GESTÃO DE SEGURANÇA DA INFORMAÇÃO (ISO 27001)

Graduação Tecnológica em Redes de Computadores.

Professor Marco Antônio Chaves Câmara

Agenda

- Introdução
  - A norma 27001
  - Por quê um SGSI certificado?
  - Como utilizar a norma
  - Escopo da Norma
  - A Base da Implantação
- Termos e Definições
- Conhecendo a Norma Básica
- Anexo A: Objetivos e Controles

INTRODUÇÃO

A Norma ISO27001

- ISO 27001: Escopo, referências, termos e definições, sistema de gestão da segurança da informação, responsabilidade da direção, auditorias internas do SGSI, revisão estratégica do SGSI, melhoria do SGSI.

- Também será útil:
  - ISO 27002 (NBR 17799): Escopo, termos e definições, estrutura, análise/ avaliação, política e segurança, organização da segurança da informação, gestão de ativos, segurança em recursos humanos, segurança física e do ambiente, gerenciamento das operações e comunicações, controle de acesso, aquisição, desenvolvimento e manutenção de sistemas, gestão de incidente de segurança da informação, gestão da continuidade do negócio, conformidade.

Por quê um SGSI certificado?

- Vantagens
  - A organização pode conquistar mais facilmente a Confiança de clientes atuais e futuros;
  - Foco na melhora contínua de processos de segurança;
  - Segurança da avaliação externa baseada em um padrão reconhecido e aceito em mais de 40 países.

A ISO27000

- Como utilizar a norma?
  - Prestar muita atenção aos detalhes da norma e suas revisões;
  - Sua rotina atual de segurança sempre será comparada com a norma. Qualquer livro, curso ou material será desprezado quando entrar em conflito com a norma;
  - Faça referência explícita aos seus itens, e prepare seus argumentos para defender quaisquer passos de sua implementação que estejam em desacordo;
  - Lembrar que, com a evolução tecnológica e novas ameaças e vulnerabilidades, muitas vezes os requerimentos precisam ser mais rigorosos e abrangentes do que aqueles recomendados pela norma.

Escopo da ISO 27001

- Dado um Sistema de Gerenciamento de Segurança da Informação (SGSI), a norma define:
  - Estabelecimento;
  - Implantação;
  - Operação;
  - Monitoramento;
  - Análise Crítica;
  - Manutenção;
  - Melhoramento.

A BASE DA IMPLANTAÇÃO

- O projeto e implementação do SGSI de uma organização depende da estrutura da organização, e pode e deve ser revisto à medida em que esta se modifica com o passar dos anos;
- Por outro lado, os requerimentos da norma são genéricos, e podem ser aplicados a qualquer tipo de empresa, independente de seu tamanho, tipo e natureza
  - A exclusão de qualquer controle precisa ser devidamente justificada, evidenciando que tal retirada não afetou a habilidade ou a responsabilidade da empresa de garantir a segurança da informação aderente aos requerimentos estabelecidos pela análise de riscos e requerimentos legais ou regulatórios.

TERMOS E DEFINIÇÕES

TERMOS E DEFINIÇÕES

- Análise de risco
  - Uso sistemático de informações visando a identificação e estimativa das fontes de risco; Confiabilidade
- Ativo
  - Qualquer elemento que tenha valor para a organização;
- Autenticidade
  - Propriedade de estar associado a uma determinada pessoa, entidade ou processo;
- Confidencialidade
  - A propriedade de não estar disponível ou acessível para pessoas, entidades ou processos não autorizados;

TERMOS E DEFINIÇÕES

- Declaração de Aplicabilidade
  - Documento apresentando os objetivos dos controles que são relevantes para o SGSI da organização;
- Disponibilidade
  - A propriedade de estar disponível e utilizável diante da demanda de uma entidade devidamente autorizada;
- Evento
  - Ocorrência identificada de um estado de rede, serviço ou sistema que indique uma possível falha da política de segurança ou falha das salvaguardas, ou mesmo uma situação até então desconhecida que pode se tornar relevante em termos de segurança;

TERMOS E DEFINIÇÕES

- Incidente
  - Evento ou série de eventos indesejados ou inesperados que provavelmente comprometerão as operações da empresa ou ameaçam a segurança da informação;
- Integridade
  - A propriedade de salvaguardar a precisão e completude dos ativos;
- Não-Repúdio
  - É a propriedade de garantir que uma pessoa ou entidade participante numa dada operação jamais possa negar essa participação;

TERMOS E DEFINIÇÕES

- Gerenciamento de Riscos
  - Atividades coordenadas visando direcionar e controlar uma organização com foco nos riscos;
- Processo
  - Qualquer atividade utilizando recursos e gerenciamento para promover a transformação de entradas em saídas;
- Responsabilização (*accountability*)
  - É a propriedade de informar eventuais ações e decisões, mesmo quando as mesmas vão de encontro à política de segurança estabelecida;

TERMOS E DEFINIÇÕES

- Segurança da Informação
  - Preservação da confidencialidade, integridade e disponibilidade da informação. Além disto, outras propriedades, como autenticidade, responsabilização, não-repúdio e confiabilidade podem também estar envolvidas;
- Tratamento de Risco
  - Descreve o processo de seleção e implementação de medidas visando modificar o risco;

CONHECENDO A NORMA BÁSICA

DEFINIÇÃO DO SGSI

- Definir o escopo e limites do SGSI
  - Levar em consideração as características da organização:
    - Localização;
    - Recursos;
    - Tecnologia;
  - Detalhar e justificar eventuais exclusões do escopo.

DEFINIÇÃO DO SGSI

- Definir a política de segurança
  - Definir os princípios que nortearão as ações relacionadas à segurança da informação;
  - Levar em consideração os requerimentos legais e contratuais, além dos marcos regulatórios associados à segurança da informação;
  - Garantir o alinhamento com o gerenciamento estratégico de riscos;
  - Estabelecer critérios para cada um dos riscos sendo avaliados;
  - Obter a aprovação da gerência.

DEFINIÇÃO DO SGSI

- Definir a estratégia de gerenciamento de riscos
  - Identificar a metodologia de avaliação de riscos mais adequada ao SGSI da organização, garantindo a produção de resultados comparáveis e que possam ser reproduzidos.
  - Definir critério para aceitação e identificação dos níveis aceitáveis de risco;

DEFINIÇÃO DO SGSI

- Identificar os riscos
  - Identificar os ativos e seus respectivos "proprietários";
  - Identificar as ameaças a estes ativos;
  - Identificar as vulnerabilidades que podem ser exploradas por estas ameaças;
  - Identificar quais os impactos que a perda de confidencialidade, integridade ou disponibilidade causarão sobre estes ativos.

DEFINIÇÃO DO SGSI

- Analisar e avaliar os riscos
  - Analisar os impactos das falhas de segurança sobre a organização;
  - Avaliar a probabilidade real de ocorrência de falhas de segurança à luz das ameaças e vulnerabilidades conhecidas, e dos controles atualmente implementados;
  - Estimar os níveis de risco;
  - Determinar se os riscos são aceitáveis ou requerem tratamento especial usando os critérios estabelecidos para a aceitação de riscos.

DEFINIÇÃO DO SGSI

- Identificar e avaliar opções de tratamento de riscos, optando por uma ou mais das seguintes estratégias:
  - Aplicação de controles apropriados;
  - Aceitar os riscos, desde que estes satisfaçam claramente as condições estipuladas para tal;
  - Implantação de estratégias que permitam evitar os riscos;
  - Transferir os riscos para terceiros, como seguradoras, fornecedores etc.

DEFINIÇÃO DO SGSI

- Selecionar objetivos e controles para o tratamento de riscos
  - Os objetivos e controles devem ser selecionados e implementados de forma a atender aos requerimentos estabelecidos pela análise de riscos;
  - O Anexo A da Norma ISO 27.001 relaciona os objetivos e controles que podem ser selecionados como adequados ao atendimento dos requerimentos estabelecidos pela análise de riscos;
  - Os objetivos e controles listados no anexo citado acima não eliminam a possibilidade de implantação de outros controles.

DEFINIÇÃO DO SGSI

- Obter aprovação da diretoria
  - Quanto aos riscos residuais
    - A gerência da organização precisa estar ciente e assumir a responsabilidade pela ausência de tratamento de riscos residuais não previstos no SGSI.
  - Para implantação e operação do SGSI
    - Apenas o comprometimento da alta direção garantirá a implantação e operação do SGSI, já que este normalmente afeta o dia-a-dia da operação da organização, além de tipicamente implicar em investimentos.

DEFINIÇÃO DO SGSI

- Preparar uma Declaração de Aplicabilidade. Esta deve incluir:
  - Os objetivos e controles selecionados, e as razões de sua seleção;
  - Os objetivos e controles atualmente implementados;
  - As justificativas para a exclusão de quaisquer objetivos e controles relacionados no Anexo I da Norma ISO 27.001 que não foram adotados. Isto garante que nenhum controle deixou de ser adotado por mero esquecimento ou falha.

IMPLANTAÇÃO E OPERAÇÃO DO SGSI

- Para implantar e operar o SGSI definido, a organização deve:
  - Formular um plano de tratamento de riscos que identifique as ações de gerenciamento apropriadas, recursos necessários, responsabilidades e prioridades;
  - Implementar um plano de ação para atingir os objetivos definidos;
  - Implementar os controles definidos, definindo um método de mensurar posteriormente a eficácia de suas implementações;
  - Definir um programa de treinamento e divulgação do SGSI;
  - Gerenciar os recursos e a operação do SGSI.

MONITORAÇÃO E ANÁLISE CRÍTICA DO SGSI

- Monitorar e rever procedimentos e controles
  - Identificar e registrar eventos e incidentes de segurança;
  - Avaliar se as atividades de segurança delegadas a pessoas ou implementadas através de recursos de tecnologia da informação estão ocorrendo como deveriam;
  - Avaliar os indicadores;
  - Avaliar se as ações resultantes de uma falha de segurança obtiveram resultado efetivo.
- Realizar auditorias periódicas do SGSI;

MONITORAÇÃO E ANÁLISE CRÍTICA DO SGSI

- Rever em intervalos planejados a avaliação de riscos e os riscos residuais, além dos níveis de risco considerados aceitáveis em função das mudanças:
  - Na organização;
  - Tecnológicas;
  - Nos objetivos e processos de negócio;
  - Nas ameaças identificadas;
  - Na eficiência dos controles adotados;
  - Em eventos externos, como na legislação ou marcos regulatórios, contratos externos, ou mesmo no ambiente social.

Melhoramento do SGSI

- As mudanças recomendadas pela análise crítica do SGSI devem provocar:
  - A implantação das melhorias identificadas;
  - A tomada de ações preventivas e corretivas visando a melhoria do SGSI. Aqui valem as experiências apreendidas tanto internamente quanto externamente, através do exemplo de outras organizações;
  - A divulgação das ações e melhoramentos para todas as partes interessadas.

Documentando o SGSI

- A documentação do SGSI deve incluir o registro das decisões de gerenciamento, assim como o registro dos resultados obtidos;
- É importante demonstrar o relacionamento dos controles selecionados com os resultados da avaliação de risco e com os processos de tratamento de riscos, além da política e objetivos do SGSI;

Documentando o SGSI

- Declaração da Política de Segurança e seus objetivos;
- Escopo do SGSI;
- Procedimentos e controles implementados;
- Descrição da metodologia de avaliação de riscos;
- Relatório da Avaliação de Riscos;
- Plano de Tratamento de Riscos;
- Procedimentos documentados do planejamento, operação e controle dos processos de Segurança da Informação, incluindo a medição da eficiência dos controles implementados;
- Registros das evidências de conformidade e operação efetiva do SGSI;
- Declaração de Aplicabilidade.

Documentando o SGSI

- Todos os documentos requeridos pelo SGSI devem ser protegidos e controlados, como em qualquer sistema normatizado. Um procedimento documentado deve ser definido para garantir que:
  - Todos os documentos serão adequadamente aprovados antes de seu uso efetivo;
  - Os documentos serão revistos ou atualizados quanto necessário, com posterior re-aprovação dos mesmos;
  - Mudanças na versão atual de um documento serão identificadas;
  - Os documentos aplicáveis estarão disponíveis em todos os pontos de uso nas suas versões relevantes;
  - Os documentos serão perfeitamente legíveis e identificáveis pelos seus usuários;
  - Documentos de fonte externa serão adequadamente identificados;
  - Os documentos terão distribuição controlada, com prevenção contra o uso de versões obsoletas.

Responsabilidade da Gerência

- A gerência deve prover evidência de seu comprometimento com o SGSI;
- Recursos necessários devem ser alocados às diversas fases do SGSI;
- Todas aqueles com responsabilidades definidas no SGSI devem estar capacitados a realizar as tarefas atribuídas;
- A gerência deve garantir a realização das auditorias periódicas do SGSI.

ANÁLISE CRÍTICA DO SGSI

- O SGSI precisa ser revisto periodicamente (no mínimo anualmente) para garantir sua adequação, compatibilidade e eficiência;
- A análise crítica deve ser feita com base nos seguintes itens:
  - Resultados das auditorias e revisões anteriores;
  - Comentários das partes interessadas;
  - Situação atual das ações preventivas e corretivas;
  - Vulnerabilidades e ameaças não previstas na avaliação de risco anterior;
  - Indicadores de eficiência;
  - Acompanhamento das ações determinadas pela última análise crítica do SGSI.

ANÁLISE CRÍTICA DO SGSI

- Como resultado da análise crítica, podem ser obtidos os seguintes resultados:
  - Melhoramento da eficiência do SGSI;
  - Atualização da Avaliação de Riscos e do Plano de Tratamento de Riscos;
  - Modificação de Procedimentos e Controles que afetam a Segurança da Informação;
  - Revisão dos Recursos necessários;
  - Melhoramento dos indicadores de eficiência dos controles.

MELHORAMENTO CONTÍNUO DO SGSI

- Ações corretivas
  - A organização precisa tomar ações para eliminar as causas de não-conformidades evitando sua reincidência. As ações precisam ser registradas e posteriormente revisadas.
- Ações preventivas
  - Analogamente, a organização também precisa tratar as não-conformidades potenciais visando evitar a sua ocorrência. Da mesma forma, as ações resultantes deste trabalho também precisam ser registradas e revisadas.

Anexo A: Objetivos e Controles

ANEXO A - OBJETIVOS E CONTROLES
A.5.1 – POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

- A.5.1.1 Documento da Política de Segurança da Informação
  - Este documento precisa ser elaborado, aprovado pela gerência, e divulgado para todos os funcionários, contratados e terceiros envolvidos no negócio da organização.
- A.5.1.2 Análise Crítica da Política de Segurança da Informação
  - A Política de Segurança da Informação precisa ser revista periodicamente, ou sempre que ocorrerem mudanças significativas.

ANEXO A - OBJETIVOS E CONTROLES

A.6.1 – ORGANIZAÇÃO DA SEGURANÇA DA INFORMAÇÃO

- A.6.1.1 Comprometimento da gerência com a Segurança da Informação
- A.6.1.2 Coordenação da Segurança da Informação
  - As atividades de Segurança da Informação devem ser coordenadas por representantes de papéis relevantes em diferentes partes da organização.
- A.6.1.3 Definição de Responsabilidades da Segurança da Informação
- A.6.1.4 Verificação prévia de novos recursos para processamento de informação
- A.6.1.5 Acordos de confidencialidade

ANEXO A - OBJETIVOS E CONTROLES

A.6.1 – ORGANIZAÇÃO DA SEGURANÇA DA INFORMAÇÃO

- A.6.1.6 Contatos com autoridades
  - Manter contatos com autoridades policiais, órgãos regulatórios, provedores de telecomunicação e conteúdo de forma a garantir ações apropriadas e rápidas em caso de incidentes de segurança.
- A.6.1.7 Contatos com Grupos de Interesse
  - Manter contatos com grupos de interesse, especialistas e associações profissionais relacionadas à segurança da informação.
- A.6.1.8 Revisão Independente da Segurança da Informação
  - A abordagem de segurança da informação e sua implementação (objetivos, controles, políticas, processos e procedimentos) devem ser submetidos a revisões externas periódicas, ou quando ocorrerem mudanças significativas.

ANEXO A - OBJETIVOS E CONTROLES
A.6.2 – TERCEIROS

- A.6.2.1 Identificação de Riscos relacionados a terceiros
- A.6.2.2 Levar em consideração a Segurança no relacionamento com clientes
  - Todos os requerimentos de segurança devem ser avaliados antes de oferecer acesso dos clientes às informações e ativos da organização.
- A.6.2.3 Levar em consideração a Segurança da Informação no relacionamento com parceiros comerciais e prestadores de serviços
  - Todos os requerimentos de segurança devem ser avaliados no relacionamento com terceiros que se envolvam no acesso, processamento, comunicação ou gerenciamento de ativos.

ANEXO A - OBJETIVOS E CONTROLES
A.7.1 – RESPONSABILIDADE SOBRE OS ATIVOS

- A.7.1.1 Inventário dos Ativos
- A.7.1.2 Propriedade sobre os Ativos
  - Todos as informações e ativos associados a recursos de processamento de informações devem ser de "propriedade" de uma parte determinada da organização.
- A.7.1.3 Utilização adequada dos Ativos
  - Devem ser identificadas, documentadas e implementadas regras adequadas para o uso de informações e ativos associados a recursos de processamento de informações.

ANEXO A - OBJETIVOS E CONTROLES
A.7.2 – CLASSIFICAÇÃO DA INFORMAÇÃO

- A.7.2.1 Parâmetros de Classificação
  - As informações devem ser classificadas em termos de seu valor, requerimentos legais, sensibilidade e o quanto a mesma é crítica para a organização.
- A.7.2.2 Identificação e Manipulação das informações
  - Deve ser estabelecido e implementado um conjunto de procedimentos para identificação e manipulação de informações de acordo com a classificação adotada pela organização.

ANEXO A - OBJETIVOS E CONTROLES
A.8.1 – SEGURANÇA E RH (ANTES DA CONTRATAÇÃO)

- A.8.1.1 Cargos e Responsabilidades
  - Os cargos e responsabilidades de segurança dos funcionários, contratados e terceiros precisam estar definidos e documentados de acordo com a Política de Segurança de Informação da Empresa.
- A.8.1.2 Triagem
  - Todos os candidatos à contratação e terceiros devem ser verificados de acordo com os requerimentos legais, regulamentações e ética profissional, conforme os requerimentos do negócio, estabelecendo a classificação das informações que os mesmos terão acesso, e os riscos percebidos.

ANEXO A - OBJETIVOS E CONTROLES
A.8.1 – SEGURANÇA E RH (ANTES DA CONTRATAÇÃO)

- A.8.1.3 Termos e Condições de Contratação
  - Os contratos estabelecidos com os funcionários, contratados e terceiros devem estabelecer suas responsabilidades perante a organização quanto à segurança da informação.

ANEXO A - OBJETIVOS E CONTROLES
A.8.2 – SEGURANÇA E RH (DURANTE A VIGÊNCIA)

- A.8.2.1 Responsabilidades da Gerência
  - A gerência deve requerer que os funcionários, contratados e terceiros obedeçam às políticas e procedimentos de segurança estabelecidos pela organização.
- A.8.2.2 Divulgação e Treinamento
  - Todos os funcionários da organização, e quando relevante, também os contratados e terceiros, devem receber treinamentos regulares acerca das políticas e procedimentos de segurança relevantes para as suas funções na organização.
- A.8.2.3 Processos Disciplinares
  - Deve ser estabelecido formalmente um processo disciplinar para funcionários que provocarem falhas de segurança.

ANEXO A - OBJETIVOS E CONTROLES
A.8.3 – SEGURANÇA E RH (TÉRMINO CONTRATAÇÃO)

- A.8.3.1 Responsabilidade pelo Término
- A.8.3.2 Devolução de Ativos
  - Todos os funcionários, contratados e terceiros devem devolver todos os ativos da organização que estiverem em seu poder logo após o término de seus respectivos contratos.
- A.8.3.3 Remoção dos Direitos de Acesso

ANEXO A - OBJETIVOS E CONTROLES
A.9.1 – ÁREAS SEGURAS

- A.9.1.1 Perímetro Físico de Segurança
  - Devem existir barreiras (paredes, portas com controle de acesso etc) para proteger áreas que contém recursos de processamento de informação.
- A.9.1.2 Controle Físico de Acesso
  - As áreas seguras devem ser protegidas de forma a permitir o acesso apenas de pessoas autorizadas.
- A.9.1.3 Segurança Física de Escritórios, Salas e Instalações
- A.9.1.4 Proteção contra ameaças externas e ambientais
  - Devem ser estabelecidas proteções contra fogo, alagamento, terremotos, explosões, desordem civil e outras formas de desastres naturais ou provocados pelo homem.

ANEXO A - OBJETIVOS E CONTROLES
A.9.1 – ÁREAS SEGURAS

- A.9.1.5 Trabalho em áreas seguras
  - Deve ser estabelecida segurança física e procedimentos para o trabalho em áreas seguras.
- A.9.1.6 Áreas públicas, de entregas e carga/ descarga
  - As áreas onde pessoas não autorizadas podem ter acesso devem ser controladas e preferencialmente isoladas das instalações de processamento de informações para evitar o acesso não autorizado.

ANEXO A - OBJETIVOS E CONTROLES
A.9.2 – SEGURANÇA DE EQUIPAMENTOS

- A.9.2.1 Posicionamento e Segurança
  - A localização de um equipamento deve ser definida de forma a minimizar o acesso não autorizado à área de trabalho (acesso desnecessário, ângulo de visão etc).
- A.9.2.2 Recursos de Suporte
  - Os equipamentos devem ser protegidos de falhas de alimentação elétrica e outras interrupções que possam ocorrer com os recursos de suporte (refrigeração, por exemplo).
- A.9.2.3 Segurança do Cabeamento
  - Cabos de alimentação elétrica e telecomunicações que suportam serviços de informação devem ser protegidos contra danos e interrupções.

ANEXO A - OBJETIVOS E CONTROLES
A.9.2 – SEGURANÇA DE EQUIPAMENTOS

- A.9.2.4 Manutenção
  - Os equipamentos devem sofrer manutenção preventiva adequada de forma a não afetar sua disponibilidade e integridade.
- A.9.2.5 Segurança de Equipamentos Externos
  - Procedimentos de segurança devem ser aplicados aos equipamentos submetidos à operação fora das instalações da organização.
- A.9.2.6 Descarte ou Reciclagem segura
  - Todos os equipamentos que contém mídias de armazenamento devem ser devidamente checados antes de descartados, para garantir a remoção de dados sensíveis e licenças de software.

ANEXO A - OBJETIVOS E CONTROLES
A.9.2 – SEGURANÇA DE EQUIPAMENTOS

- A.9.2.7 Autorização de Remoção
  - Os equipamentos, informações ou softwares não devem sair da organização sem autorização prévia.

ANEXO A - OBJETIVOS E CONTROLES
A.10.1 – PROC.OPERACIONAIS E RESPONSABILIDADES

- A.10.1.1 Documentação de Proc.Operacionais
  - Todos os procedimentos operacionais devem ser documentados e estar disponíveis para todos os usuários que os utilizem.
- A.10.1.2 Gerenciamento de Modificações
  - Modificações no processamento de informações devem ser devidamente controladas.
- A.10.1.3 Segregação de atividades e responsabilidades por grupo
  - Atividades e áreas de responsabilidade de grupos específicos de usuários devem ser devidamente segregadas para reduzir a chance de modificações não intencionais ou não autorizadas, ou mesmo uso incorreto dos ativos.
- A.10.1.4 Separação das instalações de desenvolvimento, teste e operação

ANEXO A - OBJETIVOS E CONTROLES
A.10.2 – GERENCIAMENTO DE TERCEIROS

- A.10.2.1 Entrega de Serviços
  - Devem ser garantidos que todos os controles de segurança, definições de serviço e níveis de atendimento definidos no contrato com o terceiro sejam devidamente implementados, operados e mantidos pelo mesmo.
- A.10.2.2 Monitoramento
  - Os serviços, relatórios e registros oferecidos pelo terceiro devem ser regularmente monitorados e revisados. Auditorias também devem ser realizadas regularmente.
- A.10.2.3 Mudanças nos serviços de terceiros
  - Mudanças na prestação de serviços, incluindo a manutenção e o melhoramento das políticas de segurança da informação, procedimentos e controles devem ser acompanhadas levando-se em consideração o quão críticos são os processos afetados e a re-atribuição de riscos associados.

ANEXO A - OBJETIVOS E CONTROLES
A.10.3 – PLANEJ. E HOMOLOGAÇÃO DE SISTEMAS

- A.10.3.1 Gerenciamento de Capacidade
  - O uso de recursos deve ser monitorado e ajustado. Devem ser feitas projeções de requerimentos futuros de capacidade visando garantir a performance requerida pelo sistema.
- A.10.3.2 Homologação
  - Devem ser estabelecidos critérios de homologação para novos sistemas de processamento de informação, atualizações e novas versões, envolvendo testes adequados.

ANEXO A - OBJETIVOS E CONTROLES
A.10.4 – CÓDIGOS MALICIOSOS E MÓVEIS

- A.10.4.1 Controles contra códigos maliciosos
  - Devem ser implementados controles para detecção, prevenção e recuperação associada a códigos maliciosos. Deve ser realizado também o treinamento dos usuários para evitar a ocorrência de eventos e incidentes.
- A.10.4.2 Controles contra códigos móveis
  - Quando o uso de códigos móveis (por exemplo *scripts*, *applets*, Flash e macros) for permitido, a configuração dos sistemas deve ser estabelecida de forma que este código opere de acordo com a política de segurança estabelecida. Códigos móveis não autorizados devem ter sua execução bloqueada.

ANEXO A - OBJETIVOS E CONTROLES
A.10.5 – BACK-UP

- A.10.5.1 Back-Up das Informações
  - Cópias de back-up das informações e softwares devem ser realizadas e testadas regularmente de acordo com o estabelecido na política acordada de back-up.

ANEXO A - OBJETIVOS E CONTROLES
A.10.6 – GERÊNCIA DE SEGURANÇA DE REDE

- A.10.6.1 Controles sobre a rede
  - As redes devem ser devidamente gerenciadas e controladas para proteção contra ameaças, e para manter a segurança para os sistemas e aplicações que a utilizam, e também para as informações que por ela transitam.
- A.10.6.2 Segurança dos Serviços de Rede
  - Recursos de segurança, níveis de serviço, e requerimentos de gerenciamento de todos os serviços de rede devem ser devidamente identificados e claramente incluídos na contração de serviços de rede, independente destes serviços serem prestados internamente ou por terceiros.

ANEXO A - OBJETIVOS E CONTROLES
A.10.7 – MANIPULAÇÃO DE MÍDIAS

- A.10.7.1 Gerenciamento de Mídias removíveis
  - Devem existir procedimentos para o gerenciamento de mídias removíveis.
- A.10.7.2 Descarte de Mídia
  - As mídias devem ser descartadas de forma segura quando não mais forem necessárias, seguindo procedimentos formais.
- A.10.7.3 Manipulação de Informações
  - Devem ser estabelecidos procedimentos para a manipulação e armazenamento de informações para evitar o uso inadequado ou exposição não autorizada.
- A.10.7.4 Segurança da Documentação do Sistema
  - A documentação dos sistemas deve protegida contra o acesso não autorizado.

ANEXO A - OBJETIVOS E CONTROLES
A.10.8 – TROCA DE INFORMAÇÃO

- A.10.8.1 Política e Procedimentos
  - Devem ser definida uma política e procedimentos para o controle da troca de informações sobre todos os tipos de recursos de comunicação.
- A.10.8.2 Acordo para Troca de Informações
  - Devem ser estabelecidos acordos formais para a troca de informações e softwares entre a organização e terceiros.
- A.10.8.3 Proteção de Mídia em trânsito
  - Mídias contendo informações devem ser protegidas contra o acesso ou uso não autorizado e corrupção de seu conteúdo durante o transporte fora dos limites físicos da organização.
- A.10.8.4 Proteção de mensagens eletrônicas
- A.10.8.5 Proteção na conexão entre sistemas de informação

ANEXO A - OBJETIVOS E CONTROLES
A.10.9 – SERVIÇOS DE COMÉRCIO ELETRÔNICO

- A.10.9.1 Comércio Eletrônico
  - Informações envolvidas em comércio eletrônico enviadas através de redes públicas devem ser protegidas de atividades fraudulentas, disputas comerciais, modificações e exposição não autorizadas.
- A.10.9.2 Transações On-Line
  - As informações envolvidas em transações on-line devem ser protegidas contra falhas na transmissão, rotas indevidas, alteração, duplicação, re-envio e exposição não autorizadas.
- A.10.9.3 Publicação e Publicidade
  - Informações disponíveis para publicação devem ser protegidas contra alterações não autorizadas.

ANEXO A - OBJETIVOS E CONTROLES
A.10.10 – MONITORAÇÃO DO PROCESSAMENTO

- A.10.10.1 Registro de Auditoria
  - Devem ser gerados e preservados, durante um período determinado em procedimento formal, registros das atividades dos usuários, exceções ocorridas e eventos.
- A.10.10.2 Monitoramento de Uso
  - Devem ser estabelecidos procedimentos que permitam o monitoramento dos recursos de processamento de informações, cujos resultados devem ser revistos regularmente.
- A.10.10.3 Proteção dos registros
  - Os registros de auditoria devem ser protegidos contra alterações ou acessos não autorizados.
- A.10.10.4 Registro das atividades de operação e administração

ANEXO A - OBJETIVOS E CONTROLES
A.10.10 – MONITORAÇÃO DO PROCESSAMENTO

- A.10.10.5 Registro de Falhas
  - Todas as falhas devem ser registradas e analisadas. Ações adequadas devem ser tomadas com base nesta análise.
- A.10.10.6 Sincronização de Relógios
  - Os relógios de todos os sistemas de processamento de informações relevantes devem devidamente sincronizados com uma fonte confiável de horário.

ANEXO A - OBJETIVOS E CONTROLES
A.11.1 – CONTROLE DE ACESSO - REQUERIMENTO

- A.11.1.1 Política de Controle de Acesso
  - Uma política de controle de acesso deve ser estabelecida, documentada e revista com base nos requerimentos de segurança e de negócio da organização.

ANEXO A - OBJETIVOS E CONTROLES
A.11.2 – CONTROLE ACESSO – GERÊNCIA USUÁRIO

- A.11.2.1 Registro do Usuários
  - Deve existir um processo formal de registro e cancelamento de registro dos usuários que determine os direitos de acesso aos sistemas de informação e serviços.
- A.11.2.2 Gerenciamento de Privilégios
  - A alocação e uso de privilégios deve ser restrita e controlada.
- A.11.2.3 Gerenciamento de Senhas
  - A atribuição de senhas de acesso deve ser controlada através de um processo formal de gerenciamento.
- A.11.2.4 Revisão de Direitos de Acesso
  - A gerência deve estabelecer um processo de revisão periódica dos direitos de acesso dos usuários.

ANEXO A - OBJETIVOS E CONTROLES
A.11.3 – CONTROLE ACESSO – RESP. DO USUÁRIO

- A.11.3.1 Uso de Senhas
  - Deve existir um processo formal de registro e cancelamento de registro dos usuários que determine os direitos de acesso aos sistemas de informação e serviços.
- A.11.3.2 Equipamentos desassistidos
  - Os usuários devem garantir a proteção de seus equipamentos contra o acesso não autorizado quando se afastarem do mesmo.
- A.11.3.3 Política de mesa e tela “limpas”
  - Os usuários devem promover uma política que garanta a ausência de papéis e mídias removíveis sobre suas mesas, assim como telas de computador ativas, sempre que precisarem se afastar de seus equipamentos.

ANEXO A - OBJETIVOS E CONTROLES
A.11.4 – CONTROLE ACESSO – ACESSO À REDE

- A.11.4.1 Política de Uso dos Serviços de Rede
  - Os usuários só devem ter acesso aos serviços para os quais foram expressamente autorizados.
- A.11.4.2 Autenticação de Usuários Remotos
- A.11.4.3 Identificação dos equipamentos
  - A identificação automática de equipamentos deve ser considerada como meio de autenticação de conexões de determinados locais e equipamentos.
- A.11.4.4 Proteção de acesso remoto a portas de configuração e diagnóstico
  - O acesso lógico e físico a portas de configuração e diagnóstico deve ser controlado.

ANEXO A - OBJETIVOS E CONTROLES
A.11.4 – CONTROLE ACESSO – ACESSO À REDE

- A.11.4.5 Segregação de Grupos na Rede
  - Diferentes grupos de serviços, usuários e sistemas de informação devem ser segregados na rede.
- A.11.4.6 Controle da Conexão à Rede
  - Para redes compartilhadas, especialmente para aquelas que ultrapassam os limites da organização, o acesso de usuários à rede deve ser restrito, de acordo com a política de controle de acesso da organização, e com os requerimentos das aplicações de negócio.
- A.11.4.7 Controle das Rotas de Tráfego de Informações

ANEXO A - OBJETIVOS E CONTROLES
A.11.5 – CONTROLE ACESSO – SIST. OPERACIONAIS

- A.11.5.1 Procedimentos seguros de *log-on*
- A.11.5.2 Identificação e Autenticação de Usuários
  - Todos os usuários devem possuir uma identificação única, de uso pessoal e intransferível. Deve ser utilizada também uma técnica adequada para autenticar o usuário.
- A.11.5.3 Gerenciamento de Senhas
  - Os sistemas de gerenciamento de senhas devem ser interativos e garantir o uso de senhas de alta qualidade.
- A.11.5.4 Restrição ao uso de Utilitários
  - O uso de utilitários capazes de evitar controles de aplicação e sistemas deve ser restrito e extremamente controlado.

ANEXO A - OBJETIVOS E CONTROLES
A.11.5 – CONTROLE ACESSO – SIST. OPERACIONAIS

- A.11.5.5 *Time-Out*
  - Sessões inativas devem ser desativadas depois de um determinado período de inatividade.
- A.11.5.6 Limitação de Tempo de Conexão
  - Pode ser implementado um controle de tempo máximo de conexão como uma segurança adicional para aplicações de alto risco.

ANEXO A - OBJETIVOS E CONTROLES
A.11.6 – CONTROLE ACESSO – SIST. APLICATIVOS

- A.11.6.1 Restrição de Acesso a Sistemas Aplicativos
  - O acesso a informações e funções de um sistema aplicativo pelo pessoal de suporte deve ser restrito e deve ocorrer em conformidade com a política de controle de acesso.
- A.11.6.2 Isolamento de Sistemas Sensíveis
  - É recomendável que sistemas sensíveis sejam instalados em um ambiente computacional isolado e dedicado.

ANEXO A - OBJETIVOS E CONTROLES
A.11.7 – CONTR.ACESSO – COMP.MÓVEL E REMOTA

- A.11.7.1 Comunicação e Computação Remota
  - Deve ser estabelecida uma política formal com medidas de segurança apropriadas para proteção contra os riscos derivados do uso de recursos de comunicação e computação remota.
- A.11.7.2 Trabalho em Casa (*Teleworking*)
  - Devem ser estabelecidos procedimentos, planos operacionais e políticas específicas para o trabalho em casa.

ANEXO A - OBJETIVOS E CONTROLES

A.12.1 – ANÁLISE E ESPECIFICAÇÃO DE REQUERIMENTOS DE SEGURANÇA PARA SISTEMAS DE INFORMAÇÃO

- A.12.1.1 Análise e Especificação
  - Os requerimentos para novos sistemas de informação, ou para o melhoramento de sistemas já existentes devem incluir os requerimentos de segurança.

ANEXO A - OBJETIVOS E CONTROLES
A.12.2 – PROCESS. CORRETO DE INFORMAÇÕES

- A.11.2.1 Validação de entrada de dados
- A.11.2.2 Validação interna de resultados
  - As aplicações devem incluir a validação de dados visando detectar a corrupção de informações provocada por eventuais erros ou atos indevidos.
- A.11.2.3 Integridade de Mensagens
  - Os sistemas devem garantir a autenticidade e integridade de mensagens.
- A.11.2.4 Validação de saída de dados
  - As saídas de dados de uma aplicação devem ser validadas para garantir que o processamento das informações armazenadas foi correto e apropriado aos resultados esperados.

ANEXO A - OBJETIVOS E CONTROLES
A.12.3 – CRIPTOGRAFIA

- A.12.3.1 Política de uso de controles critografados
- A.12.3.2 Gerenciamento de Chaves
  - Uma política de gerenciamento de chaves pode ser implementada para suporte ao uso de técnicas de criptografia pela organização.

ANEXO A - OBJETIVOS E CONTROLES
A.12.4 – SEGURANÇA DOS ARQUIVOS DE SISTEMA

- A.12.4.1 Controle de Instalação de Softwares
- A.12.4.2 Proteção de Dados de teste do Sistema
  - Os dados de teste devem ser cuidadosamente selecionados, protegidos e controlados.
- A.12.4.3 Acesso ao Código Fonte
  - O acesso ao código fonte deve ser restrito.

ANEXO A - OBJETIVOS E CONTROLES
A.12.5 – DESENVOLV. E SUPORTE ÀS APLICAÇÕES

- A.12.5.1 Procedimentos de Controle de Mudanças
- A.12.5.2 Revisão técnica das aplicações
  - Quando ocorrer mudanças nos sistemas operacionais, as aplicações críticas devem ser revistas e testadas para garantir que não haverá nenhum impacto às operações ou segurança da organização.
- A.12.5.3 Restrições à alteração de Pacotes de Software
  - As modificações em pacotes de software deve ser desencorajada, devendo-se limitar àquelas mudanças necessárias, e precisam ser estritamente controladas.

ANEXO A - OBJETIVOS E CONTROLES
A.12.5 – DESENVOLV. E SUPORTE ÀS APLICAÇÕES

- A.12.5.4 Vazamento de Informações
  - As oportunidade de vazamento de informações precisam ser evitadas.
- A.12.5.5 Desenvolvimento externo de aplicações
  - O desenvolvimento externo de aplicações deve ser supervisionado e monitorado pela organização.

ANEXO A - OBJETIVOS E CONTROLES
A.12.6 – GERENC. DE VULNERABILIDADES TÉCNICAS

- A.12.6.1 Controle de Vulnerabilidades
  - Devem ser obtidas periodicamente informações atualizadas sobre vulnerabilidades de sistemas de informação em uso. Deve-se avaliar a exposição da organização aos riscos indicados, e devem ser tomadas as medidas apropriadas para eliminar tal risco.

ANEXO A - OBJETIVOS E CONTROLES
A.13.1 – RELATANDO EVENTOS E FRAGILIDADES

- A.13.1.1 Relatar eventos
  - Os eventos de segurança da informação devem ser relatados através dos canais de gerenciamento apropriados com a maior agilidade possível.
- A.13.1.2 Relatar fragilidades
  - Todos os empregados, contratados e terceiros devem relatar quaisquer fragilidade suspeita ou mesmo observada nos sistemas e serviços.

ANEXO A - OBJETIVOS E CONTROLES
A.13.2 – INCIDENTES E MELHORAMENTOS

- A.13.2.1 Responsabilidades e Procedimentos
  - Devem ser estabelecidas responsabilidades e procedimentos que garantam uma resposta rápida e eficiente aos incidentes de segurança.
- A.13.2.2 Aprendendo a partir dos incidentes
  - Devem ser estabelecidos mecanismos que permitam quantificar e monitorar os tipos, volumes e custos derivados dos incidentes.
- A.13.2.3 Coleta de evidências
  - Devem ser coletadas e armazenadas evidências do incidente de segurança que permitam inclusive a apresentação de ações judiciais contra os responsáveis pela falha.

ANEXO A - OBJETIVOS E CONTROLES
A.14.1 – CONTINUIDADE DE NEGÓCIOS

- A.14.1.1 Incluir a segurança da informação nos processos de continuidade de negócio
- A.14.1.2 Avaliação de Riscos
  - Os eventos que podem provocar a interrupção dos processos de negócio devem ser identificados, assim como a probabilidade e o impacto destas interrupções e suas conseqüências para a segurança da informação.
- A.14.1.3 Desenvolver e implementar planos de continuidade de negócios envolvendo sistemas de informação
  - Planos devem prever a disponibilidade de informações necessárias dentro de um período de tempo aceitável.

ANEXO A - OBJETIVOS E CONTROLES
A.14.1 – CONTINUIDADE DE NEGÓCIOS

- A.14.1.4 Conjunto de Planos de Continuidade
  - Um único conjunto de planos de continuidade de negócios deve ser elaborado visando a consistência entre os mesmos e definição adequada de prioridades para teste e manutenção.
- A.14.1.5 Teste, Manutenção e Atualização dos Planos de Continuidade de Negócios
  - Os planos de continuidade de negócios devem ser testados e atualizados regularmente visando a confirmação de que os mesmos permanecem atualizados e efetivos.

ANEXO A - OBJETIVOS E CONTROLES
A.15.1 – CONFORMIDADE COM REQUISITOS LEGAIS

- A.15.1.1 Identificação de Legislação Aplicável
  - Todos os requerimentos legais, contratuais e regulatórios precisam explicitamente definidos, documentados e mantidos atualizados.
- A.15.1.2 Direitos de Propriedade Intelectual
- A.15.1.3 Proteção de registros organizacionais
  - Os registros importantes da organização devem ser protegidos da perda, destruição e falsificação, de acordo com a legislação, contratos e aspectos regulatórios.
- A.15.1.4 Proteção dos dados pessoais e garantia de privacidade

ANEXO A - OBJETIVOS E CONTROLES
A.15.1 – CONFORMIDADE COM REQUISITOS LEGAIS

- A.15.1.5 Proteção contra o uso não autorizado dos sistemas de processamento de informações.
- A.15.1.6 Obediência aos regulamentos de uso de recursos de criptografia.

ANEXO A - OBJETIVOS E CONTROLES
A.15.2 – CONFORM. REQUISITOS DE SEGURANÇA

- A.15.2.1 Garantir a conformidade com as normas e padrões de segurança aplicáveis.
- A.15.2.2 Verificação de conformidade técnica
  - Os sistemas de informação devem ser regularmente verificados quanto à conformidade com os padrões de implementação de segurança.

ANEXO A - OBJETIVOS E CONTROLES
A.15.3 – CONSIDERAÇÕES SOBRE A AUDITORIA

- A.15.3.1 Controle sobre a Auditoria de Sistemas
  - As atividades e requerimentos de auditoria que envolvam a verificação de sistemas devem ser cuidadosamente planejadas e negociadas de forma a minimizar o risco de impacto sobre os processos de negócio.
- A.15.3.2 Proteção das ferramentas de auditoria dos Sistemas de Informação.