Anexo A
(normativo)

Objetivos de controle e controles

Os objetivos de controle e controles listados na tabela A.1 são derivados diretamente e estão alinhados com aqueles listados na ABNT NBR ISO/IEC 17799:2005 – seções 5 a 15. As listas na tabela A.1 não são exaustivas e uma organização pode considerar que objetivos de controle e controles adicionais são necessários. Os objetivos de controle e controles desta tabela devem ser selecionados como parte do processo de SGSI especificado em 4.2.1.

A ABNT NBR ISO/IEC 17799:2005 - seções 5 a 15 fornece recomendações e um guia de implementação das melhores práticas para apoiar os controles especificados em A.5 a A.15.

Tabela A.1 — Objetivos de controle e controles

A.5 Política de segurança		
A.5.1 Política de segurança da informação *Objetivo:* 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.		
A.5.1.1	Documento da política de segurança da informação	*Controle* Um documento da política de segurança da informação deve ser aprovado pela direção, publicado e comunicado para todos os funcionários e partes externas relevantes.
A.5.1.2	Análise crítica da política de segurança da informação	*Controle* A política de segurança da informação deve ser analisada criticamente a intervalos planejados ou quando mudanças significativas ocorrerem, para assegurar a sua contínua pertinência, adequação e eficácia.
A.6 Organizando a segurança da informação		
A.6.1 Infra-estrutura da segurança da informação *Objetivo:* Gerenciar a segurança da informação dentro da organização.		
A.6.1.1	Comprometimento da direção com a segurança da informação	*Controle* A Direção deve apoiar ativamente a segurança da informação dentro da organização, por meio de um claro direcionamento, demonstrando o seu comprometimento, definindo atribuições de forma explícita e conhecendo as responsabilidades pela segurança da informação.
A.6.1.2	Coordenação da segurança da informação	*Controle* As atividades de segurança da informação devem ser coordenadas por representantes de diferentes partes da organização, com funções e papéis relevantes.

A.6.1.3	Atribuição de responsabilidades para a segurança da informação	*Controle* Todas as responsabilidades pela segurança da informação devem estar claramente definidas.
A.6.1.4	Processo de autorização para os recursos de processamento da informação	*Controle* Deve ser definido e implementado um processo de gestão de autorização para novos recursos de processamento da informação.
A.6.1.5	Acordos de confidencialidade	*Controle* Os requisitos para confidencialidade ou acordos de não divulgação que reflitam as necessidades da organização para a proteção da informação devem ser identificados e analisados criticamente, de forma regular.
A.6.1.6	Contato com autoridades	*Controle* Contatos apropriados com autoridades relevantes devem ser mantidos.
A.6.1.7	Contato com grupos especiais	*Controle* Contatos apropriados com grupos de interesses especiais ou outros fóruns especializados de segurança da informação e associações profissionais devem ser mantidos.
A.6.1.8	Análise crítica independente de segurança da informação	*Controle* O enfoque da organização para gerenciar a segurança da informação e a sua implementação (por exemplo, controles, objetivo dos controles, políticas, processos e procedimentos para a segurança da informação) deve ser analisado criticamente, de forma independente, a intervalos planejados, ou quando ocorrerem mudanças significativas relativas à implementação da segurança da informação.
A.6.2 Partes externas *Objetivo:* Manter a segurança dos recursos de processamento da informação e da informação da organização, que são acessados, processados, comunicados ou gerenciados por partes externas.		
A.6.2.1	Identificação dos riscos relacionados com partes externas	*Controle* Os riscos para os recursos de processamento da informação e para a informação da organização oriundos de processos do negócio que envolvam as partes externas devem ser identificados e controles apropriados devem ser implementados antes de se conceder o acesso.
A.6.2.2	Identificando a segurança da informação quando tratando com os clientes.	*Controle* Todos os requisitos de segurança da informação identificados devem ser considerados antes de conceder aos clientes o acesso aos ativos ou às informações da organização.
A.6.2.3	Identificando segurança da informação nos acordos com terceiros	*Controle* Os acordos com terceiros envolvendo o acesso, processamento, comunicação ou gerenciamento dos recursos de processamento da informação ou da informação da organização, ou o acréscimo de produtos ou serviços aos recursos de processamento da informação devem cobrir todos os requisitos de segurança da informação relevantes.

A.7 Gestão de ativos		
A.7.1 Responsabilidade pelos ativos		
Objetivo: Alcançar e manter a proteção adequada dos ativos da organização.		
A.7.1.1	Inventário dos ativos	*Controle* Todos os ativos devem ser claramente identificados e um inventário de todos os ativos importantes deve ser estruturado e mantido.
A.7.1.2	Proprietário dos ativos	*Controle* Todas as informações e ativos associados com os recursos de processamento da informação devem ter um "proprietário"[3)] designado por uma parte definida da organização.
A.7.1.3	Uso aceitável dos ativos	*Controle* Devem ser identificadas, documentadas e implementadas regras para que seja permitido o uso de informações e de ativos associados aos recursos de processamento da informação.
A.7.2 Classificação da informação		
Objetivo: Assegurar que a informação receba um nível adequado de proteção.		
A.7.2.1	Recomendações para classificação	*Controle* A informação deve ser classificada em termos do seu valor, requisitos legais, sensibilidade e criticidade para a organização.
A.7.2.2	Rótulos e tratamento da informação	*Controle* Um conjunto apropriado de procedimentos para rotular e tratar a informação deve ser definido e implementado de acordo com o esquema de classificação adotado pela organização.
A.8 Segurança em recursos humanos		
A.8.1 Antes da contratação[4)]		
Objetivo: Assegurar que os funcionários, fornecedores e terceiros entendam suas responsabilidades, e estejam de acordo com os seus papéis, e reduzir o risco de roubo, fraude ou mau uso de recursos.		
A.8.1.1	Papéis e responsabilidades	*Controle* Os papéis e responsabilidades pela segurança da informação de funcionários, fornecedores e terceiros devem ser definidos e documentados de acordo com a política de segurança da informação da organização.

[3)] Explicação: O termo “proprietário” identifica uma pessoa ou organismo que tenha uma responsabilidade autorizada para controlar a produção, o desenvolvimento, a manutenção, o uso e a segurança dos ativos. O termo “proprietário” não significa que a pessoa realmente tenha qualquer direito de propriedade pelo ativo

[4)] Explicação: A palavra “contratação”, neste contexto, visa cobrir todas as seguintes diferentes situações: contratação de pessoas (temporárias ou por longa duração), nomeação de funções, mudança de funções, atribuições de contratos e encerramento de quaisquer destas situações.

A.8.1.2	Seleção	*Controle* Verificações de controle de todos os candidatos a emprego, fornecedores e terceiros devem ser realizadas de acordo com as leis relevantes, regulamentações e éticas, e proporcionalmente aos requisitos do negócio, à classificação das informações a serem acessadas e aos riscos percebidos.
A.8.1.3	Termos e condições de contratação	*Controle* Como parte das suas obrigações contratuais, os funcionários, fornecedores e terceiros devem concordar e assinar os termos e condições de sua contratação para o trabalho, os quais devem declarar as suas responsabilidade e da organização para a segurança da informação.
A.8.2 Durante a contratação		
Objetivo: Assegurar que os funcionários, fornecedores e terceiros estão conscientes das ameaças e preocupações relativas à segurança da informação, suas responsabilidades e obrigações, e estão preparados para apoiar a política de segurança da informação da organização durante os seus trabalhos normais, e para reduzir o risco de erro humano.		
A.8.2.1	Responsabilidades da direção	*Controle* A direção deve solicitar aos funcionários, fornecedores e terceiros que pratiquem a segurança da informação de acordo com o estabelecido nas políticas e procedimentos da organização.
A.8.2.2	Conscientização, educação e treinamento em segurança da informação	*Controle* Todos os funcionários da organização e, onde pertinente, fornecedores e terceiros devem receber treinamento apropriado em conscientização, e atualizações regulares nas políticas e procedimentos organizacionais relevantes para as suas funções.
A.8.2.3	Processo disciplinar	*Controle* Deve existir um processo disciplinar formal para os funcionários que tenham cometido uma violação da segurança da informação.
A.8.3 Encerramento ou mudança da contratação		
Objetivo: Assegurar que funcionários, fornecedores e terceiros deixem a organização ou mudem de trabalho de forma ordenada.		
A.8.3.1	Encerramento de atividades	*Controle* As responsabilidades para realizar o encerramento ou a mudança de um trabalho devem ser claramente definidas e atribuídas.
A.8.3.2	Devolução de ativos	*Controle* Todos os funcionários, fornecedores e terceiros devem devolver todos os ativos da organização que estejam em sua posse após o encerramento de suas atividades, do contrato ou acordo.

A.8.3.3	Retirada de direitos de acesso	*Controle* Os direitos de acesso de todos os funcionários, fornecedores e terceiros às informações e aos recursos de processamento da informação devem ser retirados após o encerramento de suas atividades, contratos ou acordos, ou devem ser ajustados após a mudança destas atividades.
A.9 Segurança física e do ambiente		
A.9.1 Áreas seguras *Objetivo:* Prevenir o acesso físico não autorizado, danos e interferências com as instalações e informações da organização.		
A.9.1.1	Perímetro de segurança física	*Controle* Devem ser utilizados perímetros de segurança (barreiras tais como paredes, portões de entrada controlados por cartão ou balcões de recepção com recepcionistas) para proteger as áreas que contenham informações e recursos de processamento da informação.
A.9.1.2	Controles de entrada física	*Controle* As áreas seguras devem ser protegidas por controles apropriados de entrada para assegurar que somente pessoas autorizadas tenham acesso.
A.9.1.3	Segurança em escritórios salas e instalações	*Controle* Deve ser projetada e aplicada segurança física para escritórios, salas e instalações.
A.9.1.4	Proteção contra ameaças externas e do meio ambiente	*Controle* Deve ser projetada e aplicada proteção física contra incêndios, enchentes, terremotos, explosões, perturbações da ordem pública e outras formas de desastres naturais ou causados pelo homem.
A.9.1.5	Trabalhando em áreas seguras	*Controle* Deve ser projetada e aplicada proteção física, bem como diretrizes para o trabalho em áreas seguras.
A.9.1.6	Acesso do público, áreas de entrega e de carregamento	*Controle* Pontos de acesso, tais como áreas de entrega e de carregamento e outros pontos em que pessoas não autorizadas possam entrar nas instalações, devem ser controlados e, se possível, isolados dos recursos de processamento da informação, para evitar o acesso não autorizado.
A.9.2 Segurança de equipamentos *Objetivo:* Impedir perdas, danos, furto ou comprometimento de ativos e interrupção das atividades da organização.		
A.9.2.1	Instalação e proteção do equipamento	*Controle* Os equipamentos devem ser colocados no local ou protegidos para reduzir os riscos de ameaças e perigos do meio ambiente, bem como as oportunidades de acesso não autorizado.

A.9.2.2	Utilidades	*Controle* Os equipamentos devem ser protegidos contra falta de energia elétrica e outras interrupções causadas por falhas das utilidades.
A.9.2.3	Segurança do cabeamento	*Controle* O cabeamento de energia e de telecomunicações que transporta dados ou dá suporte aos serviços de informações deve ser protegido contra interceptação ou danos.
A.9.2.4	Manutenção dos equipamentos	*Controle* Os equipamentos devem ter manutenção correta, para assegurar sua disponibilidade e integridade permanente.
A.9.2.5	Segurança de equipamentos fora das dependências da organização	*Controle* Devem ser tomadas medidas de segurança para equipamentos que operem fora do local, levando em conta os diferentes riscos decorrentes do fato de se trabalhar fora das dependências da organização.
A.9.2.6	Reutilização e alienação segura de equipamentos	*Controle* Todos os equipamentos que contenham mídias de armazenamento de dados devem ser examinados antes do descarte, para assegurar que todos os dados sensíveis e *softwares* licenciados tenham sido removidos ou sobregravados com segurança.
A.9.2.7	Remoção de propriedade	*Controle* Equipamentos, informações ou *software* não devem ser retirados do local sem autorização prévia.
A.10 Gerenciamento das operações e comunicações		
A.10.1 Procedimentos e responsabilidades operacionais *Objetivo:* Garantir a operação segura e correta dos recursos de processamento da informação.		
A.10.1.1	Documentação dos procedimentos de operação	*Controle* Os procedimentos de operação devem ser documentados, mantidos atualizados e disponíveis a todos os usuários que deles necessitem.
A.10.1.2	Gestão de mudanças	*Controle* Modificações nos recursos de processamento da informação e sistemas devem ser controladas.
A.10.1.3	Segregação de funções	*Controle* Funções e áreas de responsabilidade devem ser segregadas para reduzir as oportunidades de modificação ou uso indevido não autorizado ou não intencional dos ativos da organização.
A.10.1.4	Separação dos recursos de desenvolvimento, teste e de produção	*Controle* Recursos de desenvolvimento, teste e produção devem ser separados para reduzir o risco de acessos ou modificações não autorizadas aos sistemas operacionais.

A.10.2 Gerenciamento de serviços terceirizados		
Objetivo: Implementar e manter o nível apropriado de segurança da informação e de entrega de serviços em consonância com acordos de entrega de serviços terceirizados.		
A.10.2.1	Entrega de serviços	*Controle* Deve ser garantido que os controles de segurança, as definições de serviço e os níveis de entrega incluídos no acordo de entrega de serviços terceirizados sejam implementados, executados e mantidos pelo terceiro.
A.10.2.2	Monitoramento e análise crítica de serviços terceirizados	*Controle* Os serviços, relatórios e registros fornecidos por terceiro devem ser regularmente monitorados e analisados criticamente, e auditorias devem ser executadas regularmente.
A.10.2.3	Gerenciamento de mudanças para serviços terceirizados	*Controle* Mudanças no provisionamento dos serviços, incluindo manutenção e melhoria da política de segurança da informação, dos procedimentos e controles existentes, devem ser gerenciadas levando-se em conta a criticidade dos sistemas e processos de negócio envolvidos e a reanálise/reavaliação de riscos.
A.10.3 Planejamento e aceitação dos sistemas		
Objetivo: Minimizar o risco de falhas nos sistemas.		
A.10.3.1	Gestão de capacidade	*Controle* A utilização dos recursos deve ser monitorada e sincronizada e as projeções devem ser feitas para necessidades de capacidade futura, para garantir o desempenho requerido do sistema.
A.10.3.2	Aceitação de sistemas	*Controle* Devem ser estabelecidos critérios de aceitação para novos sistemas, atualizações e novas versões e que sejam efetuados testes apropriados do(s) sistema(s) durante seu desenvolvimento e antes da sua aceitação.
A.10.4 Proteção contra códigos maliciosos e códigos móveis		
Objetivo: Proteger a integridade do *software* e da informação.		
A.10.4.1	Controle contra códigos maliciosos	*Controle* Devem ser implantados controles de detecção, prevenção e recuperação para proteger contra códigos maliciosos, assim como procedimentos para a devida conscientização dos usuários.
A.10.4.2	Controles contra códigos móveis	*Controle* Onde o uso de códigos móveis é autorizado, a configuração deve garantir que o código móvel autorizado opere de acordo com uma política de segurança da informação claramente definida e que códigos móveis não autorizados tenham sua execução impedida.

A.10.5 Cópias de segurança		
Objetivo: Manter a integridade e disponibilidade da informação e dos recursos de processamento de informação.		
A.10.5.1	Cópias de segurança das informações	*Controle* Cópias de segurança das informações e dos *softwares* devem ser efetuadas e testadas regularmente, conforme a política de geração de cópias de segurança definida.
A.10.6 Gerenciamento da segurança em redes		
Objetivo: Garantir a proteção das informações em redes e a proteção da infra-estrutura de suporte.		
A.10.6.1	Controles de redes	*Controle* Redes devem ser adequadamente gerenciadas e controladas, de forma a protegê-las contra ameaças e manter a segurança de sistemas e aplicações que utilizam estas redes, incluindo a informação em trânsito.
A.10.6.2	Segurança dos serviços de rede	*Controle* Características de segurança, níveis de serviço e requisitos de gerenciamento dos serviços de rede devem ser identificados e incluídos em qualquer acordo de serviços de rede, tanto para serviços de rede providos internamente como para terceirizados.
A.10.7 Manuseio de mídias		
Objetivo: Prevenir contra divulgação não autorizada, modificação, remoção ou destruição aos ativos e interrupções das atividades do negócio.		
A.10.7.1	Gerenciamento de mídias removíveis	*Controle* Devem existir procedimentos implementados para o gerenciamento de mídias removíveis.
A.10.7.2	Descarte de mídias	*Controle* As mídias devem ser descartadas de forma segura e protegida quando não forem mais necessárias, por meio de procedimentos formais.
A.10.7.3	Procedimentos para tratamento de informação	*Controle* Devem ser estabelecidos procedimentos para o tratamento e o armazenamento de informações, para proteger tais informações contra a divulgação não autorizada ou uso indevido.
A.10.7.4	Segurança da documentação dos sistemas	*Controle* A documentação dos sistemas deve ser protegida contra acessos não autorizados.
A.10.8 Troca de informações		
Objetivo: Manter a segurança na troca de informações e *softwares* internamente à organização e com quaisquer entidades externas.		
A.10.8.1	Políticas e procedimentos para troca de informações	*Controle* Políticas, procedimentos e controles devem ser estabelecidos e formalizados para proteger a troca de informações em todos os tipos de recursos de comunicação.

A.10.8.2	Acordos para a troca de informações	*Controle* Devem ser estabelecidos acordos para a troca de informações e *softwares* entre a organização e entidades externas.
A.10.8.3	Mídias em trânsito	*Controle* Mídias contendo informações devem ser protegidas contra acesso não autorizado, uso impróprio ou alteração indevida durante o transporte externo aos limites físicos da organização.
A.10.8.4	Mensagens eletrônicas	*Controle* As informações que trafegam em mensagens eletrônicas devem ser adequadamente protegidas.
A.10.8.5	Sistemas de informações do negócio	*Controle* Políticas e procedimentos devem ser desenvolvidos e implementados para proteger as informações associadas com a interconexão de sistemas de informações do negócio.
A.10.9 Serviços de comércio eletrônico *Objetivo:* Garantir a segurança de serviços de comércio eletrônico e sua utilização segura.		
A.10.9.1	Comércio eletrônico	*Controle* As informações envolvidas em comércio eletrônico transitando sobre redes públicas devem ser protegidas de atividades fraudulentas, disputas contratuais, divulgação e modificações não autorizadas.
A.10.9.2	Transações *on-line*	*Controle* Informações envolvidas em transações *on-line* devem ser protegidas para prevenir transmissões incompletas, erros de roteamento, alterações não autorizadas de mensagens, divulgação não autorizada, duplicação ou reapresentação de mensagem não autorizada.
A.10.9.3	Informações publicamente disponíveis	*Controle* A integridade das informações disponibilizadas em sistemas publicamente acessíveis deve ser protegida, para prevenir modificações não autorizadas.
A.10.10 Monitoramento *Objetivo:* Detectar atividades não autorizadas de processamento da informação.		
A.10.10.1	Registros de auditoria	*Controle* Registros (*log*) de auditoria contendo atividades dos usuários, exceções e outros eventos de segurança da informação devem ser produzidos e mantidos por um período de tempo acordado para auxiliar em futuras investigações e monitoramento de controle de acesso.
A.10.10.2	Monitoramento do uso do sistema	*Controle* Devem ser estabelecidos procedimentos para o monitoramento do uso dos recursos de processamento da informação e os resultados das atividades de monitoramento devem ser analisados criticamente, de forma regular.

A.10.10.3	Proteção das informações dos registros (*logs*)	*Controle* Os recursos e informações de registros (*log*) devem ser protegidos contra falsificação e acesso não autorizado.
A.10.10.4	Registros (*log*) de administrador e operador	*Controle* As atividades dos administradores e operadores do sistema devem ser registradas.
A.10.10.5	Registros (*logs*) de falhas	*Controle* As falhas ocorridas devem ser registradas e analisadas, e devem ser adotadas as ações apropriadas.
A.10.10.6	Sincronização dos relógios	*Controle* Os relógios de todos os sistemas de processamento de informações relevantes, dentro da organização ou do domínio de segurança, devem ser sincronizados de acordo com uma hora oficial.
A.11 Controle de acessos		
A.11.1 Requisitos de negócio para controle de acesso *Objetivo:* Controlar o acesso à informação.		
A.11.1.1	Política de controle de acesso	*Controle* A política de controle de acesso deve ser estabelecida, documentada e analisada criticamente, tomando-se como base os requisitos de acesso dos negócios e da segurança da informação.
A.11.2 Gerenciamento de acesso do usuário *Objetivo:* Assegurar acesso de usuário autorizado e prevenir acesso não autorizado a sistemas de informação.		
A.11.2.1	Registro de usuário	*Controle* Deve existir um procedimento formal de registro e cancelamento de usuário para garantir e revogar acessos em todos os sistemas de informação e serviços.
A.11.2.2	Gerenciamento de privilégios	*Controle* A concessão e o uso de privilégios devem ser restritos e controlados.
A.11.2.3	Gerenciamento de senha do usuário	*Controle* A concessão de senhas deve ser controlada por meio de um processo de gerenciamento formal.
A.11.2.4	Análise crítica dos direitos de acesso de usuário	*Controle* O gestor deve conduzir a intervalos regulares a análise crítica dos direitos de acesso dos usuários, por meio de um processo formal.

A.11.3 Responsabilidades dos usuários		
Objetivo: Prevenir o acesso não autorizado dos usuários e evitar o comprometimento ou roubo da informação e dos recursos de processamento da informação.		
A.11.3.1	Uso de senhas	*Controle* Os usuários devem ser orientados a seguir boas práticas de segurança da informação na seleção e uso de senhas.
A.11.3.2	Equipamento de usuário sem monitoração	*Controle* Os usuários devem assegurar que os equipamentos não monitorados tenham proteção adequada.
A.11.3.3	Política de mesa limpa e tela limpa	*Controle* Deve ser adotada uma política de mesa limpa de papéis e mídias de armazenamento removíveis e uma política de tela limpa para os recursos de processamento da informação.
A.11.4 Controle de acesso à rede		
Objetivo: Prevenir acesso não autorizado aos serviços de rede.		
A.11.4.1	Política de uso dos serviços de rede	*Controle* Os usuários devem receber acesso somente aos serviços que tenham sido especificamente autorizados a usar.
A.11.4.2	Autenticação para conexão externa do usuário	*Controle* Métodos apropriados de autenticação devem ser usados para controlar o acesso de usuários remotos.
A.11.4.3	Identificação de equipamento em redes	*Controle* Devem ser consideradas as identificações automáticas de equipamentos como um meio de autenticar conexões vindas de localizações e equipamentos específicos.
A.11.4.4	Proteção e configuração de portas de diagnóstico remotas	*Controle* Deve ser controlado o acesso físico e lógico para diagnosticar e configurar portas.
A.11.4.5	Segregação de redes	*Controle* Grupos de serviços de informação, usuários e sistemas de informação devem ser segregados em redes.
A.11.4.6	Controle de conexão de rede	*Controle* Para redes compartilhadas, especialmente as que se estendem pelos limites da organização, a capacidade de usuários para conectar-se à rede deve ser restrita, de acordo com a política de controle de acesso e os requisitos das aplicações do negócio (ver 11.1).
A.11.4.7	Controle de roteamento de redes	*Controle* Deve ser implementado controle de roteamento na rede para assegurar que as conexões de computador e fluxos de informação não violem a política de controle de acesso das aplicações do negócio.

A.11.5 Controle de acesso ao sistema operacional		
Objetivo: Prevenir acesso não autorizado aos sistemas operacionais.		
A.11.5.1	Procedimentos seguros de entrada no sistema (*log-on*)	*Controle* O acesso aos sistemas operacionais deve ser controlado por um procedimento seguro de entrada no sistema (*log-on*).
A.11.5.2	Identificação e autenticação de usuário	*Controle* Todos os usuários devem ter um identificador único (ID de usuário), para uso pessoal e exclusivo, e uma técnica adequada de autenticação deve ser escolhida para validar a identidade alegada por um usuário.
A.11.5.3	Sistema de gerenciamento de senha	*Controle* Sistemas para gerenciamento de senhas devem ser interativos e assegurar senhas de qualidade.
A.11.5.4	Uso de utilitários de sistema	*Controle* O uso de programas utilitários que podem ser capazes de sobrepor os controles dos sistemas e aplicações deve ser restrito e estritamente controlado.
A.11.5.5	Desconexão de terminal por inatividade	*Controle* Terminais inativos devem ser desconectados após um período definido de inatividade.
A.11.5.6	Limitação de horário de conexão	*Controle* Restrições nos horários de conexão devem ser utilizadas para proporcionar segurança adicional para aplicações de alto risco.
A.11.6 Controle de acesso à aplicação e à informação		
Objetivo: Prevenir acesso não autorizado à informação contida nos sistemas de aplicação.		
A.11.6.1	Restrição de acesso à informação	*Controle* O acesso à informação e às funções dos sistemas de aplicações por usuários e pessoal de suporte deve ser restrito de acordo com o definido na política de controle de acesso.
A.11.6.2	Isolamento de sistemas sensíveis	*Controle* Sistemas sensíveis devem ter um ambiente computacional dedicado (isolado).
A.11.7 Computação móvel e trabalho remoto		
Objetivo: Garantir a segurança da informação quando se utilizam a computação móvel e recursos de trabalho remoto.		
A.11.7.1	Computação e comunicação móvel	*Controle* Uma política formal deve ser estabelecida e medidas de segurança apropriadas devem ser adotadas para a proteção contra os riscos do uso de recursos de computação e comunicação móveis.
A.11.7.2	Trabalho remoto	*Controle* Uma política, planos operacionais e procedimentos devem ser desenvolvidos e implementados para atividades de trabalho remoto.

A.12 Aquisição, desenvolvimento e manutenção de sistemas de informação		
A.12.1 Requisitos de segurança de sistemas de informação *Objetivo:* Garantir que segurança é parte integrante de sistemas de informação.		
A.12.1.1	Análise e especificação dos requisitos de segurança	*Controle* Devem ser especificados os requisitos para controles de segurança nas especificações de requisitos de negócios, para novos sistemas de informação ou melhorias em sistemas existentes.
A.12.2 Processamento correto de aplicações *Objetivo:* Prevenir a ocorrência de erros, perdas, modificação não autorizada ou mau uso de informações em aplicações.		
A.12.2.1	Validação dos dados de entrada	*Controle* Os dados de entrada de aplicações devem ser validados para garantir que são corretos e apropriados.
A.12.2.2	Controle do processamento interno	*Controle* Devem ser incorporadas, nas aplicações, checagens de validação com o objetivo de detectar qualquer corrupção de informações, por erros ou por ações deliberadas.
A.12.2.3	Integridade de mensagens	*Controle* Requisitos para garantir a autenticidade e proteger a integridade das mensagens em aplicações devem ser identificados e os controles apropriados devem ser identificados e implementados.
A.12.2.4	Validação de dados de saída	*Controle* Os dados de saída das aplicações devem ser validados para assegurar que o processamento das informações armazenadas está correto e é apropriado às circunstâncias.
A.12.3 Controles criptográficos *Objetivo:* Proteger a confidencialidade, a autenticidade ou a integridade das informações por meios criptográficos.		
A.12.3.1	Política para o uso de controles criptográficos	*Controle* Deve ser desenvolvida e implementada uma política para o uso de controles criptográficos para a proteção da informação.
A.12.3.2	Gerenciamento de chaves	*Controle* Um processo de gerenciamento de chaves deve ser implantado para apoiar o uso de técnicas criptográficas pela organização.
A.12.4 Segurança dos arquivos do sistema *Objetivo:* Garantir a segurança de arquivos de sistema.		
A.12.4.1	Controle de *software* operacional	*Controle* Procedimentos para controlar a instalação de *software* em sistemas operacionais devem ser implementados.
A.12.4.2	Proteção dos dados para teste de sistema	*Controle* Os dados de teste devem ser selecionados com cuidado, protegidos e controlados.

A.12.4.3	Controle de acesso ao código- fonte de programa	*Controle* O acesso ao código-fonte de programa deve ser restrito.
A.12.5 Segurança em processos de desenvolvimento e de suporte *Objetivo:* Manter a segurança de sistemas aplicativos e da informação.		
A.12.5.1	Procedimentos para controle de mudanças	*Controle* A implementação de mudanças deve ser controlada utilizando procedimentos formais de controle de mudanças.
A.12.5.2	Análise crítica técnica das aplicações após mudanças no sistema operacional	*Controle* Aplicações críticas de negócios devem ser analisadas criticamente e testadas quando sistemas operacionais são mudados, para garantir que não haverá nenhum impacto adverso na operação da organização ou na segurança.
A.12.5.3	Restrições sobre mudanças em pacotes de *software*	*Controle* Modificações em pacotes de *software* não devem ser incentivadas e devem estar limitadas às mudanças necessárias, e todas as mudanças devem ser estritamente controladas.
A.12.5.4	Vazamento de informações	*Controle* Oportunidades para vazamento de informações devem ser prevenidas.
A.12.5.5	Desenvolvimento terceirizado de *software*	*Controle* A organização deve supervisionar e monitorar o desenvolvimento terceirizado de *software*.
A.12.6 Gestão de vulnerabilidades técnicas *Objetivo:* Reduzir riscos resultantes da exploração de vulnerabilidades técnicas conhecidas.		
A.12.6.1	Controle de vulnerabilidades técnicas	*Controle* Deve ser obtida informação em tempo hábil sobre vulnerabilidades técnicas dos sistemas de informação em uso, avaliada a exposição da organização a estas vulnerabilidades e tomadas as medidas apropriadas para lidar com os riscos associados.
A.13 Gestão de incidentes de segurança da informação		
A.13.1 Notificação de fragilidades e eventos de segurança da informação *Objetivo:* Assegurar que fragilidades e eventos de segurança da informação associados com sistemas de informação sejam comunicados, permitindo a tomada de ação corretiva em tempo hábil.		
A.13.1.1	Notificação de eventos de segurança da informação	*Controle* Os eventos de segurança da informação devem ser relatados através dos canais apropriados da direção, o mais rapidamente possível.
A.13.1.2	Notificando fragilidades de segurança da informação	*Controle* Os funcionários, fornecedores e terceiros de sistemas e serviços de informação devem ser instruídos a registrar e notificar qualquer observação ou suspeita de fragilidade em sistemas ou serviços.

A.13.2 Gestão de incidentes de segurança da informação e melhorias		
Objetivo: Assegurar que um enfoque consistente e efetivo seja aplicado à gestão de incidentes de segurança da informação.		
A.13.2.1	Responsabilidades e procedimentos	*Controle* Responsabilidades e procedimentos de gestão devem ser estabelecidos para assegurar respostas rápidas, efetivas e ordenadas a incidentes de segurança da informação.
A.13.2.2	Aprendendo com os incidentes de segurança da informação	*Controle* Devem ser estabelecidos mecanismos para permitir que tipos, quantidades e custos dos incidentes de segurança da informação sejam quantificados e monitorados.
A.13.2.3	Coleta de evidências	*Controle* Nos casos em que uma ação de acompanhamento contra uma pessoa ou organização, após um incidente de segurança da informação, envolver uma ação legal (civil ou criminal), evidências devem ser coletadas, armazenadas e apresentadas em conformidade com as normas de armazenamento de evidências da jurisdição ou jurisdições pertinentes.
A.14 Gestão da continuidade do negócio		
***A.14.1* Aspectos da gestão da continuidade do negócio, relativos à 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.		
A.14.1.1	Incluindo segurança da informação no processo de gestão da continuidade de negócio	*Controle* Um processo de gestão deve ser desenvolvido e mantido 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.
A.14.1.2	Continuidade de negócios e análise/avaliação de risco	*Controle* Devem ser identificados os eventos que podem causar interrupções aos processos de negócio, junto à probabilidade e impacto de tais interrupções e as conseqüências para a segurança de informação.
A.14.1.3	Desenvolvimento e implementação de planos de continuidade relativos à segurança da informação	*Controle* 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.
A.14.1.4	Estrutura do plano de continuidade do negócio	*Controle* Uma estrutura básica dos planos de continuidade do negócio deve ser mantida para assegurar que todos os planos são consistentes, para contemplar os requisitos de segurança da informação e para identificar prioridades para testes e manutenção.

A.14.1.5	Testes, manutenção e reavaliação dos planos de continuidade do negócio	*Controle* Os planos de continuidade do negócio devem ser testados e atualizados regularmente, de forma a assegurar sua permanente atualização e efetividade.
A.15 Conformidade		
A.15.1 **Conformidade com requisitos legais** *Objetivo:* Evitar violação de qualquer lei criminal ou civil, estatutos, regulamentações ou obrigações contratuais e de quaisquer requisitos de segurança da informação		
A.15.1.1	Identificação da legislação vigente	*Controle* Todos os requisitos estatutários, regulamentares e contratuais relevantes, e o enfoque da organização para atender a estes requisitos devem ser explicitamente definidos, documentados e mantidos atualizados para cada sistema de informação da organização.
A.15.1.2	Direitos de propriedade intelectual	*Controle* Procedimentos apropriados devem ser implementados para garantir a conformidade com os requisitos legislativos, regulamentares e contratuais no uso de material, em relação aos quais pode haver direitos de propriedade intelectual e sobre o uso de produtos de *software* proprietários.
A.15.1.3	Proteção de registros organizacionais	*Controle* Registros importantes devem ser protegidos contra perda, destruição e falsificação, de acordo com os requisitos regulamentares, estatutários, contratuais e do negócio.
A.15.1.4	Proteção de dados e privacidade da informação pessoal	*Controle* A privacidade e a proteção de dados devem ser asseguradas conforme exigido nas legislações relevantes, regulamentações e, se aplicável, nas cláusulas contratuais.
A.15.1.5	Prevenção de mau uso de recursos de processamento da informação	*Controle* Os usuários devem ser dissuadidos de usar os recursos de processamento da informação para propósitos não autorizados.
A.15.1.6	Regulamentação de controles de criptografia	*Controle* Controles de criptografia devem ser usados em conformidade com leis, acordos e regulamentações relevantes.
A.15.2 **Conformidade com normas e políticas de segurança da informação e conformidade técnica** *Objetivo:* Garantir conformidade dos sistemas com as políticas e normas organizacionais de segurança da informação.		
A.15.2.1	Conformidade com as políticas e normas de segurança da informação	*Controle* Os gestores devem garantir que todos os procedimentos de segurança dentro da sua área de responsabilidade sejam executados corretamente para atender à conformidade com as normas e políticas de segurança da informação.
A.15.2.2	Verificação da conformidade técnica	*Controle* Os sistemas de informação devem ser periodicamente verificados quanto à sua conformidade com as normas de segurança da informação implementadas.

A.15.3 **Considerações quanto à auditoria de sistemas de informação** *Objetivo:* Maximizar a eficácia e minimizar a interferência no processo de auditoria dos sistemas de informação.		
A.15.3.1	Controles de auditoria de sistemas de informação	*Controle* Os requisitos e atividades de auditoria envolvendo verificação nos sistemas operacionais devem ser cuidadosamente planejados e acordados para minimizar os riscos de interrupção dos processos do negócio.
A.15.3.2	Proteção de ferramentas de auditoria de sistemas de informação	*Controle* O acesso às ferramentas de auditoria de sistema de informação deve ser protegido para prevenir qualquer possibilidade de uso impróprio ou comprometimento.