as regras aplicadas dentro da empresa para uso de recursos tecnológicos e descarte de informações.

A grosso modo, pode-se afirmar que com a implantação de uma política de segurança da informação é significativa a redução da probabilidade de ocorrência de quebra da confidencialidade, da integridade e da disponibilidade da informação, tal como a redução de danos causados por eventuais ocorrências.

A política, preferencialmente, deve ser criada antes da ocorrência de problemas com a segurança, ou depois, para evitar reincidências. Ela é uma ferramenta tanto para prevenir problemas legais como para documentar a aderência ao processo de controle de qualidade. (FERREIRA;FERNANDO, 2008, p.36)

Características e Benefícios

Para seu efetivo funcionamento, a política deve ter certas peculiaridades, tais como: ser verdadeira, ser válida para todos, ser simples, contar com o comprometimento dos gestores da empresa e outras. De nada adianta implantar uma política que não é coerente com as ações executadas pela empresa, pois isso impossibilita seu cumprimento.

Ferreira afirma que a curto prazo pode-se notar a prevenção de acessos não autorizados, danos ou interferências no andamento do negócio, além de já se conseguir maior segurança nos processos do negócio. Em médio prazo surge a padronização dos procedimentos, a adaptação já de forma segura de novos processos e a qualificação e quantificação de respostas a incidentes. E, a longo prazo, obtém-se o retorno do investimento, por meio da diminuição de problemas relacionados a incidentes de segurança da informação.

Considerações Finais

Nem sempre se pode ter o controle sobre as ameaças que geralmente originam-se de agentes externos, portanto, é essencial a redução das vulnerabilidades existentes para se minimizar o risco.

Existem diversas medidas de segurança que podem ser adotadas pelas empresas com o intuito de proteger suas informações, por isso, as políticas de segurança da informação são tão importantes, são elas que nortearão os colaboradores a como agir baseados em procedimentos pré-estabelecidos.

Conceitos de Segurança

A Segurança da Informação se refere à proteção existente sobre as informações de uma determinada empresa ou pessoa, isto é, aplica-se tanto as informações corporativas quanto às pessoais. Entende-se por informação todo e qualquer conteúdo ou dado que tenha valor para alguma organização ou pessoa. Ela pode estar guardada para uso restrito ou exposta ao público para consulta ou aquisição.

Podem ser estabelecidas métricas (com o uso ou não de ferramentas) para a definição do nível de segurança existente e, com isto, serem estabelecidas as bases para análise da melhoria ou piora da situação de segurança existente. A segurança de uma determinada informação pode ser afetada por fatores comportamentais e de uso de quem se utiliza dela, pelo ambiente ou infraestrutura que a cerca ou por pessoas mal intencionadas que têm o objetivo de furtar, destruir ou modificar tal informação.

A tríade CIA (Confidentiality, Integrity and Availability) -- Confidencialidade, Integridade e Disponibilidade -- representa os principais atributos que, atualmente, orientam a análise, o planejamento e a implementação da segurança para um determinado grupo de informações que se deseja proteger. Outros atributos importantes são a irretratabilidade, a autenticidade e a conformidade. Com a evolução do comércio eletrônico e da sociedade da informação, a privacidade é também uma grande preocupação.

Portanto os atributos básicos, segundo os padrões internacionais (ISO/IEC 17799:2005) são os seguintes:

Confidencialidade - propriedade que limita o acesso a informação tão somente às entidades legítimas, ou seja, àquelas autorizadas pelo proprietário da informação.
Integridade - propriedade que garante que a informação manipulada mantenha todas as características originais estabelecidas pelo proprietário da informação, incluindo controle de mudanças e garantia do seu ciclo de vida (nascimento,manutenção e destruição).
Disponibilidade - propriedade que garante que a informação esteja sempre disponível para o uso legítimo, ou seja, por aqueles usuários autorizados pelo proprietário da informação.
Autenticidade - propriedade que garante que a informação é proveniente da fonte anunciada e que não foi alvo de mutações ao longo de um processo.
Irretratabilidade - propriedade que garante a impossibilidade de negar a autoria em relação a uma transação anteriormente feita

Conformidade: propriedade que garante que o sistema deve seguir as leis e regulamentos associados a este tipo de processo.

Para a montagem desta política, deve-se levar em conta:

Riscos associados à falta de segurança;
Benefícios;
Custos de implementação dos mecanismos.

Mecanismos de segurança

O suporte para as recomendações de segurança pode ser encontrado em:

Controles físicos: são barreiras que limitam o contato ou acesso direto a informação ou a infraestrutura (que garante a existência da informação) que a suporta.

Existem mecanismos de segurança que apoiam os controles físicos:

Portas / trancas / paredes / blindagem / guardas / etc ..

Controles lógicos: são barreiras que impedem ou limitam o acesso a informação, que está em ambiente controlado, geralmente eletrônico, e que, de outro modo, ficaria exposta a alteração não autorizada por elemento mal intencionado.

Existem mecanismos de segurança que apóiam os controles lógicos:

Mecanismos de cifração ou encriptação: Permitem a transformação reversível da informação de forma a torná-la ininteligível a terceiros.

Utiliza-se para tal, algoritmos determinados e uma chave secreta para, a partir de um conjunto de dados não criptografados, produzir uma sequência de dados criptografados. A operação inversa é a decifração.

Assinatura digital: Um conjunto de dados criptografados, associados a um documento do qual são função, garantindo a integridade e autenticidade do documento associado, mas não a sua confidencialidade.
Mecanismos de garantia da integridade da informação: Usando funções de "Hashing" ou de checagem, é garantida a integridade através de comparação do resultado do teste local com o divulgado pelo autor.
Mecanismos de controle de acesso: Palavras-chave, sistemas biométricos, firewalls, cartões inteligentes.

Mecanismos de certificação: Atesta a validade de um documento. Integridade: Medida em que um serviço/informação é genuíno, isto é, está protegido contra a personificação por intrusos.

Honeypot: É uma ferramenta que tem a função de propositalmente simular falhas de segurança de um sistema e colher informações sobre o invasor enganando-o, fazendo-o pensar que esteja de fato explorando uma vulnerabilidade daquele sistema. É um espécie de armadilha para invasores. O HoneyPot não oferece nenhum tipo de proteção.

Protocolos seguros: Uso de protocolos que garantem um grau de segurança e usam alguns dos mecanismos citados aqui.

Existe hoje em dia um elevado número de ferramentas e sistemas que pretendem fornecer segurança. Alguns exemplos são os detectores de intrusões, os antivírus, firewalls, firewalls locais, filtros anti-spam, fuzzers, analisadores de código etc.1

Ameaças à Segurança

As ameaças à segurança da informação são relacionadas diretamente à perda de uma de suas 3 características principais, quais sejam:

Perda de Confidencialidade: seria quando há uma quebra de sigilo de uma determinada informação (ex: a senha de um usuário ou administrador de sistema) permitindo que sejam expostas informações restritas as quais seriam acessíveis apenas por um determinado grupo de usuários.

Perda de Integridade: aconteceria quando uma determinada informação fica exposta a manuseio por uma pessoa não autorizada, que efetua alterações que não foram aprovadas e não estão sob o controle do proprietário (corporativo ou privado) da informação.

Perda de Disponibilidade: acontece quando a informação deixa de estar acessível por quem necessita dela. Seria o caso da perda de comunicação com um sistema importante para a empresa, que aconteceu com a queda de um servidor ou de uma aplicação crítica de negócio, que apresentou uma falha devido a um erro causado por motivo interno ou externo ao equipamento ou por ação não autorizada de pessoas com ou sem má intenção.

No caso de ameaças à rede de computadores ou a um sistema, estas podem vir de agentes maliciosos, muitas vezes conhecidos como crackers, (hackers não são agentes maliciosos, pois tentam ajudar a encontrar possíveis falhas).

Estas pessoas são motivadas para fazer esta ilegalidade por vários motivos. Os principais são: notoriedade, auto-estima, vingança e o dinheiro. De acordo com pesquisa elaborada pelo Computer Security Institute ([1]), mais de 70% dos ataques partem de usuários legítimos de sistemas de informação (Insiders) -- o que motiva corporações a investir largamente em controles de segurança para seus ambientes corporativos (intranet).

Invasões na Internet

Todo sistema de computação necessita de um sistema para proteção de arquivos. Este sistema é um conjunto de regras que garantem que a informação não seja lida, ou modificada por quem não tem permissão. A segurança é usada especificamente para referência do problema genérico do assunto, já os mecanismos de proteção são usados para salvar as informações a serem protegidas.

A segurança é analisada de várias formas, sendo os principais problemas causados com a falta dela a perda de dados e as invasões de intrusos.

A perda de dados na maioria das vezes é causada por algumas razões: fatores naturais: incêndios, enchentes, terremotos, e vários outros problemas de causas naturais; Erros de hardware ou de software: falhas no processamento, erros de comunicação, ou bugs em programas; Erros humanos: entrada de dados incorreta, montagem errada de disco ou perda de um disco. Para evitar a perda destes dados é necessário manter um backup confiável, guardado longe destes dados originais.

Exemplos de Invasões

O maior acontecimento causado por uma invasão foi em 1988, quando um estudante colocou na internet um programa malicioso (worm), derrubando milhares de computadores pelo mundo, que foi identificado e removido logo após.

Mas até hoje há controvérsias de que ele não foi completamente removido da rede. Esse programa era feito em linguagem C, e não se sabe até hoje qual era o objetivo, o que se sabe é que ele tentava descobrir todas as senhas que o usuário digitava.

Mas esse programa se auto-copiava em todos os computadores em que o estudante invadia. Essa “brincadeira” não durou muito, pois o estudante foi descoberto pouco tempo depois, processado e condenado a liberdade condicional, e teve que pagar uma alta multa.

Um dos casos mais recentes de invasão por meio de vírus foi o do Vírus Conficker (ou Downup, Downadup e Kido) que tinha como objetivo afetar computadores dotados do sistema operacional Microsoft Windows, e que foi primeiramente detectado em outubro de 2008.

Uma versão anterior do vírus propagou-se pela internet através de uma vulnerabilidade de um sistema de rede do Windows 2000, Windows XP, Windows Vista, Windows Server 2003, Windows Server 2008, Windows 7 Beta e do Windows Server 2008 R2 Beta, que tinha sido lançado anteriormente naquele mês. O vírus bloqueia o acesso a websites destinados à venda, protegidos com sistemas de segurança e, portanto, é possível a qualquer usuário de internet verificar se um computador está infectado ou não, simplesmente por meio do acesso a websites destinados a venda de produtos dotados de sistemas de segurança.

Em janeiro de 2009, o número estimado de computadores infectados variou entre 9 e 15 milhões. Em 13 de fevereiro de 2009, a Microsoft estava oferecendo 250.000 dólares americanos em recompensa para qualquer informação que levasse à condenação e à prisão de pessoas por trás da criação e/ou distribuição do Conficker.

Em 15 de outubro de 2008, a Microsoft liberou um patch de emergência para corrigir a vulnerabilidade MS08-067, através da qual o vírus prevalece-se para poder se espalhar. As aplicações da atualização automática se aplicam somente para o Windows XP SP2, SP3, Windows 2000 SP4 e Windows Vista; o Windows XP SP1 e versões mais antigas não são mais suportados. Os softwares antivírus não-ligados a Microsoft, tais como a BitDefender, Enigma Software, Eset,F-Secure, Symantec, Sophos, e o Kaspersky Lab liberaram atualizações com programas de detecção em seus produtos e são capazes de remover o vírus.

Através desses dados vemos que os antivírus devem estar cada vez mais atualizados, estão surgindo novos vírus rapidamente, e com a mesma velocidade deve ser lançado atualizações para os bancos de dados dos antivírus para que os mesmos sejam identificados e excluídos.

Com a criação da internet essa propagação de vírus é muito rápida e muito perigosa, pois se não houver a atualização dos antivírus o computador e usuário estão vulneráveis, pois com a criação da internet várias empresas começarão a utilizar internet como exemplo empresas mais precisamente bancos, mas como é muito vulnerável esse sistema, pois existem vírus que tem a capacidade de ler o teclado (in/out), instruções privilegiadas como os keyloggers. Com esses vírus é possível ler a senha do usuário que acessa sua conta no banco, com isso é mais indicado utilizar um teclado virtual para digitar as senhas ou ir diretamente ao banco.

Nível de Segurança

Depois de identificado o potencial de ataque, as organizações têm que decidir o nível de segurança a estabelecer para uma rede ou sistema os recursos físicos e lógicos a necessitar de proteção. No nível de segurança devem ser quantificados os custos associados aos ataques e os associados à implementação de mecanismos de proteção para minimizar a probabilidade de ocorrência de um ataque.

Segurança Física

Considera as ameaças físicas como incêndios, desabamentos, relâmpagos, alagamento, algo que possa danificar a parte física da segurança, acesso indevido de estranhos, forma inadequada de tratamento e manuseio do veículo.

Segurança Lógica

Atenta contra ameaças ocasionadas por vírus, acessos remotos à rede, backup desatualizados, violação de senhas, furtos de identidades, etc.

Segurança lógica é a forma como um sistema é protegido no nível de sistema operacional e de aplicação. Normalmente é considerada como proteção contra ataques, mas também significa proteção de sistemas contra erros não intencionais, como remoção acidental de importantes arquivos de sistema ou aplicação.

Políticas de Segurança

De acordo com o RFC 2196 (The Site Security Handbook), uma política de segurança consiste num conjunto formal de regras que devem ser seguidas pelos utilizadores dos recursos de uma organização.

As políticas de segurança devem ter implementação realista, e definir claramente as áreas de responsabilidade dos utilizadores, do pessoal de gestão de sistemas e redes e da direção. Deve também adaptar-se a alterações na organização. As políticas de segurança fornecem um enquadramento para a implementação de mecanismos de segurança, definem procedimentos de segurança adequados, processos de auditoria à segurança e estabelecem uma base para procedimentos legais na sequência de ataques.

O documento que define a política de segurança deve deixar de fora todos os aspectos técnicos de implementação dos mecanismos de segurança, pois essa implementação pode variar ao longo do tempo. Deve ser também um documento de fácil leitura e compreensão, além de resumido.

Algumas normas definem aspectos que devem ser levados em consideração ao elaborar políticas de segurança. Entre essas normas estão a BS 7799 (elaborada pela British Standards Institution) e a **NBR ISO/IEC 17799** (a versão brasileira desta primeira).

A ISO começou a publicar a série de normas 27000, em substituição à ISO 17799 (e por conseguinte à BS 7799), das quais a primeira, ISO 27001, foi publicada em 2005.

Existem duas filosofias por trás de qualquer política de segurança: a proibitiva (tudo que não é expressamente permitido é proibido) e a permissiva (tudo que não é proibido é permitido).

Os elementos da política de segurança devem ser considerados:

A Disponibilidade: o sistema deve estar disponível de forma que quando o usuário necessitar, possa usar. Dados críticos devem estar disponíveis ininterruptamente.
A Legalidade.
A Integridade: o sistema deve estar sempre íntegro e em condições de ser usado.
A Autenticidade: o sistema deve ter condições de verificar a identidade dos usuários, e este ter condições de analisar a identidade do sistema.
A Confidencialidade: dados privados devem ser apresentados somente aos donos dos dados ou ao grupo por ele liberado.

Políticas de Senhas

Dentre as políticas utilizadas pelas grandes corporações a composição da senha ou password é a mais controversa. Por um lado profissionais com dificuldade de memorizar varias senhas de acesso, por outro funcionários displicentes que anotam a senha sob o teclado no fundo das gavetas, em casos mais graves o colaborador anota a senha no monitor.

Recomenda-se a adoção das seguintes regras para minimizar o problema, mas a regra fundamental é a conscientização dos colaboradores quanto ao uso e manutenção das senhas.

Senha com data para expiração

Adota-se um padrão definido onde a senha possui prazo de validade com 30 ou 45 dias, obrigando o colaborador ou usuário a renovar sua senha.

Inibir a Repetição

Adota-se através de regras predefinidas que uma senha uma vez utilizada não poderá ter mais que 60% dos caracteres repetidos, p. ex: senha anterior “123senha” nova senha deve ter 60% dos caracteres diferentes como “456seuse”, neste caso foram repetidos somente os caracteres “s” “e” os demais diferentes.

Obrigar a composição com número mínimo de caracteres numéricos e alfabéticos

Define-se obrigatoriedade de 4 caracteres alfabéticos e 4 caracteres numéricos, por exemplo:

1s4e3u2s posicional os 4 primeiros caracteres devem ser numéricos e os 4 subsequentes alfabéticos por exemplo: 1432 seus.

Criar um conjunto com possíveis senhas que não podem ser utilizadas

Monta-se uma base de dados com formatos conhecidos de senhas e proibir o seu uso, como por exemplo o usuário chama-se Jose da Silva, logo sua senha não deve conter partes do nome como 1221jose ou 1212silv etc, os formatos DDMMAAAA ou 19XX, 1883emc ou I2B3M4

Recomenda-se ainda utilizar senhas com Case Sensitive e utilização de caracteres especiais como: @ # $ % & *
Proibição de senhas que combinam com o formato de datas do calendário, placas , números de telefone, ou outros números comuns
Proibição do uso do nome da empresa ou uma abreviatura
Uma senha de Meio Ambiente, da seguinte forma: consoante, vogal, consoante, consoante, vogal, consoante, número, número (por exemplo pinray45). A desvantagem desta senha de 8 caracteres é conhecida a potenciais atacantes, o número de possibilidades que precisam ser testados é menos do que uma senha de seis caracteres de nenhuma forma.

Outros sistemas de criar a senha para os usuários ou deixar que o usuário escolha um de um número limitado de opções exibidas.

A Gestão de Riscos unida à Segurança da Informação

A Gestão de Riscos, por sua vez, fundamental para garantir o perfeito funcionamento de toda a estrutura tecnológica da empresa, engloba a Segurança da Informação, já que hoje a quantidade de vulnerabilidades e riscos que podem comprometer as informações da empresa é cada vez maior.

Ao englobar a Gestão da Segurança da Informação, a Gestão de Riscos tem como principais desafios proteger um dos principais ativos da organização – a informação – assim como a reputação e a marca da empresa, implementar e gerir controles que tenham como foco principal os objetivos do negócio, promover ações corretivas e preventivas de forma eficiente, garantir o cumprimento de regulamentações e definir os processos de gestão da Segurança da Informação. Entre as vantagens de investir na Gestão de Riscos voltada para a Segurança da Informação estão a priorização das ações de acordo com a necessidade e os objetivos da empresa e a utilização de métricas e indicadores de resultados.

A ISO/IEC 17799 1 foi atualizada para numeração ISO/IEC 27002 em julho de 2007. É uma norma de Segurança da Informação revisada em 2005 pela ISO e pela IEC. A versão original foi publicada em 2000, que por sua vez era uma cópia fiel do padrão britânico BS 7799-1:1999.

No mundo atual, globalizado e interativo, temos a capacidade de disponibilizar e absorver uma quantidade considerável de informação, principalmente através dos meios de comunicação e da internet. Informação significa, de acordo com os dicionários vigentes, o ‘ato ou o efeito de informar, a transmissão de notícia e/ou conhecimentos, uma instrução’ (Dicionário WEB). Quando levamos em consideração as organizações, a informação toma uma dimensão extremamente importante, pois decisões importantes são tomadas com base na mesma.

Assim, neste ambiente de empresas interligadas e extremamente competitivas, a informação se torna um fator essencial para a abertura e manutenção de negócios e como tal, precisa ser protegida. A segurança da informação é a forma encontrada pelas organizações para proteger os seus dados, através de regras e controles rígidos, estabelecidos, implementados e monitorados constantemente. É sabido que muitos sistemas de informação não foram projetados para protegerem as informações que geram ou recebem, e essa é uma realidade tanto do setor Público como Privado.

A interligação de redes públicas e privadas e o compartilhamento de recursos de informação dificultam o controle e a segurança do acesso, isso porque a computação distribuída acaba se tornando um empecilho à implementação eficaz de um controle de acesso centralizado. O sucesso da implementação de regras e controles rígidos de segurança da informação dependem de diversos fatores tais como: comprometimento de todos os níveis gerenciais; requisitos de segurança claros e objetivos; política de segurança que reflita o negócio da organização; processo eficaz de gestão dos incidentes da segurança da informação que possam acontecer, dentre outros.

De acordo com a norma ABNT NBR ISO/IEC 17799:2005, o objetivo da política de segurança da informação é "Prover uma orientação e apoio da direção para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações relevantes. Convém que a direção estabeleça uma política clara, alinhada com os objetivos do negócio e demonstre apoio e comprometimento com a segurança da informação por meio da publicação e manutenção de uma política de segurança da informação para toda a organização".

Se a orientação e o apoio aos objetivos da segurança da informação devem partir da direção da organização, fica claro que o profissional de TI é peça chave nesse contexto, já que uma das principais responsabilidades do mesmo é a gerência, manutenção e segurança das informações, dos servidores e dos equipamentos da rede. Este profissional deverá estar comprometido, apoiando ativamente todos os processos e diretrizes implementadas. Caso seja necessário, a direção da organização poderá direcionar e identificar as necessidades para a consultoria de um especialista interno ou externo em segurança da informação, analisando e coordenando os resultados desta consultoria por toda a organização.

O padrão é um conjunto de recomendações para práticas na gestão de Segurança da Informação. Ideal para aqueles que querem criar, implementar e manter um sistema.

A Norma ABNT NBR ISO/IEC-17799 foi elaborada no Comitê Brasileiro de Computadores e Processamento de Dados (ABNT/CB-21) pela Comissão de Estudo de Segurança Física em Instalações de Informática (CE-21:2-4.01) integra uma família de normas de sistema de gestão de segurança da informação SGSI que inclui normas sobre requisitos de sistema de gestão da segurança da informação, gestão de riscos, métricas e medidas, e diretrizes para implementação. Esta família de normas adota um esquema de numeração usando a série de números 27000 em sequência.

A Norma ABNT NBR ISO/IEC-17799 estabelece as diretrizes e princípios gerais para iniciar, implementar, manter e melhorar a gestão de segurança da informação em uma organização. Também pode ser utilizada como um guia prático para desenvolver os procedimentos de segurança da informação da organização.

Seções

A Norma ABNT NBR ISO/IEC-17799 foi elaborada em 11 seções, sendo elas apresentadas a seguir:

Política de Segurança da Informação;
Organizando a Segurança da Informação;
Gestão de Ativos;
Segurança em Recursos Humanos;
Segurança Física e do Ambiente;
Gestão das Operações e Comunicações;
Controle de Acesso;
Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação;
Gestão de Incidentes de Segurança da Informação;
Gestão da Continuidade do Negócio;
Conformidade.
Cada seção apresenta o seu objetivo. A seção se subdivide em categorias, e estas apresentam Controle, Diretrizes para implementação e Informações adicionais

Seção 0:

A introdução visa esclarecer os conceitos básicos sobre o que é segurança da informação, porque a segurança da informação é necessária, como estabelecer os requisitos de segurança da informação, como analisar e avaliar os riscos, as seleções de controle, o ponto de partida para segurança da informação, os fatores críticos de sucesso e desenvolvendo suas próprias diretrizes.

Seção 6: Organizando a Segurança da Informação

6.1 Infra estrutura da segurança da informação. É necessário uma estrutura de gerenciamento para controlar a segurança dentro da organização. E que a direção coordene e analise criticamente toda implementação da segurança da informação.

6.1.1 Comprometimento da direção com a segurança da informação. A direção precisa demonstrar total apoio a segurança da informação dentro da organização, definindo atribuições de forma clara e reconhecendo as responsabilidades da segurança da informação.

6.1.2 Coordenação da segurança da informação. As atividades de segurança da informação devem ser coordenadas por representantes de diferentes partes da organização. A participação e cooperação de gerentes, usuários, administradores, desenvolvedores, auditores, pessoal de segurança é essencial.

6.1.3 Atribuição de responsabilidades para a segurança da informação. Todas as

responsabilidades envolvendo esse papel devem ser explícitas. A atribuição da segurança da informação deve está em conformidade com a política de segurança da informação (Ver seção 5).

Convém que estas responsabilidades sejam mais detalhadas para diferentes locais e recursos de processamentos. Pessoas com responsabilidades definidas podem delegar as tarefas de segurança da informação para outros usuários assim como verificar se as tarefas delegadas estão sendo executadas corretamente.

6.1.4 Processo de autorização para os recursos de processamento da informação. A gestão de autorização para novos recursos de processamento da informação deve ser implementada. Diretrizes consideradas no processo de autorização: a) Os novos recursos devem ter a autorização pela parte administrativa e que essa autorização seja feita juntamente ao gestor responsável pela segurança da informação. b) Hardware e software sejam verificados afim de garantir compatibilidade com o sistema. c) O uso de novos recursos de informação, pessoais ou privados, exemplos: notebooks, palmtop e etc. podem inserir vulnerabilidades, sendo necessário a identificação e controle dos mesmos.

6.1.5 Acordos de confidencialidade. Convém que acordos de não divulgação que assegurem a proteção da organização sejam identificados e analisados criticamente. Tais acordos de confidencialidade e de não divulgação devem está em conformidade com as leis e regulamentações para a qual se aplicam (Ver 15.1.1) Requisitos para esses acordos de confidencialidade e de não divulgação devem ser analisados criticamente e periodicamente. Existem possibilidades de uma organização usar diferentes formas de acordos de confidencialidade irá depender das circunstâncias.

6.1.6 Contato com autoridades. Controle – Contactar com as autoridades Diretrizes para implementação – Saber quando e quais autoridades devem sercontatadas e se a lei foi violada, devem ser violada em tempo hábil. Avisar as organizações que estão sofrendo ataque (provedor de internet, operador de telecomunicações). Informações adicionais - Objetivo: Assegurar que um enfoque consistente e efetivo seja aplicado à gestão de incidentes de segurança da informação. Convém que responsabilidades e procedimentos estejam definidos para o manuseio efetivo de eventos de segurança da informação e fragilidades, uma vez que estes tenham sido notificados. Convém que um processo de melhoria contínua seja aplicado às respostas,monitoramento, avaliação e gestão total deincidentes de segurança da informação. Convém que onde evidências sejam exigidas, estas sejam coletadas para assegurar a conformidade com as exigências legais.

6.1.7 Contato com grupos especiais. Controle - Convém que sejam mantidos contatos apropriados com grupos de interesses especiais ou outros fórunsespecializados de segurança da informação e associações profissionais. Informações adicionais - Acordos de compartilhamento de informações podem ser estabelecidos para melhorar a cooperação e coordenação de assuntos de segurança da informação. Convém que tais acordos identifiquem requisitos para a proteção de informações sensíveis.

6.1.8 Análise crítica independente de segurança da informação. Controle - Convém que o enfoque da organização para gerenciar a segurança da informação e a sua implementaçãoseja analisado criticamente, de forma independente, a intervalos planejados,ou quando ocorreremmudanças significativas relativas à implementação da segurança da informação. Diretrizes para implementação - Convém que a análise crítica independente seja iniciada pela direção. E que a análise crítica seja executada por pessoas independentes da área avaliada. Os resultados tem que ser registrados e relatados para a direção que iniciou a análise e que esses registros fiquem mantidos. Tomar ações corretivas, se a análise crítica entender que sim. Informações adicionais - Convém que as áreas onde os gerentes regularmente fazem a análise críticapossam também ser analisadas criticamente de forma independente.

6.2 Partes externas. Objetivos: Manter a segurança dos recursos de processamento da informação e da informação da organização, que são acessados,processados, comunicados ou gerenciados por partes externa.

6.2.1 Identificação dos riscos relacionados com partes externas. Controle - Convém que os riscos para os recursos de processamento da informação e da informação da organização oriundos de processos do negócio que envolva as partes externas sejam identificados e controles apropriadosimplementados antes de se conceder o acesso. Diretrizes para implementação -Análise e avaliação de riscos sejam feitas para identificar quaisquer requisitos de controles específicos.

6.2.2 Identificando a segurança da informação, quando tratando com os clientes. Controle - Convém que todos os requisitos de segurança da informação identificados sejam considerados antes de conceder aos clientes o acesso aos ativos ou às informações da organização.

6.2.3 Identificando segurança da informação nos acordos com terceiros. Controle - Cobertura de todos os requisitos de segurança da informação relevantes. Diretrizes para implementação - Convém que o acordo assegure que não existe mal-entendido entre a organização e o terceiro.

Convém que as organizações considerem a possibilidade de indenização de terceiros. Entretanto, é importante que a organização planeje e gerencie a transição para um terceirizado e tenha processos adequados implantados para gerenciar as mudanças e renegociar ou encerrar os acordos. Acordos com terceiros podem também envolver outras partes

De um modo geral os acordos são geralmente elaborados pela organização. A organização precisa assegurar que a sua própria segurança da informação não é afetada desnecessariamente pelos requisitos do terceiro, estipulados no acordo imposto.

Seção 7: Gestão de Ativos

Responsabilidade pelos ativos. O objetivo e alcançar e manter a proteção adequada dos ativos da organização. Convém que todos os ativos sejam inventariados e tenham um proprietário responsável. Convém que os proprietários dos ativos sejam identificados e a eles seja atribuída a responsabilidade pela manutenção apropriada dos controles.

Proprietário dos ativos. Convém que todas as informações e ativos associados com os recursos de processamento da informação tenham um proprietário designado por uma parte definida da organização. As tarefas de rotina podem ser delegadas, por exemplo, para um custo diante que cuida do ativo no dia-a-dia, porém a responsabilidade permanece com o proprietário.

Em sistemas de informação complexos pode ser útil definir grupos de ativos que atuem juntos para fornecer uma função particular, como serviços. Neste caso, o proprietário do serviço é o responsável pela entrega do serviço, incluindo o funcionamento dos ativos, que provê os serviços.

Classificação da informação. Objetivo: Assegurar que a informação receba um nível adequado de proteção. Convém que a informação seja classificada para indicar a necessidade, prioridades e o nível esperado de proteção quando do tratamento da informação. A informação possui vários níveis de sensibilidade e criticidade. Alguns itens podem necessitar um nível adicional de proteção ou tratamento especial. Convém que um sistema de classificação da informação seja usado para definir um conjunto apropriado de níveis de proteção e determinar a necessidade de medidas especiais de tratamento.

Recomendações para classificação. Que a informação seja classificada em termos do seu valor, requisitos legais, sensibilidade e criticidade para a organização.

E seus respectivos controles de proteção levem em consideração as necessidades de compartilhamento ou restrição de informações e os respectivos impactos nos negócios, associados com tais necessidades. Cuidados sejam tomados com a quantidade de categorias de classificação e com os benefícios obtidos pelo seu uso. Esquemas excessivamente complexos podem tornar o uso incômodo e ser inviáveis economicamente ou impraticáveis.

O nível de proteção pode ser avaliado analisando a confidencialidade, a integridade e a disponibilidade da informação, Em geral, a classificação dada à informação é uma maneira de determinar como esta informação vai ser tratada e protegida.

Seção 10: Gerenciamento das operações e comunicações Documentação dos procedimentos de operação

Convém que os procedimentos de operação sejam documentados, mantidos atualizados e disponíveis a todos os usuários que deles necessitem.

Gestão de Mudanças

Convém que modificações nos recursos de processamento da informação e sistemas sejam controladas. como:

a) identificação e registro de mudanças significativas; b) planejamento e testes das mudanças; c) avaliação de impactos potenciais, incluindo impactos de segurança, de tais mudanças; d) procedimento formal de aprovação das mudanças propostas; e) comunicação dos detalhes das mudanças para todas as pessoas envolvidas; f) procedimentos de recuperação, incluindo procedimentos e responsabilidades pela interrupção e recuperação de mudanças em caso de insucesso ou na ocorrência de eventos inesperados.

Entrega de Serviços

Convém que seja garantido que os controles de segurança, as definições de serviços e os níveis de entrega incluídos no acordo de entrega de serviços terceirizados sejam implementados, executados e mantidos pelo terceiro.

Mídias em Trânsito

Temos que proteger melhor as Mídias contra acesso de pessoas não autorizadas , para que não façam uso impróprio ou que não mudem ou façam alterações durante o transporte de alguma informação.

• Métodos de proteção:

• Meio de transporte que sejam confiáveis;

• Definir seus gestores;

• Estabelecer procedimentos para verificação;

• Adotar controles para proteger o conteúdo entre outros.

Mensagens Eletrônicas

Colocar uma segurança boa no seu computador ou dispositivo móvel para que não acha problemas com hackers .

São consideradas de segurança da informação as seguintes:

• Proteção contra acesso não permitido; • Verificar endereço da mensagem; • Confiar no serviço geral; • Aprovação para o uso de serviços públicos e etc.

Mensagens eletrônicas como correio eletrônico cumpre um papel cada vez mais importante nas comunicações do negócio. Tem seus riscos, mas não se compara com a comunicação de documentos.

Sistemas de informações do negócio

Temos que desenvolver e implantar para proteger as informações associadas com a conexão de dados sobre os negócios sócios ou organizacionais.

A segurança e implementação das conexões de sistemas tem os seguintes:

• Facilidades de acesso das informações de sistemas administrativos, pois são compartilhados em diferentes setores; • Política e controles apropriados para gerenciar o compartilhamento de informações; • Restrição de categorias e documentos secretos; • Restrição ao relacionamento com indivíduos específicos; • Restrição aos recursos selecionados para cada categoria ou usuário; • Identificação das permissões dos usuários; • Proibição de copias de qualquer arquivo de segurança entre outros.

Esse sistema de escritório trás uma oportunidade de rápida disseminação para compartilha informações, documentos, computadores, celulares, redes sem fio, entre outros.

Serviços de Comércio Eletrônico

Papel: Garantir a segurança de serviços de comércio eletrônico e sua utilização segura.

As implicações de segurança associadas ao uso do comercio eletrônico, tem transições.

On-line, ela tem que ter controles e que sejam bem controladas.

Comércio Eletrônico

As informações envolvidas no comercio eletrônico , sendo usadas em conexões publicas , disputam problemas e modificações não autorizadas.

• Comércio eletrônico é vulnerável a inúmeras ameaças de rede que podem resultar em atividades fraudulentas, disputas contratuais, e divulgação ou modificação de informação. • Comércio eletrônico pode utilizar métodos seguros de autenticação, como, por exemplo, criptografia de chave pública e assinaturas digitais para reduzir os riscos. Ainda, terceiros confiáveis podem ser utilizados onde tais serviços forem necessários.

Transações On-Line

Elas tem que ser protegidas para prevenir roubo de dados ou perda, que por algum motivo venha a ser alterada prejudicado seus usuários.

Considerações Seguintes são:

• Uso de assinaturas eletrônicas; • Credenciais dos usuários; • Transação confidencial; • Privacidade dos envolvidos sobre os dados; • Protocolos para comunicação entre usuários entre outros.

A extensão dos controles adotados precisará ser proporcional ao nível de risco associado a cada forma de Transação on-line pode ser: Transações podem precisar estar de acordo com leis, regras e regulamentações na jurisdição em que a Transação é gerada, processada, completa ou armazenada.

Monitoramento

• Detectar atividades não autorizadas.

• Os sistemas devem ser monitorados e que sejam registrados se houver alguma mudança.

• As organizações estejam de acordo com todos os requisitos legais relevantes aplicáveis para suas atividades de registro e monitoramento.

O monitoramento do sistema seja utilizado para checar a eficácia dos controles adotados e para verificar a conformidade com o modelo de política de acesso.

Proteção das informações dos registros

Os recursos e informações de registros sejam protegidos contra falsificação e acesso não autorizado.

Os controles implementados objetivem a proteção contra modificações não autorizadas e problemas operacionais com os recursos dos registros, tais como:

• Alterações dos tipos de mensagens que são gravadas;

• Arquivos de registros sendo editados ou excluídos;

• Capacidade de armazenamento da mídia magnética do arquivo de registros excedida, resultando em falhas no registro de eventos ou sobreposição do registro de evento anterior.

• De sistema normalmente contêm um grande volume de informações e muitos dos quais não dizem respeito ao monitoramento da segurança

• Ajudar a identificar eventos significativos para propósito de monitoramento de segurança convém que a cópia automática dos tipos de mensagens para a execução de consulta seja considerada e/ou o uso de sistemas utilitários adequados ou ferramentas de auditoria para realizar a racionalização e investigação do arquivo seja considerado.

Controles Contra Códigos Móveis

Controla a autorização de códigos móveis para que os não autorizados sejam impedidos. Adicional: Código móvel é um código transferido de um computador a outro executando automaticamente e realizando funções específicas com pequena ou nenhuma interação por parte do usuário.

Para proteger contra ação não autorizada são adotadas algumas ações como, a execução de códigos móveis em locais isolados logicamente, e bloqueios de recebimento de códigos móveis;
É importante notar que é sempre recomendável ter cópias de segurança de todo conteúdo;

E que a gerencia tenha total controle sob mídias removíveis e rede, para protege-la de ameaças, e impedir a divulgação não autorizada, ou para usos indevidos;
Também convém que as mídias ao serem descartadas, estejam devidamente protegidas;
Mantendo também total controle nas trocas de informações;
Sincronização dos relógios

Os relógios de todos os sistemas de processamento da informação relevantes, dentro da organização ou do domínio de segurança.

Um computador ou dispositivo de comunicação tiver a capacidade para operar um relógio de tempo real, convém que o relógio seja ajustado conforme o padrão acordado. A interpretação correta do formato data/hora é importante para assegurar que o timestamp reflete a data/hora real.

O estabelecimento correto dos relógios dos computadores é importante para assegurar a exatidão dos Registros de auditoria, que podem ser requeridos por investigações ou como evidências em casos legais ou disciplinares. Registros de auditoria incorretos podem impedir tais investigações e causar danos à credibilidade das evidências. Um relógio interno ligado ao relógio atômico nacional via transmissão de rádio pode ser utilizado como relógio principal para os sistemas de registros.

Seção 12: Aquisição, Desenvolvimento e Manutenção de Sistema de Informação

Análise e especificação dos requisitos de segurança. Convém que sejam especificados os requisitos para controles de segurança nas especificações de requisitos de negócios, para novos sistemas de informação ou melhorias em sistemas existentes.

Processamento Correto nas Aplicações.

Objetivo: Prevenir a ocorrência de erros, perdas, modificação não autorizada ou mau uso de informações em aplicações.

Convém que requisitos para garantir a autenticidade e proteger a integridade das mensagens em aplicações sejam identificados e os controles apropriados sejam identificados e implementados.

Diretrizes para implementação. Convém que seja efetuada uma análise/avaliação dos riscos de segurança para determinar se a integridade das mensagens é requerida e para identificar o método mais apropriado de implementação.

Controles Criptográficos.

Objetivo: Proteger a confidencialidade, a autenticidade ou a integridade das informações por meios criptográficos. Convém que uma política seja desenvolvida para o uso de controles criptográficos. Convém que o

Controle de software operacional. Convém que procedimentos para controlar a instalação de software em sistemas operacionais sejam implementados. Convém que acessos físicos e lógicos sejam concedidos a fornecedores, quando necessário, para a finalidade de suporte e com aprovação gerencial. Convém que as atividades do fornecedor sejam monitoradas. Os softwares para computadores podem depender de outros softwares e módulos fornecidos externamente, os quais convém ser monitorados e controlados para evitar mudanças não autorizadas, que podem introduzir fragilidades na segurança.

Informações adicionais. Convém que sistemas operacionais sejam atualizados quando existir um requisito para tal, por exemplo, se a versão atual do sistema operacional não suportar mais os requisitos do negócio. Convém que as atualizações não sejam efetivadas pela mera disponibilidade de uma versão nova do sistema operacional. Novas versões de sistemas operacionais podem ser menos seguras, com menor estabilidade, e ser menos entendidas do que os sistemas atuais.

Seção 13: Gestão de Incidentes de Segurança da Informação

Notificação de eventos de segurança da informação. Trabalha com ações preventivas.

Controle - Qualquer incidente deve ser relatado imediatamente aos responsáveis capacitados por interceptá-los através de canais confiáveis e de integridade inquestionável.

Diretrizes para implementação - Consiste na elaboração de ferramentas para tornar qualquer incidente visível às pessoas responsáveis por resolvê-los; - É criado um padrão de notificações de modo que nenhuma pessoa tome uma decisão precipitada ou por si só, mas que todos estejam cientes e preparados para resolver o problema de acordo com duas funcionalidades.

Gestão de incidentes de sistema de informação e melhorias.

Foco numa precisa e consistente gestão de incidentes. Gerir com base em melhorias requer atenção total.

Controle - Com precisão detalhada e ordenada devem ser estabelecidas responsabilidades e procedimentos.

Diretrizes para implementação - Se faz necessária aplicação de ferramentas de verificação de vulnerabilidade tanto dos dados quando da parte física (hardware e meios de transmissão).

Seção 14: Gestão da Continuidade do Negócio

14.1 Aspectos da Gestão da continuidade do negócio, relativos a segurança da informação.

Objetivo: Não permitir a interrupção das atividades do negócio e proteger os processos críticos contra efeitos de falhas ou desastres significativos , e assegurar a sua retomada em tempo hábil , se for o caso . Este processo deve identificar os processos críticos e que integre a gestão da segurança da informação com as exigências da gestão da continuidade do negócio com outros requisitos de continuidade relativo e tais aspectos como operações , funcionários , materiais , transporte e instalações , todas as partes de uma empresa .

14.1.1 Incluindo Segurança da Informação no Processo de gestão da continuidade de negócio.

Desenvolver e manter um processo de gestão para assegurar a continuidade do negócio por toda a organização e que contemple os requisitos de segurança da informação necessários para a continuidade do negócio da organização .

14.1.2 Continuidade de negócios e análise/avaliação de riscos.

Identificar os eventos que podem causar interrupções aos processos de negócio, junto a probabilidade e impacto de tais interrupções e as consequências para a segurança de informação.

14.1.3 Desenvolvimento e implementação de planos de continuidade relativos à segurança da informação .

Os planos devem ser desenvolvidos e implementados para a manutenção ou recuperação das operações e para assegurar a disponibilidade da informação no nível requerido e na escala de tempo requerida, após a ocorrência de interrupções ou falhas dos processos críticos do negócio.

14.1.4 Estrutura do plano de continuidade do negócio.

Manter uma estrutura básica dos planos de continuidade do negócio para assegurar que todos os planos são consistentes, para alcançar os requisitos de segurança da informação e para identificar as prioridades para testes e manutenção.

14.1.5 Testes , manutenção e reavaliação dos planos de continuidade do negócio.

Os Planos de continuidade do negócio devem ser testados e atualizados regulamente , de forma a assegurar sua permanente atualização e efetividade .

Seção 15: Conformidade

15.1 Conformidade e seus requisitos legais. Tem como objetivo principal: evitar a violação de qualquer lei criminal ou civil, estatutos, regulamentações ou obrigações contratuais e de quaisquer requisitos de segurança da informação.

15.1.1 Identificação da legislação vigente. Convém que todos os requisitos estatuários, regulamentares e contratuais relevantes, e o enfoque da organização para atender a esses requisitos, sejam explicitamente definidos, documentados e mantidos atualizados para cada sistema de informação da organização.

15.1.2 Direitos de propriedade intelectual. Convém que as seguintes diretrizes sejam consideradas para proteger qualquer material que possa ser considerado como propriedade intelectual:

divulgar uma política de conformidade como os direitos de propriedade intelectual que defina o uso legal de produtos de software e de informação;

Adquirir software somente por meio de fonte conhecidas e de reputação, para assegurar que o direito autoral não está sendo violado;

Manter conscientização das políticas para proteger os direitos de propriedades intelectual e notificar a intenção de tomar ações disciplinares contra pessoas que violarem essas políticas;

Manter de forma adequada os registros ativos e identificar todos os ativos com requisitos para proteger os direitos de propriedade intelectual;

Manter provas e evidencias da propriedade de licenças, discos-mestre, manuais etc.;
Implementar controles para assegurar que o número máximo de usuários permitidos não excede o número de licenças adquiridas;

Não duplicar, converter para outro formato ou extrair de registros comercias (filmes, áudios) outros que não os permitidos pela lei de direito autoral;

Não copiar, no tolo ou em partes, livros, artigos, relatórios ou outros documentos, além daqueles permitidos pela lei de direito autoral.

Direitos de propriedade intelectual incluem direito de software ou documento, direito de projeto, marcas, patentes e licenças de código-fonte.

15.1.3 Proteção de registros organizacionais. Para atender aos objetivos de proteção de registros, convém que os seguintes passos sejam tomados dentro da organização:

Emitir diretrizes gerais para retenção, armazenamento, tratamento e disposição de registros e informações;

Elaborar uma programação para retenção, identificando os registros essenciais e o período que cada um deve ser mantido;

Manter um inventario das fontes de informação-chave;

Implementar controles apropriados para proteger registros e informações contra perda, destruição e falsificação.

15.1.4 Proteção de dados e privacidade de informações pessoais. A conformidade com esta política e todas as legislação e regulamentações relevantes de produtos de dados necessita de uma estrutura de gestão e de controles apropriados. Geralmente isto é melhor alcançado através de uma pessoa responsável, como por exemplo, um gestor de proteção de dados, que deve fornecer orientações gerais para gerentes, usuários e provedores de serviço sobre as responsabilidades de cada um e sobre quais procedimentos específicos recomenda-se seguir. Convém que a responsabilidade pelo tratamento das informações pessoais e a garantia da conscientização dos princípios de proteção dos dados sejam tratados de acordo com as legislações e regulamentações relevantes. Convém que medidas organizacionais e técnicas apropriadas para proteger as informações pessoais sejam implementadas.

15.1.5 Prevenção de mau uso de recursos de procedimentos da informação. Convém que todos os usuários estejam conscientes de escopo preciso de suas permissões de acesso e da monitoração realizada para detectar o uso não autorizado.

Isto pode ser alcançado pelo registro das autorizações dos usuários por escrito, convém que a cópia seja assinada pelo usuário e armazenada de forma segura pela organização. Convém que os funcionários de uma organização, fornecedores e terceiros sejam informados de que nenhum acesso é permitido com exceção daqueles que foram autorizados.

15.1.6 Regulamentação de controles de criptografia. Convém que os seguintes itens sejam considerados para conformidade com leis, acordos e regulamentações relevantes:

Restrições à importação e/ou exportação de hardware e software de computador para execução de funções criptográficas;

Restrições à importação e/ou exportação de hardware ou software de computador que foi projetado para ter funções criptográficas embutidas;

Restrições no uso de criptografia;

Métodos mandatários ou discricionários de acesso pela autoridades dos países à informação cifrada por hardware ou software para fornecer confidencialidade ao conteúdo.

15.2 Conformidade com normas e políticas de segurança da informação e conformidade técnica. Convém que tais analises críticas sejam executadas com base na políticas de segurança da informação apropriadas e que as plataformas técnicas e sistemas de informação sejam auditados em conformidade com as normas de segurança da informação implementadas pertinentes e com os controles de segurança documentados.

15.2.1 Conformidade com as políticas e normas de segurança da informação. Controla que os gestores garantam que todos os procedimentos de segurança da informação dentro da sua área de responsabilidade estão senso executados corretamente para atender à conformidade com as normas e políticas de segurança da informação.

15.2.2 Verificação da conformidade técnica. Se o teste de invasão ou avaliações de vulnerabilidades forem usados, convém que sejam tomadas precauções, um vez que tais atividade podem conduzir a um comprometimento da segurança do sistema. Convém que tais testes sejam planejados, documentados e repetidos, convém que qualquer verificação de conformidade técnica somente seja executada por pessoas autorizadas e competentes, ou sob a supervisão de tais pessoas.

15.3 Considerações quanto à auditoria de sistemas de informação. Tem como objetivo maximizar a eficácia e minimizar a interferência no processo de auditoria dos sistemas de informação, convém que existam controles para a proteção dos sistemas operacionais e ferramentas de auditoria durante as auditorias de sistemas de informação.

15.3.1 Controle de auditoria de sistema de informação. Convém que requisitos e atividade de auditoria envolvendo verificação nos sistemas operacionais sejam cuidadosamente planejados e acordados para minimizar os riscos de interrupção dos processos de negócio. Convém que as seguintes diretrizes sejam verificadas:

Requisitos de auditoria sejam acordados com o nível apropriado da administração;
A verificação esteja limitada ao acesso somente para leitura de software e dados;
Outros acesso diferentes de apenas leitura sejam permitidos somente através de copias isoladas dos arquivos do sistema, e sejam apagados ao final da auditoria, ou dada proteção apropriada quando existir uma obrigação para guarda tais arquivos como requisitos da documentação da auditoria;
Todos os procedimentos, requisitos e responsabilidade sejam documentados.

15.3.2 Proteção de ferramentas de auditoria de sistema de informação. Convém que o acesso às ferramentas de auditoria de sistema de informação seja protegido, para prevenir qualquer possibilidade de uso improprio ou comprometimento, as ferramentas de auditoria de sistemas de informação, por exemplo, software ou arquivos de dados, sejam separados de sistemas em desenvolvimento e em operação e não sejam mantidos em fitas de biblioteca ou áreas de usuários, a menos que seja dado um nível apropriado de proteção adicional.