

[ISO 17799] Checklist

Auditores:

Antônio M. D. S. Fortes
Diego Protta Casati
Leandro Spínola Rodrigues

Checklist	Padrão	Seção	Questão de auditoria	S	N
1	3	Política de segurança			
1.1	3.1	Política de segurança da informação			
1.1.1	3.1.1	Documento da política de segurança da informação	Se existe alguma política de segurança da informação, que seja aprovado pela direção, publicado e comunicado, de forma adequada, para todos os funcionários. Se esta expressa as preocupações da direção e estabelece as linhas-mestras para a gestão da segurança da informação.		
1.1.2	3.1.2	Análise crítica e avaliação	Se a política de segurança tem um gestor que seja responsável por sua manutenção e análise crítica, de acordo com um processo de análise crítica definido. Se o processo garante que a análise crítica ocorra como decorrência de qualquer mudança que venha afetar a avaliação de risco original. Exemplo: Incidentes de segurança significativos, novas vulnerabilidades ou mudanças organizacionais ou na infra-estrutura técnica.		
2	4	Segurança organizacional			
2.1	4.1	Infra-estrutura da segurança da informação			
2.1.1	4.1.1	Gestão do fórum de segurança da informação	Se existe um fórum de gestão para garantir um direcionamento claro e um suporte de gestão visível dos envolvidos para as iniciativas de segurança dentro da organização.		
2.1.2	4.1.2	Coordenação de segurança da informação	Se existe um fórum multifuncional com representantes da direção de áreas relevantes da organização para coordenar a implementação de controles de segurança da informação.		
2.1.3	4.1.3	Atribuição das responsabilidades de segurança da informação	Se as responsabilidades pela proteção de cada ativo e pelo cumprimento de processos de segurança específicos sejam claramente definidos.		
2.1.4	4.1.4	Processo de autorização para as instalações de processamento da informação	Se foi implantado um processo de gestão de autorização para novos recursos de processamento da informação. Isto deve incluir todos os novos recursos, como hardware e software.		
2.1.5	4.1.5	Consultoria especializada em segurança da informação	Se uma consultoria especializada em segurança da informação é obtida quando apropriado. Um indivíduo específico deve ser identificado para coordenar conhecimentos e experiências dentro da organização para assegurar consistência, e prover ajuda na decisão de segurança.		
2.1.6	4.1.6	Cooperação entre organizações	Se são mantidos contatos apropriados com autoridades legais, organismos regulamentadores, provedores de serviço de informação e operadores de telecomunicações, para garantir que ações adequadas e apoio especializado possam ser rapidamente acionados na ocorrência de incidentes de segurança.		
2.1.7	4.1.7	Análise crítica independente de segurança da informação	Se a implementação da política de segurança é analisada criticamente, de forma independente. Isto é para fornecer garantia de que as práticas da organização refletem apropriadamente a política, e que esta é adequada e eficiente.		
2.2	4.2	Segurança no acesso de prestadores de serviço			
2.2.1	4.2.1	Identificação no acesso de prestadores de serviço	Se os riscos do acesso de prestadores de serviço são identificados e controles de segurança apropriados foram implementados. Se os tipos de acesso são identificados, classificados e as razões para o acesso são justificadas.		

			Se os riscos de segurança com prestadores de serviço trabalhando no ambiente da empresa foram identificados e controles apropriados são identificados.			
2.2.2	4.2.2	Requisitos de segurança nos contratos com prestadores de serviço	Se existe um contrato formal contendo ou referenciando todos os requisitos de segurança para assegurar a conformidade com as normas e políticas de segurança da informação.			
2.3	4.3	Terceirização				
2.3.1	4.3.1	Requisitos de segurança dos contratos da terceirização	Se os requisitos de segurança são definidos no contrato com prestadores de serviços, quando a organização tiver terceirizado o gerenciamento e controle de todos ou alguns dos sistemas de informação, redes e/ ou estações de trabalho. O contrato deve definir como os requisitos legais são referenciados, como a segurança dos ativos é mantida e testada, e o direito de auditoria, características de segurança física e como a disponibilidade dos serviços é mantida em um evento de desastre.			
3	5	Classificação e controle dos ativos de informação				
3.1	5.1	Contabilização dos ativos				
3.1.1	5.1.1	Inventário dos ativos de informação	Se um inventário ou registro é mantido com os ativos importantes relacionados com cada sistema de informação. Se cada ativo identificado possui um gestor, se foi definido e acordado na classificação de segurança, e se sua localização foi definida.			
3.2	5.2	Classificação da informação				
3.2.1	5.2.1	Recomendações para classificação	Se foi implantado um esquema ou diretriz de classificação da informação, que define como a informação é tratada e protegida.			
3.2.2	5.2.1	Rótulos e tratamento da informação	Se um conjunto apropriado de procedimentos foi definido para rotular e tratar a informação de acordo com o esquema de classificação adotado pela organização.			
4	6	Segurança em pessoas				
4.1	6.1	Segurança na definição e nos recursos de trabalho				
4.1.1	6.1.1	Incluindo segurança nas responsabilidades do trabalho	Se regras e responsabilidades de segurança são documentadas onde for apropriado, de acordo com a política de segurança da informação da organização. Isto deve incluir responsabilidades gerais pela implementação ou manutenção da política de segurança, assim como quaisquer responsabilidades específicas para a proteção de determinados ativos ou pela execução de determinados processos ou atividades de segurança.			
4.1.2	6.1.2	Seleção e política de pessoal	Se verificações sobre a equipe de trabalho permanente são conduzidas no momento da seleção de candidatos. Isto deve incluir referências de caráter, confirmação das qualificações acadêmicas e profissionais, e verificação da identidade.			
4.1.3	6.1.3	Acordos de confidencialidade	Se os funcionários são questionados a assinarem acordos de confidencialidade ou não divulgação como parte dos termos e condições iniciais de contratação. Se estes acordos cobrem a segurança dos recursos de processamento de informação e os ativos da organização.			
4.1.4	6.1.4	Termos e condições de trabalho	Se os termos e condições de trabalho determinam as responsabilidades dos funcionários pela segurança da informação. Quando apropriado, estas responsabilidades devem continuar por um período de tempo definido, após o término do contrato de trabalho.			
4.2	6.2	Treinamento dos usuários				

4.2.1	6.2.1	Educação e treinamento em segurança da informação	Se todos os funcionários da organização e, onde for relevante, prestadores de serviços recebem treinamento apropriado e atualizações regulares sobre as políticas e procedimentos organizacionais.			
4.3	6.3	Respondendo aos incidentes de segurança e ao mau funcionamento				
4.3.1	6.3.1	Notificação dos incidentes de segurança	Se existe um procedimento ou diretriz formal para reportar incidentes de segurança através dos canais apropriados da direção, o mais rapidamente possível.			
4.3.2	6.3.2	Notificando falhas na segurança	Se existe um procedimento ou diretriz formal para que os usuários sejam instruídos a registrar e notificar quaisquer fragilidades ou ameaças, ocorridas ou suspeitas, na segurança de sistemas ou serviços.			
4.3.3	6.3.3	Notificando mau funcionamento de software	Se foram estabelecidos procedimentos para notificar qualquer mau funcionamento de software.			
4.3.4	6.3.4	Aprendendo com os incidentes	Se existem mecanismos para permitir que tipos, quantidades e custos dos incidentes e dos maus funcionamentos sejam quantificados e monitorados.			
4.3.5	6.3.5	Processo disciplinar	Se existe um processo disciplinar formal para os funcionários que tenham violado as políticas e procedimentos de segurança organizacional. Tal processo pode dissuadir funcionários que, de outra forma, seriam inclinados a desrespeitar os procedimentos de segurança.			
5	7	Segurança física e do ambiente				
5.1	7.1	Áreas de segurança				
5.1.1	7.1.1	Perímetro da segurança física	Se barreiras físicas, como recursos de segurança, foram implementadas para proteger o serviço de processamento da informação. Alguns exemplos de tais recursos de segurança são o controle por cartão do portão de entrada, muros, presença de um funcionário na recepção, etc.			
5.1.2	7.1.2	Controles de entrada física	Se existem controles de entrada para permitir somente a entrada do pessoal autorizado dentro de várias áreas da organização.			
5.1.3	7.1.3	Segurança em escritórios, salas e instalações de processamento	Se as salas, que possuem o serviço de processamento de informação ou contêm armários fechados ou cofres, são trancadas.			
			Se o serviço de processamento de informação é protegido contra desastres naturais ou causados pelo homem.			
			Se existe alguma ameaça potencial de propriedades vizinhas.			
5.1.4	7.1.4	Trabalhando em áreas de segurança	Se existe algum controle de segurança para prestadores de serviço ou funcionários trabalhando em área de segurança. A informação só deve ser fornecida quando necessário.			
5.1.5	7.1.5	Isolamento das áreas de expedição e carga	Se as áreas de expedição e carga e de processamento de informação são isoladas uma da outra, para evitar acesso não autorizado.			
			Se uma avaliação de risco foi realizada para determinar a segurança de tais áreas.			
5.2	7.2	Segurança dos equipamentos				

5.2.1	7.2.1	Instalação e proteção de equipamentos	Se o equipamento foi instalado em local apropriado para minimizar acesso não autorizado à área de trabalho.		
			Se os itens que requerem proteção especial foram isolados para reduzir o nível geral de proteção exigida.		
			Se controles foram adotados para minimizar o risco de ameaças potenciais, como roubo, fogo, explosão, fumaça, água, poeira, vibração, efeitos químicos, interferência no fornecimento elétrico, radiação eletromagnética, inundação.		
			Se existe uma política especial para alimentação, bebida e fumo nas proximidades das instalações de processamento da informação.		
			Se os aspectos ambientais são monitorados para evitar condições que possam afetar de maneira adversa a operação das instalações de processamento da informação.		
5.2.2	7.2.2	Fornecimento de energia	Se o equipamento é protegido contra falhas de energia e outras anomalias na alimentação elétrica., utilizando fornecimento de energia permanente como alimentação múltipla, no-break, gerador de reserva, etc.		
5.2.3	7.2.3	Segurança do cabeamento	Se o cabeamento elétrico e de telecomunicações que transmite dados ou suporta os serviços de informação é protegido contra interceptação ou dano.		
			Se existe algum controle de segurança adicional para informações sensíveis ou críticas.		
5.2.4	7.2.4	Manutenção de equipamentos	Se os equipamentos têm manutenção de acordo com intervalos e especificações do fabricante.		
			Se a manutenção é realizada apenas pelo pessoal autorizado.		
			Se são mantidos registros com todas as falhas suspeitas ou ocorridas e de toda a manutenção corretiva e preventiva.		
			Se os controles apropriados são utilizados quando do envio de equipamentos para manutenção fora da instalação física.		
			Se todos os requisitos impostos pelas apólices de seguro são atendidos.		
5.2.5	7.2.5	Segurança de equipamentos fora das instalações	Se um equipamento é autorizado pela direção quando necessitar ser utilizado fora das instalações da organização.		
5.2.6	7.2.6	Reutilização e alienação segura de equipamentos	Se dispositivos de armazenamento contendo informações sensíveis são fisicamente destruídos ou sobrescritos de maneira segura.		
5.3	7.3	Controles gerais			
5.3.1	7.3.1	Política de mesa limpa e tela limpa	Se um serviço de bloqueio automático de tela de computador está ativo. Isso irá travar o computador sempre que for deixado ocioso por um determinado tempo.		
			Se os empregados são avisados para deixar qualquer material confidencial de forma segura e trancada.		
5.3.2	7.3.2	Remoção de propriedade	Se equipamentos, informações ou software podem ser retirados em adequada autorização.		
			Se inspeções regulares são realizadas para detectar remoção de propriedade não autorizada.		
			Se as pessoas estão cientes que estas inspeções regulares estão realizadas.		
6	8	Gerenciamento das operações e comunicações			
6.1	8.1	Procedimentos e responsabilidades operacionais			

6.1.1	8.1.1	Documentação dos procedimentos de operação	Se uma política de segurança identifica qualquer procedimento operacional como backup, manutenção de equipamentos, etc. Se estes procedimentos estão documentados e são utilizados.		
6.1.2	8.1.2	Mudanças operacionais	Se todos os programas executados no sistema de produção são submetidos ao controle estrito de mudanças. Qualquer mudança nesses programas de produção deve ser autorizada pelo controle de mudanças. Se registros são mantidos para qualquer modificação nos programas de produção.		
6.1.3	8.1.3	Procedimentos para o gerenciamento de incidentes	Se existe um procedimento de gerenciamento de incidente definido para uma resposta a incidentes de segurança. Se o procedimento define as responsabilidades de gerenciamento de incidente, de maneira organizada e rápida em resposta a incidentes de segurança. Se o procedimento define diferentes tipos de incidentes, desde Negação de Serviço (DoS) até quebra de confidencialidade, assim como modos de gerencia-los. Se registros e evidências relacionadas aos incidentes são mantidos, e ações pro-ativas são realizadas de maneira que os incidentes não mais ocorram.		
6.1.4	8.1.4	Segregação de funções	Se tarefas e áreas de responsabilidades são separadas para reduzir a possibilidade de modificação não autorizada ou mal uso de informação ou serviços.		
6.1.5	8.1.5	Separação de ambientes de desenvolvimento e de produção	Se os ambientes de desenvolvimento e de teste são isolados do ambiente de produção. Por exemplo, software em desenvolvimento deve ser executado em um computador diferente do computador com software de produção. Quando necessário, as redes de desenvolvimento e produção devem ser separadas uma da outra.		
6.1.6	8.1.6	Gestão de recursos terceirizados	Se algum recurso de processamento de Informação é gerenciado por terceiros. Se os riscos associados a tal gerenciamento são detalhadamente identificados, discutidos com a terceira parte, e controles apropriados foram incorporados no contrato. Se aprovação necessária foi obtida dos empresários e donos de aplicações.		
6.2	8.2	Planejamento e aceitação dos sistemas			
6.2.1	8.2.1	Planejamento de capacidade	Se as demandas de capacidade são monitoradas e projeções de capacidade futuras são realizadas. Isto é para assegurar que a adequada potência de processamento e armazenamento estão disponíveis. Exemplo: Monitoramento do espaço em disco rígido, RAM, CPU em servidores críticos.		
6.2.2	8.2.2	Aceitação de sistemas	Se critérios de aceitação de sistemas foram estabelecidos para novos sistemas de Informação, atualizações e novas versões. Se testes foram realizados antes da aceitação.		
6.3	8.3	Proteção contra software malicioso			

6.3.1	8.3.1	Proteção contra software malicioso	Se existe algum controle contra o uso de software malicioso.		
			Se a política de segurança define características de licenciamento de software como proibição do uso de software não autorizado.		
			Se existe algum procedimento de verificar todos os boletins de aviso referentes ao uso de software malicioso.		
			Se um software antivírus está instalado nos computadores para verificar e isolar ou remover qualquer vírus do computador ou mídia.		
			Se a assinatura deste software está atualizada em uma base regular para verificar por últimas versões de vírus.		
			Se todo o tráfego originado de uma rede insegura para a organização é verificado por vírus. Exemplo: Verificar vírus no e-mail, anexos de e-mail, web, tráfego FTP.		
6.4.1	8.4.1	Cópias de segurança	Se cópias de segurança de informações essenciais aos negócios como servidor de produção, componentes críticos de rede, configuração, etc, são realizadas regularmente. Exemplo: Segunda-Quinta: Cópia incremental. Sexta: Cópia completa.		
			Se a mídia que contém a cópia de segurança e o procedimento para restaurar tal cópia são armazenados seguramente e bem longe do local onde foram realizadas.		
			Se a mídia é regularmente testada para assegurar que os dados poderiam ser restaurados no período de tempo definido no procedimento operacional para restauração.		
6.4.2	8.4.2	Registros de operação	Se o pessoal de operação mantém um registro de suas atividades como nome da pessoa, erros, ação corretiva, etc.		
			Se os registros de operação são verificados regularmente de acordo com os procedimentos operacionais.		
6.4.3	8.4.3	Registros de falhas	Se falhas são reportadas e bem gerenciadas. Isto inclui ações corretivas bem tomadas, revisões de registros de falhas e verificações de ações tomadas.		
6.5.1	8.5.1	Controles da rede	Se controles operacionais eficientes como separar redes e recursos de administração de sistema foram estabelecidos onde necessário.		
			Se responsabilidades e procedimentos de gerenciamento de equipamentos remotos, incluindo equipamentos em área de usuários foram estabelecidos.		
			Se existe algum controle especial para assegurar confidencialidade e integridade do processamento de dados em uma rede pública e para proteger sistemas conectados. Exemplo: Redes privadas virtuais (VPN), outros mecanismos de encriptação e hashing, etc.		
6.6	8.6	Segurança e tratamento de mídias			
6.6.1	8.6.1	Gerenciamento de mídias removíveis	Se existe um procedimento para o gerenciamento de mídia removível de computador como fitas, discos, cassetes, cartões de memória e relatórios.		
6.6.2	8.6.2	Descarte de mídias	Se as mídias que não são mais necessárias são descartadas de forma segura e protegida.		
			Se o descarte de itens sensíveis são registrados quando necessário com o objetivo de manter uma trilha de auditoria.		
6.6.3	8.6.3	Procedimentos para tratamento de informação	Se existe um procedimento para tratar o armazenamento de informação. Este procedimento define características como proteção de informação contra acesso não autorizado ou mal		

			uso da informação.			
6.6.4	8.6.4	Segurança da documentação dos sistemas	Se a documentação do sistema é protegida contra acesso não autorizado. Se a lista de acesso para a documentação do sistema é mantida mínima e autorizada pelo dono da aplicação. Exemplo: Documentação do sistema necessita ser mantida em um drive compartilhado para fins específicos. A documentação necessita ter listas de controle de acessos ativa (para ser acessada somente por usuários limitados).			
6.7	8.7	Troca de informações e software				
6.7.1	8.7.1	Acordos para a troca de informações e software	Se existe algum acordo formal ou informal entre as organizações para a troca de informações ou software. Se o acordo define as características de segurança baseadas na sensibilidade das informações de negócio envolvidas.			
6.7.2	8.7.2	Segurança de mídias em trânsito	Se existe segurança da mídia enquanto está sendo transportada. Se a mídia é bem protegida contra acesso não autorizado, mal uso ou corrupção.			
6.7.3	8.7.3	Segurança de comércio eletrônico	Se o comércio eletrônico é bem protegido e se controle foram implementados para proteção contra atividades fraudulentas, disputa de contrato, exposição ou modificação da informação. Se controles de segurança como autenticação e autorização são considerados no ambiente de comércio eletrônico. Se acordos de comércio eletrônico entre parceiros estão documentados, com concordância de todas as partes, incluindo detalhes de segurança.			
6.7.4	8.7.4	Segurança do correio eletrônico	Se existe uma política ativa para o uso de correio eletrônico ou política de segurança que define características em relação ao uso do correio eletrônico. Se controles como verificação de antivírus, isolamento de anexos potencialmente inseguros, controle de spam, anti relaying, etc, estão ativos para reduzir os riscos criados pelo correio eletrônico.			
6.7.5	8.7.5	Segurança dos sistemas eletrônicos de escritório	Se existe uma política aceitável para definir o uso de sistemas eletrônicos de escritório. Se existe alguma diretriz ativa para controlar efetivamente os negócios e os riscos de segurança associados com os sistemas eletrônicos de escritório.			
6.7.6	8.7.6	Sistemas disponíveis publicamente	Se existe algum processo de autorização formal ativo para a disponibilização pública da informação, como aprovação do controle de mudanças, que inclui empresários, donos de aplicações, etc. Se existe algum controle ativo para proteger a integridade desta informação publicamente disponível contra acesso não autorizado. Isso deve incluir controles como firewalls, obstáculos do sistema operacional, qualquer ferramenta de detecção de intrusão utilizada para monitorar o sistema, etc.			

6.7.7	8.7.7	Outras formas de troca de informação	Se existe alguma política, procedimento ou controle ativo para proteger a troca de informações através do uso de voz, facsimile e dispositivos de comunicação de vídeo. Se os empregados são lembrados de manter a confidencialidade de informações sensíveis enquanto usarem tais formas de troca de informação.			
7	9	Controle de acesso				
7.1	9.1	Requisitos do negócio para controle de acesso				
7.1.1	9.1.1	Política de controle de acesso	Se os requisitos do negócio para controle de acesso foram definidos e documentados. Se a política de controle de acesso define as regras e direitos para cada usuário ou um grupo de usuários. Se os usuários ou provedores de serviço receberam um documento contendo claramente os controles de acesso que satisfaçam os requisitos do negócio.			
7.2	9.2	Gerenciamento de acessos do usuário				
7.2.1	9.2.1	Registro de usuário	Se existe algum procedimento formal de registro e cancelamento de registro para garantir o acesso a todos os sistemas de informação e serviços multiusuários.			
7.2.2	9.2.2	Gerenciamento de privilégios	Se a concessão e o uso de quaisquer privilégios de um sistema de informação multiusuário é restrito e controlado, por exemplo, se privilégios são concedidos pela necessidade do usuário, e somente depois de um processo de autorização formal.			
7.2.3	9.2.3	Gerenciamento de senha dos usuários	Se os usuários são solicitados a assinar uma declaração a fim de manter a confidencialidade de sua senha pessoal. A concessão e alteração de senhas devem ser controladas por um processo de gerenciamento formal.			
7.2.4	9.2.4	Análise crítica dos direitos de acesso do usuário	Se existe um processo de revisão dos direitos de acesso do usuário em intervalos regulares. Exemplo: Revisão de privilégio especial a cada 3 meses, e de privilégios normais a cada 6 meses.			
7.3	9.3	Responsabilidades do usuário				
7.3.1	9.3.1	Uso de senhas	Se existe alguma diretriz para guiar usuários na escolha e manutenção segura de senhas.			
7.3.2	9.3.2	Equipamentos de usuário sem monitoração	Se usuários e prestadores de serviço são avisados dos requisitos de segurança e procedimentos para proteger equipamentos sem monitoração, assim como suas responsabilidades para implementar tal proteção. Exemplo: Efetuar logoff quando a seção for finalizada, ou configurar logoff automático.			
7.3	9.4	Controle de acesso à rede				
7.4.1	9.4.1	Política de utilização dos serviços de rede	Se existe uma política que define preocupações relacionadas a redes e a serviços de rede, como: Partes de rede serem acessadas; Serviços de autorização para a determinação de quem tem acesso a que redes e a quais serviços de rede; Procedimentos e controles de gerenciamento para proteger o acesso às conexões e serviços de rede.			
7.4.2	9.4.2	Rota de rede obrigatória	Se existe algum controle que restringe a rota entre o terminal do usuário e o serviço do computador que o usuário é autorizado a acessar. Exemplo: Criação de uma rota forçada para reduzir riscos.			
7.4.3	9.4.3	Autenticação para conexão externa do usuário	Se existe algum mecanismo de autenticação para conexões externas. Exemplos: Técnicas baseadas em criptografia, dispositivos de tokens, protocolos de desafio/resposta, etc.			

7.4.4	9.4.4	Autenticação de nó	Se conexões a sistemas de computador remoto para fora do gerenciamento de segurança da organização são autenticados. Autenticação de nós podem servir como meio alternativo de autenticação de grupos de usuários quando eles estão conectados a um recurso de computador seguro e compartilhado.			
7.4.5	9.4.5	Proteção de portas de diagnóstico remotas	Se acessos a portas de diagnóstico são seguramente controladas, por exemplo, protegidas por um mecanismo de segurança.			
7.4.6	9.4.6	Segregação de redes	Se a rede (onde parceiros de negócio e/ou terceiros necessitam de acesso ao sistema de informação) é segregada usando mecanismos de segurança de perímetros como firewalls.			
7.4.7	9.4.7	Controle de conexões de rede	Se existe algum controle de conexão de rede para redes compartilhadas que se estendem aos limites da organização. Exemplo: Correio eletrônico, acesso a web, transferências de arquivos, etc.			
7.4.8	9.4.8	Controle de roteamento de rede	Se existe algum controle de rede para assegurar que conexões de computador e fluxo de informações não violam a política de controle de acesso das aplicações de negócio. Isto é sempre essencial para redes compartilhadas com usuários que não pertencem ao quadro da organização (prestadores de serviço).			
			Se os controles de roteamento são baseados em fontes confiáveis e mecanismos de checagem de endereços de destino. Exemplo: NAT (Network Address Translation).			
7.4.9	9.4.9	Segurança dos serviços de rede	Se a organização, utilizando serviço de rede público ou privado, assegura uma descrição clara dos atributos de segurança de todos os serviços disponibilizados.			
7.5	9.5	Controle de acesso ao sistema operacional				
7.5.1	9.5.1	Identificação automática de terminal	Se um mecanismo de identificação automática de terminal é utilizado para autenticar conexões.			
7.5.2	9.5.2	Procedimentos de entrada no sistema (logon)	Se o acesso ao sistema de informação é realizado através de um processo seguro de entrada no sistema. Convém que o procedimento de entrada no sistema de computador seja projetado para minimizar a oportunidade de acessos não autorizados.			
7.5.3	9.5.3	Identificação e autenticação de usuário	Se todos os usuários (incluindo o pessoal de suporte técnico, como operadores, administradores de redes, programadores de sistema e administradores de rede) tenham um identificador único. As contas genéricas de usuário devem somente ser fornecidas sobre circunstâncias excepcionais no qual há um benefício de negócio claro. Controles adicionais devem ser necessários para gerenciar as contas.			
			Se o método de autenticação utilizado confirma a identidade alegada pelo usuário. Método comumente utilizado: Senhas somente conhecidas pelos usuários.			
7.5.4	9.5.4	Sistema de gerenciamento de senhas	Se existe um sistema de gerenciamento de senhas que reforça vários controles de senhas, como: Senha individual, reforça alterações de senha, gravar senha de forma criptografada, não mostrar senhas na tela, etc.			
7.5.5	9.5.2	Uso de programas utilitários	Se programas utilitários do sistema que vêm junto com as instalações do computador, que podem sobrepor os controles do sistema e aplicações, são estritamente controlados.			

7.5.6	9.5.6	Alarme de intimidação para a salvaguarda de usuários	Se a provisão de um alarme de intimidação é considerado para usuários que podem ser alvo de coação.			
7.5.7	9.5.7	Desconexão de terminal por inatividade	Terminais inativos em áreas públicas devem ser configurados para limpar a tela ou desligar automaticamente após um período predeterminado de inatividade.			
7.5.8	9.5.8	Limitação do tempo de conexão	Se existe alguma restrição no tempo de conexão para aplicações de alto risco. Este tipo de configuração pode ser considerada para aplicações sensíveis para as quais terminais são instalados em localizações de alto risco.			
7.6	9.6	Controle de acesso às aplicações				
7.6.1	9.6.1	Restrição de acesso à informação	Se o acesso à aplicação por vários grupos ou pessoal dentro da organização é definido na política de controle de acesso como requisito de aplicação de negócio individual e é consistente com a política de acesso a Informação da organização.			
7.6.2	9.6.2	Isolamento de sistemas sensíveis	Se sistemas sensíveis são isolados do ambiente de computação, como sendo executados em computadores dedicados, recursos compartilhados somente com sistemas de informações confiáveis, etc.			
7.7	9.7	Monitoração do uso e acesso ao sistema				
7.7.1	9.7.1	Registro (log) de eventos	Se trilhas de auditoria registrando as exceções e outros eventos de segurança relevantes são produzidas e mantidas por um período de tempo acordado para auxiliar em investigações futuras e na monitoração do controle de acesso.			
7.7.2	9.7.2	Monitoração do uso do sistema	Se foram estabelecidos procedimentos para a monitoração do uso dos recursos de processamento da informação. Os procedimentos devem assegurar que os usuários estão executando apenas as atividades para as quais eles foram explicitamente autorizados. Se os resultados do monitoramento das atividades são revisados regularmente.			
7.7.3	9.7.3	Sincronização dos relógios	Se os computadores ou dispositivos de comunicação têm a capacidade de operar com um relógio em tempo real, ele deve ser ajustado conforme o padrão adotado, por exemplo, o tempo coordenado universal (Universal Coordinated time – UCT) ou um padrão local de tempo. O estabelecimento correto dos relógios dos computadores é importante para garantir a exatidão dos registros de auditoria.			
7.8	9.8	Computação móvel e trabalho remoto				
7.8.1	9.8.1	Computação móvel	Se uma política formal foi adotada levando em conta os riscos de trabalhar com recursos de computação móvel, como notebooks, palmtops, etc., especialmente em ambientes desprotegidos. Se treinamentos foram preparados para o grupo de trabalho que utiliza a computação móvel, para aumentar o nível de conscientização a respeito dos riscos adicionais resultantes desta forma de trabalho e dos controles que devem ser implementados para aliviar os riscos.			
7.8.2	9.8.2	Trabalho remoto	Se existe alguma política, procedimento e/ou padrão para controlar as atividades do trabalho remoto. Isto deve ser consistente com a política de segurança da informação. Se a proteção apropriada para o local do trabalho remoto foi implantada, para evitar o roubo de equipamentos e de informações ou o uso impróprio destes recursos.			
8	10	Desenvolvimento e manutenção de sistemas				

8.1	10.1	Requisitos de segurança de sistemas			
8.1.1	10.1.1	Análise e especificação dos Requisitos de segurança	Se os requisitos de segurança estão incorporados como parte integrante da declaração dos requisitos do negócio para novos sistemas ou para melhorias dos sistemas existentes. Requisitos de segurança e controles identificados devem refletir o valor, para o negócio, dos ativos de informação envolvidos e o dano potencial ao negócio, que pode resultar da falha ou ausência de segurança. Se a avaliação dos riscos foi completada antes de iniciar o desenvolvimento do sistema.		
8.2	10.2	Segurança nos sistemas de aplicação			
8.2.1	10.2.1	Validação de dados de entrada	Se os dados de entrada do sistema de aplicação são validados para assegurar que estão corretos e são apropriados. Se os controles como: Diferentes tipos de dados de entrada para checar por mensagens de erro, procedimentos em resposta a erros de validação, definição das responsabilidades para todo o pessoal envolvido no processo de entrada de dados, etc., são considerados.		
8.2.2	10.2.2	Controle do processamento interno	Se áreas de risco são identificadas no ciclo de processamento e que checagens de validação foram incluídas. Em alguns casos, os dados que foram corretamente inseridos podem estar corrompidos, devido a erros de processamento ou a atos deliberados. Se controles apropriados são identificados para aplicações para minimizar os riscos durante o processamento interno. Os controles irão depender naturalmente da aplicação e do impacto ao negócio de algum dado corrompido.		
8.2.3	10.2.3	Autenticação de mensagem	Se uma avaliação dos riscos de segurança foi realizada para determinar se a autenticação de mensagens é necessária; e para identificar o método mais apropriado de sua implementação, se necessária. Autenticação de mensagem é uma técnica utilizada para detectar alterações não autorizadas ou corrupção do conteúdo de mensagens eletrônicas transmitidas.		
8.2.4	10.2.4	Validação de dados de saída	Se os dados de saída do sistema de aplicação são validados para assegurar que o processo de armazenamento da informação está correto e apropriado para as circunstâncias.		
8.3	10.3	Controles de criptografia			
8.3.1	10.3.1	Política para o uso de controles de criptografia	Se foi implantada uma política para o uso de controles de criptografia para a proteção da informação. Se foi realizada uma avaliação de risco para identificar qual o nível de proteção da informação deve ser dado.		
8.3.2	10.3.2	Criptografia	Se técnicas de criptografia foram utilizadas para proteger os dados. Se avaliações foram realizadas para analisar a sensibilidade dos dados e o nível de proteção necessária.		
8.3.3	10.3.3	Assinatura digital	Se assinaturas digitais foram utilizadas para proteger a autenticidade e integridade de documentos eletrônicos.		
8.3.4	10.3.4	Serviços de não repúdio	Se serviços de não repúdio foram utilizados, onde eles devem ser necessários para resolver disputas sobre ocorrência ou não ocorrência de um evento ou ação. Exemplo: Disputa envolvendo o uso de assinatura digital em um pagamento ou contrato eletrônico.		

8.3.5	10.3.5	Gerenciamento de chaves	Se existe um sistema de gerenciamento para suportar pela organização o uso de técnicas de criptografia, como técnicas de chave secreta e técnicas de chave pública. Se o sistema de gerenciamento de chaves foi baseado em um conjunto acordado de normas, procedimentos e métodos seguros.			
8.4	10.4	Segurança de arquivos do sistema				
8.4.1	10.4.1	Controle de software em produção	Se foi implantado algum controle para implementação de software em sistemas operacionais. Isto é para minimizar os riscos de corrupção dos sistemas operacionais.			
8.4.2	10.4.2	Proteção de dados de teste do sistema	Se os dados de teste do sistema são protegidos e controlados. O uso de base de dados de produção contendo informações pessoais deve ser evitado para fins de teste. Se tais informações forem utilizadas, os dados devem ser despersonalizados antes do uso.			
8.4.3	10.4.3	Controle de acesso a bibliotecas de programa-fonte	Se foram implantados controles estritos sobre o acesso às bibliotecas de programa-fonte. Isto é para reduzir o potencial de corrupção de programas de computador.			
8.5	10.5	Segurança nos processos de desenvolvimento e suporte				
8.5.1	10.5.1	Procedimentos de controle de mudanças	Se foram implantados controles estritos sobre a implementação de mudanças no sistema de informação. Isto é para minimizar a corrupção do sistema de informação.			
8.5.2	10.5.2	Análise crítica das mudanças técnicas do sistema operacional da produção	Se foram implantados processos ou procedimentos para assegurar que o sistema de aplicação é revisto e testado após mudanças no sistema operacional. Isto é necessário periodicamente para atualizar o sistema operacional, por exemplo, para instalar "Service packs", patches, atualizações rápidas, etc.			
8.5.3	10.5.3	Restrições nas mudanças dos pacotes de software	Se foram implantadas restrições para limitar modificações dos pacotes de softwares. Tão longe quanto possível e praticável, convém que os pacotes de software adquiridos de fornecedores sejam usados sem modificações. Onde as modificações forem consideradas essenciais, o software original deve ser retido e as modificações efetuadas em uma cópia claramente identificada. Todas as modificações devem ser claramente testadas e documentadas, assim elas podem ser reaplicadas se necessário em futuras atualizações do software.			
8.5.4	10.5.4	Covert channels e cavalo de Tróia	Se foram implantados controles para assegurar que covert channels e cavalos de Tróia não foram introduzidos em novos sistemas ou atualizações. Um covert channel pode expor informações por meios indiretos e obscuros. Cavalo de Tróia é desenvolvido para afetar um sistema de forma não autorizada.			
8.5.5	10.5.5	Desenvolvimento terceirizado de software	Se foram implantados controles sobre desenvolvimento terceirizado de software. Os pontos a serem vistos incluem: Acordos sobre licenças, acordos de poder haver falha por parte de prestadores de serviços, certificação de qualidade e da exatidão do trabalho implementado, testes antes da instalação para detecção de cavalos de Tróia, etc.			
9	11	Gestão da continuidade do negócio				
9.1	11.1	Aspectos da gestão da continuidade do negócio				
9.1.1	11.1.1	Processo de gestão da continuidade do negócio	Se foi implantado um processo de gerenciamento que permeie toda a organização para desenvolvimento e manutenção da continuidade do negócio. Isto deve incluir um plano amplo de continuidade de negócio da organização, testes regulares e atualizações de planos, formulação e documentação de estratégia de continuidade de			

			negócio, etc.		
9.1.2	11.1.2	Continuidade do negócio e análise do impacto	Se eventos que podem causar interrupções ao processo de negócio foram identificados. Exemplo: Falha de equipamento, inundação e fogo.		
			Se foi realizada uma avaliação de risco para determinar o impacto de tais interrupções.		
			Se um plano estratégico foi desenvolvido baseado nos resultados da avaliação de risco para determinar uma aproximação global da continuidade do negócio.		
9.1.3	11.1.3	Documentado e implementando planos de continuidade	Se foram desenvolvidos planos para restaurar operações do negócio dentro de um período de tempo requerido após uma interrupção ou falha do processo de negócio.		
			Se o plano é regularmente testado e atualizado.		
9.1.4	11.1.4	Estrutura do plano de continuidade do negócio	Se existe uma estrutura única de plano de continuidade do negócio.		
			Se esta estrutura é mantida para assegurar que todos os planos sejam consistentes e para identificar prioridades para testes e manutenção.		
			Se esta estrutura identifica condições de ativação e responsabilidades individuais para execução de cada componente do plano.		
9.1.5	11.1.5	Testes, manutenção e reavaliação dos planos de continuidade do negócio	Se planos de continuidade do negócio são testados regularmente para assegurar que estão atualizados e são eficientes.		
			Se planos de continuidade do negócio foram mantidos por revisões regulares e atualizados para assegurar que eles continuam eficientes.		
			Se procedimentos foram incluídos dentro do programa de gerenciamento de mudanças da organização para assegurar que as questões relativas à continuidade do negócio estão devidamente tratadas.		
10	12	Conformidade			
10.1	12.1	Conformidade com requisitos legais			
10.1.1	12.1.1	Identificação da legislação vigente	Se todos os estatutos, regulamentações e cláusulas contratuais relevantes foram explicitamente definidos e documentados para cada sistema de informação.		
			Se controles e responsabilidades específicos para atender a estes requisitos foram definidos e documentados.		
10.1.2	12.1.2	Direitos de propriedade intelectual	Se existe algum procedimento para assegurar conformidade com as restrições legais no uso de material de acordo com as leis de propriedade intelectual, como as de direitos autorais, patentes ou marcas registradas.		
			Se todos os procedimentos foram bem implementados.		
			Se produtos de software proprietários são fornecidos sob um contrato de licenciamento que restringe o uso dos produtos em máquinas especificadas e que pode limitar a cópia apenas para criação de uma cópia de segurança.		
10.1.3	12.1.3	Salvaguarda de registros organizacionais	Se registros importantes da organização são protegidos contra perda, destruição ou falsificação.		
10.1.4	12.1.4	Proteção de dados e privacidade da	Se foi implantada uma estrutura de gerenciamento e controle para proteger dados e a privacidade da informação pessoal		

		informação pessoal			
10.1.5	12.1.5	Prevenção contra o uso indevido de recursos de processamento da informação	Se o uso de recursos de processamento da informação para algum propósito sem relação com o negócio ou não autorizado, sem aprovação da direção, é tratado como uso impróprio do recurso.		
			Se é apresentada uma mensagem na tela do computador, no log-on, indicando que o sistema é privado e o acesso não autorizado não é permitido.		
10.1.6	12.1.6	Regulamentação de controles de criptografia	Se a regulamentação de controles de criptografia está legal com o acordo local e nacional.		
10.1.7	12.1.7	Coleta de evidências	Se o processo envolvido na coleta de evidências está de acordo com as práticas legais e industriais.		
10.2	12.2	Análise crítica da política de segurança e da conformidade técnica			
10.2.1	12.2.1	Conformidade com a política de segurança	Se todas as áreas dentro da organização sejam consideradas na análise crítica periódica, para garantir a conformidade com as normas e políticas de segurança.		
10.2.2	12.2.2	Verificação da conformidade técnica	Se os sistemas de informação são periodicamente verificados em sua conformidade com as normas de segurança implementadas.		
			Se a verificação de conformidade técnica é liderada ou supervisionada por pessoas competentes e autorizadas.		
10.3	12.3	Considerações quanto à auditoria dos sistemas			
10.3.1	12.3.1	Controles de auditoria de sistema	Se requisitos de auditoria e atividades envolvendo verificações em sistemas operacionais são cuidadosamente planejados e acordados para minimizar o risco de interrupção dos processos do negócio.		
10.3.2	12.3.2	Proteção das ferramentas de auditoria de sistemas	Se o acesso a ferramentas de auditoria de sistemas, como software ou arquivos de dados, é protegidos para prevenir contra qualquer possibilidade de uso impróprio ou comprometimento.		
Ativos		Nível	Descrição		
Equipamentos					
Aplicações					

Usuários			
Ambientes			
Informações			
Processos			

Nível: 1=Irrelevante; 2=Relevante; 3=Importante; 4=Crítico; 5=Vital