Curso preparatório oficial para os exames das certificações Information Security Management Foundation (ISO/IEC 27001) e Information Security Controls Foundation (ISO/IEC 27002)

[Overview]

Conteúdo

- Sobre a ISO/IEC 27001
- Principais termos e definições relacionados com segurança da informação
- Principais termos e definições relacionados com Sistema de Gestão
- Sobre a ISO/IEC 27001
  - Contexto da organização
  - Liderança
  - Política
  - Planejamento
  - Apoio
  - Operação
  - Avaliação do desempenho
  - Melhoria

Conteúdo

- Sobre a ISO/IEC 27002
- Escopo
- Estrutura da norma ISO/IEC 27002
- Políticas de segurança da informação
- Organização da segurança da informação
- Segurança em recursos humanos
- Gestão de ativos
- Controle de Acesso
- Criptografia
- Segurança física e do ambiente
- Segurança nas operações
- Segurança nas comunicações
- Aquisição, desenvolvimento e manutenção de sistemas
- Relacionamento na cadeia de suprimento
- Gestão de incidentes de segurança da informação
- Aspectos da segurança da informação na gestão da continuidade do negócio
- Conformidade

Information Security Management Foundation (ISO/IEC 27001)

Normas

- **Normas**
  - Normas são documentos estabelecidos por consenso e aprovado por um organismo reconhecido, que fornece, para uso comum e repetitivo, regras, diretrizes ou características para atividades ou seus resultados, visando a obtenção de um grau ótimo de ordenação em um dado contexto.

- **Normas da família ISO IEC 27000**
  - As normas da família ISO/IEC 27000 são normas internacionais que apresentam os requisitos necessários para a implementação de um Sistema de Gestão da Segurança da Informação (SGSI) em qualquer organização por meio do estabelecimento de políticas de segurança, controles e gerenciamento de risco.

Sobre a ISO/IEC 27001

- A norma ISO/IEC 27001 especifica os **requisitos** para **estabelecer, implementar, manter e melhorar continuamente** um **sistema de gestão da segurança da informação** dentro do contexto da organização.
- Os requisitos definidos na norma são **genéricos** e são aplicáveis a **todas** as organizações, independentemente do tipo, tamanho ou natureza.
- Para os efeitos desta norma, aplicam-se os termos e definições apresentados na **ISO/IEC 27000** (visão geral e o vocabulário).

Principais termos e definições relacionados com segurança da informação (ISO/IEC 27000)

- **Ativo**
  - Algo que tenha valor para a organização e que, portanto, requer proteção.
  - Ativos primários
    - Processos e atividades de negócio
    - Informação
  - Ativos de suporte e infraestrutura
    - Hardware e software
    - Rede
    - Recursos Humanos
    - Instalações físicas

Principais termos e definições relacionados com segurança da informação (ISO/IEC 27000)

- **Ameaça**
  - Causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização.
  - Ameaças podem ser de origem natural ou humana e podem ser acidentais ou intencionais.
  - Convém que tanto as fontes de ameaças acidentais, quanto as intencionais, sejam devidamente identificadas.
  - Exemplos de ameaças
    - Acesso não autorizado
    - Espionagem industrial
    - Ações de hackers
    - Fraude
    - Roubo de documentos confidenciais
    - Enchente
    - Incêndio, etc...

Principais termos e definições relacionados com segurança da informação (ISO/IEC 27000)

- **Incidente de Segurança da Informação e Privacidade**
  - Um ou mais eventos de segurança da informação e privacidade indesejados ou inesperados, que tenham uma grande probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação.
- **Danos**
  - São as consequências de um incidente. Os danos podem ser diretos ou indiretos.
    - **Danos diretos** – são consequências diretas do incidente.
      - Exemplo: furto de um veículo.
    - **Danos indiretos** – são consequências indiretas do incidente.
      - Exemplo: após o furto do veículo, a pessoa perder compromissos.
- **Impacto**
  - Mudança adversa no nível obtido dos objetivos do negócio.

Principais termos e definições relacionados com segurança da informação (ISO/IEC 27000)

- **Segurança da Informação e privacidade**
  - Preservação da confidencialidade, integridade e disponibilidade da informação.
- **Confidencialidade**
  - Propriedade de que a informação não esteja disponível ou revelada a indivíduos, entidades ou processos não autorizados.
- **Integridade**
  - Propriedade da exatidão e completeza de ativos.
- **Disponibilidade**
  - Propriedade de estar acessível e utilizável sob demanda, por uma entidade autorizada.

Principais termos e definições relacionados com segurança da informação (ISO/IEC 27000)

- **Vulnerabilidade**
  - Fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças.
- **Risco de Segurança da Informação e Privacidade**
  - Potencial de que ameaças possam explorar vulnerabilidades de um ativo da informação ou grupo de ativos de informação, causando assim dano para a organização.
- **Risco Residual**
  - Risco remanescente após o tratamento do risco.
- **Tratamento do Risco**
  - Processo para modificar um risco.
- **Controle**
  - Medida que está modificando o risco.

Principais termos e definições relacionados com segurança da informação (ISO/IEC 27000)

- **Need to know**
  - Conceito que define que uma pessoa só precisa acessar os sistemas necessários para realizar a sua atividade.

- **Single Sign On (SSO)**
  - Mecanismo pelo qual uma única ação de autenticação do usuário pode permitir que o mesmo acesse vários ambientes, sistemas e aplicações.

- **Tokens**
  - Dispositivos físicos geradores aleatórios de código para uso como forma de autenticação em sistemas.

Principais termos e definições relacionados com Sistema de Gestão

- **Competência**
  - Capacidade de aplicar conhecimento e habilidades para atingir resultados pretendidos.
- **Melhoria Contínua**
  - Atividade recorrente para melhorar o desempenho
- **Alta direção**
  - Pessoa ou grupo de pessoas que dirigem e controlam uma organização no mais alto nível.
- **Ação corretiva**
  - Ação para eliminar a causa de uma não conformidade para prevenir a repetição.
- **Informação documentada**
  - Informação requerida para ser controlada e mantida por uma organização e o meio no qual ela está contida.
- **Parte interessada**
  - Pessoa ou organização que pode afetar, ser afetada ou perceber-se afetada por uma decisão ou atividade.

Principais termos e definições relacionados com Sistema de Gestão

- **Política**
  - Intenções e direção de uma organização formalmente expressa pela sua alta direção.
- **Análise crítica**
  - Atividade realizada para determinar a pertinência, adequação e eficácia do que está sendo examinado para alcançar os objetivos estabelecidos.
- **Auditoria**
  - Processo sistemático, documentado e independente para obter evidência objetiva e avaliá-la objetivamente para determinar a extensão na qual os critérios de auditoria são atendidos.
- **Requisito**
  - Necessidade ou expectativa que é expressa, geralmente, de forma implícita ou obrigatória.
- **Conformidade**
  - Atendimento a um requisito.
- **Não conformidade**
  - Não atendimento a um requisito.

Contexto da organização

- **Entendendo a organização e seu contexto**
  - A organização deve determinar as questões **internas e externas** que são relevantes para o seu **propósito** e que afetam sua capacidade para alcançar os resultados pretendidos do seu sistema de gestão da segurança da informação.

- **Entendendo as necessidades e as expectativas das partes interessadas**
  - A organização deve determinar:
    - a) as **partes interessadas** que são relevantes para o sistema de gestão da segurança da informação; e
    - b) os **requisitos** dessas partes interessadas relevantes para a segurança da informação.
      - Os requisitos das partes interessadas podem incluir **requisitos legais** e **regulamentares**, bem como **obrigações contratuais**.

- **Sistema de gestão da segurança da informação**
  - A organização deve **estabelecer, implementar, manter e continuamente melhorar** um **sistema de gestão da segurança da informação**, de acordo com os requisitos da norma.

Liderança

- **Liderança e comprometimento**
  - A Alta Direção deve demonstrar sua **liderança e comprometimento** em relação ao **sistema de gestão da segurança da informação**:
    - assegurando que a **política de segurança da informação** e os objetivos de segurança da informação estão estabelecidos e são compatíveis com a direção estratégica da organização;
    - assegurando que os **recursos necessários** para o sistema de gestão da segurança da informação estão disponíveis;
    - **comunicando** a importância de uma gestão eficaz da segurança da informação e da conformidade com os requisitos do sistema de gestão da segurança da informação; e promovendo a **melhoria continua.**

Política

- A Alta Direção deve **estabelecer uma política de segurança da informação** que:
  - a) seja **apropriada ao propósito** da organização;
  - b) inclua os **objetivos de segurança da informação**;
  - c) inclua o **comprometimento** em satisfazer os **requisitos** aplicáveis, relacionados com a segurança da informação;
  - d) inclua o **comprometimento** com a **melhoria contínua** do SGSI;

- A política de segurança da informação deve:
  - a) estar **disponível como informação documentada**;
  - b) ser **comunicada** dentro da organização; e
  - c) estar **disponível para as partes interessadas**, conforme apropriado.

- **Autoridades, responsabilidades e papéis organizacionais**
  - A Alta Direção deve assegurar que as **responsabilidades e autoridades** dos papéis relevantes para a segurança da informação sejam **atribuídos e comunicados**.

Planejamento

- **Ações para contemplar riscos e oportunidades**
- **Geral**
  - A organização deve determinar os **riscos e oportunidades** que precisam ser consideradas para assegurar que o SGSI possa alcançar seus resultados pretendidos.

- **Avaliação de riscos de segurança da informação**
  - A organização deve definir e aplicar um **processo de avaliação de riscos de segurança da informação**.

- **Tratamento de riscos de segurança da informação.**
  - A organização deve definir e aplicar um **processo de tratamento dos riscos de segurança da informação.**

Apoio

- **Recursos**
  - A organização deve determinar e prover **recursos necessários** para o estabelecimento, implementação, manutenção e melhoria contínua do sistema de gestão da segurança da informação.
- **Competência**
  - A organização deve:
    - **determinar** a **competência necessária** das pessoas que realizam trabalho sob o seu controle e que afeta o desempenho da segurança da informação;
    - **assegurar** que essas pessoas são competentes, com base na educação, treinamento ou experiência apropriados;
    - **reter informação documentada** apropriada como evidência da competência.
- **Conscientização**
  - Pessoas que realizam trabalho sob o controle da organização devem estar **cientes** da:
    - **política de segurança da informação**;
    - **implicações da não conformidade** com os requisitos do SGSI.
- **Comunicação**
  - A organização deve determinar as **comunicações internas e externas** relevantes para o SGSI.
- **Informação documentada**
  - O SGSI deve incluir **informação documentada** requerida pela norma.

Operação

- **Planejamento operacional e controle**
  - A organização deve **planejar, implementar e controlar** os **processos necessários** para atender aos requisitos de segurança da informação.

- **Avaliação de riscos de segurança da informação**
  - A organização deve realizar **avaliações de riscos** de segurança da informação a **intervalos planejados**, ou quando **mudanças significativas** são propostas ou ocorrem.

- **Tratamento de riscos de segurança da informação**
  - A organização deve **implementar** o **plano de tratamento de riscos de segurança da informação**.

Avaliação do desempenho

- **Monitoramento, medição, análise e avaliação**
  - A **organização** deve **avaliar o desempenho da segurança da informação** e a **eficácia** do sistema de gestão da segurança da informação.

- **Auditoria interna**
  - A organização deve conduzir **auditorias internas** a **intervalos planejados** para prover informações sobre o quanto o sistema de gestão da segurança da informação:
    - a) **está em conformidade com os próprios requisitos da organização** para o seu SGSI e com os requisitos da norma;
    - b) está **efetivamente implementado e mantido.**

- **Análise crítica pela Direção**
  - A **Alta Direção** deve **analisar criticamente** o sistema de gestão da segurança da informação da organização a **intervalos planejados**, para assegurar a sua **contínua adequação, pertinência e eficácia**.

Melhoria

- **Não conformidade e ação corretiva**
  - Quando uma não conformidade ocorre, a organização deve:
    - **reagir a não conformidade** e, conforme apropriado tomar ações para controlar e corrigi-la;
    - **avaliar a necessidade de ações para eliminar as causas de não conformidade**, para evitar sua repetição ou ocorrência;
    - **implementar** quaisquer **ações necessárias**;
    - **realizar mudanças** no SGSI.

- **Melhoria contínua**
  - A organização deve **continuamente melhorar** a **pertinência, adequação e eficácia do SGSI**.

Information Security Controls Foundation (ISO/IEC 27002)

Sobre a ISO/IEC 27002

- Escopo
  - A Norma ISO/IEC 27002 fornece **diretrizes** para práticas de gestão de segurança da informação e normas de segurança da informação para as organizações, incluindo a seleção, a implementação e o gerenciamento de controles, levando em consideração os ambientes de risco da segurança da informação da organização.

Estrutura da norma ISO/IEC 27002

- A Norma ISO/IEC 27002 contém **14 seções de controles** de segurança da informação de um total de **35 objetivos de controles** e **114 controles**.
- **Seções**
  - Cada seção definindo os controles de segurança da informação contém **um ou mais objetivos de controle**.
- **Categorias de controles**
  - Cada seção principal contém:
    - um objetivo de controle declarando **o que** se espera que seja alcançado;
    - um ou mais controles que podem ser aplicados para se alcançar o objetivo do controle.
  - As descrições do controle estão estruturadas da seguinte forma:
    - **Controle**
      - Define a declaração específica do controle, para atender ao objetivo de controle.
    - **Diretrizes para implementação**
      - Apresenta informações mais detalhadas para apoiar a implementação do controle e alcançar o objetivo do controle.
    - **Informações adicionais**
      - Apresenta mais dados que podem ser considerados, como por exemplo, questões legais e referências normativas.

5. Políticas de segurança da informação

- **5.1 Orientação da direção para segurança da informação**
  - Objetivo: Prover **orientação** da **direção** e **apoio** para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações relevantes.

- **5.1.1 Políticas para segurança da informação**
- Controle
  - Convém que um conjunto de políticas de segurança da informação seja definido, **aprovado pela direção**, **publicado** e **comunicado** para todos os funcionários e partes externas relevantes.
- Diretrizes para implementação
  - Convém que, **no mais alto nível**, a organização defina uma **política de segurança da informação**, que seja aprovada pela direção e estabeleça a abordagem da organização para gerenciar os objetivos de segurança da informação.
  - Convém que as políticas de segurança da informação contemplem requisitos oriundos de **estratégia do negócio**, **regulamentações, legislação e contratos e ambiente de ameaça da segurança da informação, atual e futuro**.

5. Políticas de segurança da informação

- **5.1.1 Políticas para segurança da informação**
  - Convém que a política de segurança da informação contenha declarações relativas a:
    - definição de segurança da informação, **objetivos** e **princípios** para orientar todas as atividades relativas à segurança da informação;
    - atribuição de **responsabilidades**, gerais e específicas, para o gerenciamento da segurança da informação para os papéis definidos;
    - **processos para o tratamento dos desvios e exceções**.
  - No nível mais baixo, convém que a política de segurança da informação seja apoiada por **políticas específicas** do tema, exemplos:
    - classificação e tratamento da informação
    - uso aceitável dos ativos;
    - mesa limpa e tela limpa;
    - dispositivos móveis e trabalho remoto;
    - restrições sobre o uso e instalação de *software*;
    - *backup*;
    - proteção contra *malware*
    - gerenciamento de vulnerabilidades técnicas
    - proteção e privacidade da informação de identificação pessoal.

5. Políticas de segurança da informação

- **5.1.2 Análise crítica das políticas para segurança da informação**
- Controle
  - Convém que as políticas de segurança da informação sejam **analisadas criticamente a intervalos planejados** ou quando mudanças significativas ocorrerem, para assegurar a sua **contínua pertinência, adequação e eficácia**.

6. Organização da segurança da informação

- **6.1 Organização interna**
- **6.1.1 Responsabilidades e papéis pela segurança da informação**
- Controle
  - Convém que todas as **responsabilidades** pela segurança da informação sejam **definidas e atribuídas**.

- Diretrizes para implementação
  - Convém que a **atribuição das responsabilidades pela segurança da informação** seja feita em **conformidade** com as **políticas de segurança da informação**.

6. Organização da segurança da informação

- **6.1.2 Segregação de funções**
- Controle
  - Convém que funções conflitantes e áreas de responsabilidade sejam **segregadas** para reduzir as oportunidades de modificação não autorizada ou não intencional, ou uso indevido dos ativos da organização.

- Diretrizes para implementação
  - Convém que sejam tomados certos cuidados para **impedir** que uma **única pessoa** possa **acessar, modificar ou usar ativos sem a devida autorização ou detecção**.

6. Organização da segurança da informação

- **6.1.3 Contato com autoridades**
- Controle
  - Convém que contatos apropriados com autoridades relevantes sejam mantidos.

- Diretrizes para implementação
  - Convém que a organização tenha procedimentos implementados que especifiquem **quando** e **quais autoridades** serão **contatadas** e como os incidentes de segurança da informação identificados serão reportados em tempo hábil.

6. Organização da segurança da informação

- **6.1.4 Contato com grupos especiais**
- Controle
  - Convém que contatos apropriados com grupos especiais, associações profissionais ou outros fóruns especializados em segurança da informação sejam mantidos.

6. Organização da segurança da informação

- **6.1.5 Segurança da informação no gerenciamento de projetos**
- Controle
  - Convém que a **segurança da informação seja considerada** no gerenciamento de projetos, **independentemente do tipo do projeto**.

- Diretrizes para implementação
  - Convém que a segurança da informação seja **integrada** nos métodos de gerenciamento de projeto da organização para assegurar que os **riscos de segurança da informação** estejam **identificados** e **considerados como parte de um projeto**.
  - Convém que os métodos de gerenciamento de projetos usados requeiram que:
    - os objetivos de segurança da informação sejam contemplados nos objetivos do projeto;
    - uma **avaliação dos riscos de segurança da informação** seja conduzida em **estágios iniciais** do projeto para identificar os controles que são necessários;
    - a segurança da informação seja **parte integrante** de **todas as fases** da metodologia do projeto.

6. Organização da segurança da informação

- **6.2 Dispositivos móveis e trabalho remoto**
  - Objetivo: Garantir a segurança das informações no trabalho remoto e no uso de dispositivos móveis.
- **6.2.1 Política para o uso de dispositivo móvel**
- Controle
  - Convém que uma **política e medidas** que apoiam a segurança da informação sejam adotadas para gerenciar os riscos decorrentes do uso de dispositivos móveis.

- Diretrizes para implementação
  - Convém que, quando se utilizam dispositivos móveis, **cuidados especiais** sejam tomados para assegurar que as informações do negócio não sejam comprometidas. Convém que a política de dispositivos móveis leve em consideração os riscos de se trabalhar com esses dispositivos móveis em ambientes desprotegidos.

6. Organização da segurança da informação

- **6.2.1 Política para o uso de dispositivo móvel (continuação)**
  - Convém que a política para uso de dispositivos móveis considere:
    - registros dos dispositivos móveis;
    - requisitos para a proteção física;
    - restrições quanto à instalação de *software*;
    - requisitos para as versões dos *software* e aplicações de *patches*;
    - controle de acesso;
    - técnicas criptográficas;
    - proteção contra *malware*;
    - desativação, bloqueio e exclusão de forma remota;
    - *backups*;
    - uso dos serviços *web*.
  - Convém que cuidados sejam tomados ao se utilizarem dispositivos móveis em **locais públicos, salas de reuniões e outras áreas desprotegidas.**
  - Convém que sejam estabelecidas proteções para **evitar o acesso não autorizado** ou a **divulgação de informações armazenadas e processadas nesses dispositivos**, por exemplo, usando técnicas de **criptografia** e uso de **autenticação segura**.

6. Organização da segurança da informação

- **6.2.2 Trabalho remoto**
- Controle
  - Convém que uma **política e medidas** que apoiam a segurança da informação sejam implementadas para proteger as informações acessadas, processadas ou armazenadas em **locais de trabalho remoto**.
- Diretrizes para implementação
  - Convém que a organização que permita a atividade de trabalho remoto publique uma **política** que defina as condições e restrições para o **uso do trabalho remoto**. Onde considerados aplicáveis e permitidos por lei, convém que os seguintes pontos sejam considerados:
    - a **segurança física** existente no local do trabalho remoto, levando-se em consideração a segurança física do prédio e o ambiente local;
    - o **ambiente físico** proposto para o trabalho remoto;
    - os requisitos de segurança nas comunicações, levando em consideração a necessidade do acesso remoto aos sistemas internos da organização, a **sensibilidade da informação** que será acessada e trafegada na linha de comunicação;
    - o fornecimento de **acesso virtual às estações de trabalho** dos usuários, para prevenir o processamento e o armazenamento da informação em um equipamento de propriedade particular;
    - a ameaça de acesso não autorizado à informação ou aos recursos de processamento da informação por outras pessoas que utilizam o local, por exemplo familiares e amigos;
    - o uso de redes domésticas e requisitos ou restrições na configuração de serviços de rede sem fio;
    - **requisitos de *firewall* e proteção antivírus**.

7. Segurança em recursos humanos

- **7.1 Antes da contratação**
  - Objetivo: Assegurar que funcionários e partes externas entendem as suas responsabilidades e estão em conformidade com os papéis para os quais eles foram selecionados.
- **7.1.1 Seleção**
- Controle
  - Convém que verificações do histórico sejam realizadas para **todos os candidatos** a emprego, de acordo com a **ética**, **regulamentações e leis relevantes**, e seja proporcional aos **requisitos do negócio**, aos riscos percebidos e à **classificação das informações** a serem acessadas.
- Diretrizes para implementação
  - Convém que as verificações levem em consideração toda a legislação pertinente relativa à **privacidade**, **proteção de dados pessoais** e do emprego e, onde permitido, incluam os seguintes itens:
    - uma verificação (da exatidão e completeza) das informações do *curriculum vitae* do candidato;
    - confirmação das qualificações acadêmicas e profissionais;
    - verificação independente da identidade (passaporte ou documento similar);
    - verificações mais detalhadas, como verificações de crédito ou verificações de registros criminais.

7. Segurança em recursos humanos

- **7.1.2 Termos e condições de contratação**
- Controle
  - Convém que as obrigações contratuais com funcionários e partes externas declarem a sua responsabilidade e as da organização para a segurança da informação.
- Diretrizes para implementação
  - Convém que as obrigações contratuais para funcionários e partes externas reflitam as políticas para segurança da informação da organização, esclarecendo e declarando:
    - que todos os funcionários, fornecedores e partes externas que tenham acesso a informações sensíveis assinem um **termo de confidencialidade ou de não divulgação**, antes de lhes ser dado o acesso aos recursos de processamento da informação;
    - as **responsabilidades legais e direitos dos funcionários e partes externas**, e quaisquer outros usuários, por exemplo, com relação às leis de direitos autorais e legislação de proteção de dados.
    - as responsabilidades pela classificação da informação e pelo gerenciamento dos ativos da organização;
    - **ações a serem tomadas** no caso de o funcionário ou partes externas, **desrespeitar os requisitos de segurança da informação** da organização;
  - Convém que as responsabilidades contidas nos termos e condições de contratação **continuem por um período de tempo definido, após o término da contratação.**
- Informações adicionais
  - Um **código de conduta** pode ser usado para estabelecer as responsabilidades de segurança da informação do funcionário ou parte externa quanto à confidencialidade, proteção de dados, ética, uso apropriado dos equipamentos e recursos da organização.

7. Segurança em recursos humanos

- **7.2 Durante a contratação**
  - Objetivo: Assegurar que os funcionários e partes externas estão conscientes e cumprem as suas responsabilidades pela segurança da informação.
- **7.2.1 Responsabilidades da Direção**
- Controle
  - Convém que a Direção solicite a todos os funcionários e partes externas que pratiquem a segurança da informação de acordo com o estabelecido nas políticas e procedimentos da organização.
- Diretrizes para implementação
  - Convém que faça parte das responsabilidades da Direção assegurar que funcionários e partes externas:
    - estejam **adequadamente instruídos sobre as suas responsabilidades e papéis** pela segurança da informação, antes de obter acesso às informações sensíveis ou aos sistemas de informação;
    - recebam **diretrizes** que definam quais as expectativas sobre a segurança da informação de suas atividades dentro da organização;
    - tenham as **habilidades e qualificações** apropriadas e sejam **treinados regularmente**;
    - tenham disponível um **canal de notificação**, de forma anônima, para **reportar violações** nas políticas e procedimentos de segurança da informação.

7. Segurança em recursos humanos

- **7.2.2 Conscientização, educação e treinamento em segurança da informação**
- Controle
  - Convém que todos os funcionários da organização e, onde pertinente, partes externas recebam **treinamento, educação e conscientização** apropriados, e as atualizações regulares das políticas e procedimentos organizacionais relevantes para as suas funções.
- Diretrizes para implementação
  - Convém que um **programa de conscientização em segurança da informação** seja estabelecido **alinhado** com as políticas e procedimentos relevantes de segurança da informação da organização, levando em consideração as informações da organização a serem protegidas e os controles que foram implementados para proteger a informação.
  - Convém que as atividades do **programa de conscientização** sejam planejadas **ao longo do tempo**, preferencialmente de **forma regular**, de tal modo que as atividades sejam repetidas e contemplem **novos funcionários e partes externas**.
  - Convém que o programa de conscientização também seja **atualizado regularmente**, de modo que ele permaneça **alinhado** com as **políticas e os procedimentos da organização**, e seja construído com base nas lições aprendidas dos incidentes de segurança da informação.
  - Convém que o treinamento em conscientização use **diferentes formas de apresentação**, incluindo treinamento presencial, treinamento à distância, treinamento baseado em *web*, autodidata e outros.
  - Convém que o **treinamento e a educação** em segurança da informação sejam realizados **periodicamente**.

7. Segurança em recursos humanos

- **7.2.3 Processo disciplinar**
- Controle
  - Convém que exista um **processo disciplinar formal**, implantado e comunicado, para tomar ações contra funcionários que tenham cometido uma **violação de segurança da informação**.
- Diretrizes para implementação
  - Convém que o processo disciplinar não seja iniciado sem uma **verificação prévia** de que a violação da segurança da informação realmente ocorreu.
  - Convém que o processo disciplinar formal assegure um **tratamento justo** e **correto** aos funcionários que sejam suspeitos de cometer violações de segurança da informação. Convém que o processo disciplinar formal apresente uma resposta de **forma gradual**, que leve em consideração fatores como a natureza e a gravidade da violação e o seu impacto no negócio, se este é ou não o primeiro delito ou delito repetido, se o infrator foi ou não adequadamente treinado, as legislações relevantes, os contratos do negócio e outros fatores, conforme requerido.
  - Convém que o processo disciplinar também seja usado como uma **forma de dissuasão**, para evitar que os funcionários e partes externas violem os procedimentos e as políticas de segurança da informação da organização.

7. Segurança em recursos humanos

- **7.3 Encerramento e mudança da contratação**
  - Objetivo: Proteger os interesses da organização como parte do processo de mudança ou encerramento da contratação.
- **7.3.1 Responsabilidades pelo encerramento ou mudança da contratação**
- Controle
  - Convém que as responsabilidades e obrigações pela segurança da informação que permaneçam válidas após um encerramento ou mudança da contratação sejam definidas, comunicadas aos funcionários ou partes externas e cumpridas.
- Diretrizes para implementação
  - Convém que a comunicação de encerramento de atividades inclua requisitos de segurança da informação e responsabilidades legais existentes e, onde apropriado, responsabilidades contidas em quaisquer acordos de confidencialidade, e os termos e condições de trabalho que permaneçam por um período definido após o fim do trabalho do funcionário ou partes externas.

8. Gestão de ativos

- **8.1 Responsabilidade pelos ativos**
  - Objetivo: Identificar os ativos da organização e definir as devidas responsabilidades pela proteção dos ativos.
- **8.1.1 Inventário dos ativos**
- Controle
  - Convém que os ativos associados à informação e aos recursos de processamento da informação **sejam identificados**, e um **inventário** destes ativos seja estruturado e mantido.
- Diretrizes para implementação
  - Convém que a organização identifique os **ativos relevantes no ciclo de vida da informação** e documente a sua importância. Convém que o ciclo de vida da informação inclua a criação, o processamento, o armazenamento, a transmissão, a exclusão e a sua destruição.

8. Gestão de ativos

- **8.1.2 Proprietário dos ativos**
- Controle
  - Convém que os ativos mantidos no inventário tenham um **proprietário**.

- Diretrizes para implementação
  - Convém que o proprietário seja designado quando os ativos são criados ou quando os ativos são transferidos para a organização. Convém que o proprietário do ativo seja responsável pelo próprio gerenciamento deste ativo ao longo do seu ciclo de vida.

8. Gestão de ativos

- **8.1.3 Uso aceitável dos ativos**
- Controle
  - Convém que regras para o uso aceitável das informações, dos ativos associados com a informação e dos recursos de processamento da informação sejam identificadas, documentadas e implementadas.

8. Gestão de ativos

- **8.1.4 Devolução de ativos**
- Controle
  - Convém que todos os funcionários e partes externas **devolvam todos os ativos** da organização que estejam em sua posse, **após o encerramento de suas atividades**, do contrato ou acordo.

- Diretrizes para implementação
  - Convém que o processo de encerramento de atividades seja **formalizado** para contemplar a devolução de todos os equipamentos **físico e eletrônico**, de propriedade da organização.

8. Gestão de ativos

- **8.2 Classificação da informação**
  - Objetivo: Assegurar que a informação receba um **nível adequado de proteção**, de acordo com a sua importância para a organização.
- **8.2.1 Classificação da informação**
- Controle
  - Convém que a informação seja **classificada** em termos do seu **valor, requisitos legais, sensibilidade e criticidade** para **evitar modificação ou divulgação não autorizada**.
- Diretrizes para implementação
  - Convém que a classificação e os controles de proteção, associados à informação, levem em consideração as necessidades do negócio para compartilhar ou restrigir a informação bem como os requisitos legais.
  - Convém que os **proprietários** de ativos de informação **sejam responsáveis por sua classificação**.
  - Convém que o esquema seja **consistente** em toda a organização, de forma que cada pessoa possa classificar a informação e os ativos relacionados da mesma forma, e tenha um entendimento comum dos requisitos de proteção e aplique a proteção apropriada.
  - Convém que os resultados da classificação sejam atualizados de acordo com as mudanças do seu valor, sensibilidade e criticidade ao longo do seu ciclo de vida.

8. Gestão de ativos

- **8.2.2 Rótulos e tratamento da informação**
- Controle
  - Convém que um conjunto apropriado de procedimentos para **rotular e tratar a informação** seja desenvolvido e implementado de acordo com o esquema de **classificação da informação** adotado pela organização.

- Diretrizes para implementação
  - Convém que procedimentos para a rotulagem da informação abranjam a informação e os seus ativos relacionados, nos formatos **físico e eletrônico.**

8. Gestão de ativos

- **8.2.3 Tratamento dos ativos**
- Controle
  - Convém que procedimentos para o tratamento dos ativos sejam desenvolvidos e implementados de acordo com o esquema de classificação da informação adotado pela organização.

- Diretrizes para implementação
  - Convém que **procedimentos** sejam estabelecidos para o **tratamento, processamento, armazenamento e transmissão** da informação, de acordo com a sua classificação.

8. Gestão de ativos

- **8.3 Tratamento de mídias**
  - Objetivo: Prevenir a divulgação não autorizada, modificação, remoção ou destruição da informação armazenada nas mídias.

- **8.3.1 Gerenciamento de mídias removíveis**
- Controle
  - Convém que existam **procedimentos** implementados para o gerenciamento de mídias removíveis, de acordo com o esquema de classificação adotado pela organização.

8. Gestão de ativos

- **8.3.2 Descarte de mídias**
- Controle
  - Convém que as mídias sejam **descartadas** de **forma segura**, quando não forem mais necessárias, por meio de **procedimentos formais**.
- Diretrizes para implementação
  - Convém que **procedimentos formais** para o **descarte seguro das mídias** sejam definidos para minimizar o risco de vazamento de informações sensíveis para pessoas não autorizadas. Os procedimentos para o descarte seguro das mídias, contendo informações confidenciais, sejam proporcionais à sensibilidade das informações.
  - Convém que mídias contendo informações confidenciais sejam **guardadas e destruídas de forma segura e protegida**, como, por exemplo, através de incineração ou trituração, ou da remoção dos dados para uso por outra aplicação dentro da organização.
- Informações adicionais
  - Equipamentos danificados contendo dados sensíveis podem exigir uma **avaliação de riscos** para determinar se é recomendado que os itens sejam **destruídos fisicamente** em vez de serem enviados para conserto ou descartados.

8. Gestão de ativos

- **8.3.3 Transferência física de mídias**
- Controle
  - Convém que mídias contendo informações sejam **protegidas contra acesso não autorizado**, uso impróprio ou corrupção, **durante o transporte**.

- Diretrizes para implementação
  - Convém que as seguintes recomendações sejam consideradas, para proteger as mídias que contêm informações, quando transportadas:
    - o meio de transporte ou o serviço de mensageiros sejam confiáveis;
    - a embalagem seja suficiente para **proteger** o conteúdo contra qualquer **dano físico**, como os que podem ocorrer durante o transporte, e que seja feita de acordo com as especificações dos fabricantes (como no caso de *software*), por exemplo, protegendo contra fatores ambientais que possam reduzir a possibilidade de restauração dos dados, como a **exposição ao calor, umidade ou campos eletromagnéticos**.

9. Controle de Acesso

- **9.1 Requisitos do negócio para controle de acesso**
  - Objetivo: Limitar o acesso à informação e aos recursos de processamento da informação.
- **9.1.1 Política de controle de acesso**
- Controle
  - Convém que uma **política de controle de acesso** seja estabelecida, documentada e analisada criticamente, baseada nos requisitos de segurança da informação e dos negócios.
- Diretrizes para implementação
  - Convém que os proprietários dos ativos determinem regras apropriadas do controle de acesso, direitos de acesso e restrições para papéis específicos dos usuários acessarem seus ativos, com o nível de detalhe e o rigor dos controles que reflitam os riscos de segurança da informação associados.
  - Convém que sejam considerados os **controles de acesso lógico e físico de forma conjunta**.
  - Convém que a política leve em consideração os seguintes itens:
    - legislação pertinente e qualquer obrigação contratual relativa à proteção de acesso para dados ou serviços;
    - gerenciamento de direitos de acesso em um ambiente distribuído e conectado à rede que reconhece todos os tipos de conexões disponíveis;
    - **segregação de funções de controle de acesso**, por exemplo, pedido de acesso, autorização de acesso, administração de acesso;
    - requisitos para autorização formal de pedidos de acesso;
    - **remoção de direitos de acesso**;
    - regras para o acesso privilegiado.

9. Controle de Acesso

- **9.1.2 Acesso às redes e aos serviços de rede**
- Controle
  - Convém que os usuários somente recebam acesso às redes e aos serviços de rede que tenham sido especificamente autorizados a usar.
- Diretrizes para implementação
  - Convém que uma **política** seja formulada com relação **ao uso de redes e serviços de rede**. Convém que esta política inclua:
    - redes e serviços de redes que são permitidos de serem acessados;
    - **procedimentos de autorização** para determinar quem tem permissão para acessar quais redes e serviços de redes;
    - **procedimentos e controles de gerenciamento** para proteger o acesso a conexões e serviços de redes;
    - os meios usados para acessar redes e serviços de rede (por exemplo, uso de VPN ou redes sem fio);
    - **requisitos de autenticação** do usuário para acessar vários serviços de rede;
    - monitoramento do uso dos serviços de rede.
  - Convém que a política do uso de serviço de rede seja consistente com a política de controle de acesso da organização.

9. Controle de Acesso

- **9.2 Gerenciamento de acesso do usuário**
  - Objetivo: Assegurar acesso de usuário autorizado e **prevenir acesso não autorizado** a sistemas e serviços.

- **9.2.1 Registro e cancelamento de usuário**
- Controle
  - Convém que um **processo formal** de **registro e cancelamento de usuário** seja implementado para permitir atribuição dos direitos de acesso.
- Diretrizes para implementação
  - Convém que o processo para gerenciar o ID de usuário inclua:
    - o uso de um ID de usuário único, para permitir relacionar os usuários às suas responsabilidades e ações;
    - a imediata remoção ou desabilitação do ID de usuário que tenham deixado a organização.

9. Controle de Acesso

- **9.2.2 Provisionamento para acesso de usuário**
- Controle
  - Convém que um **processo formal de provisionamento de acesso do usuário** seja implementado para **conceder ou revogar os direitos de acesso do usuário** para **todos os tipos de usuários** em **todos os tipos de sistemas e serviços**.

9. Controle de Acesso

- **9.2.3 Gerenciamento de direitos de acesso privilegiados**
- Controle
  - Convém que a concessão e o uso de direitos de acesso privilegiado sejam **restritos e controlados.**

- Diretrizes para implementação
  - Convém que a alocação de direitos de acesso privilegiado seja controlada por meio de um **processo de autorização formal**, de acordo com a política de controle de acesso pertinente.

9. Controle de Acesso

- **9.2.4 Gerenciamento da informação de autenticação secreta de usuários**
- Controle
  - Convém que a concessão de informação de autenticação secreta seja controlada por meio de um processo de **gerenciamento formal**.

- Diretrizes para implementação
  - Convém que o processo inclua o seguinte requisito:
    - solicitar aos usuários a **assinatura de uma declaração**, para manter a confidencialidade da informação de autenticação secreta e para manter as senhas de grupos de trabalho, exclusivamente com os membros do grupo; esta declaração assinada pode ser incluída nos termos e condições da contratação.

9. Controle de Acesso

- **9.2.5 Análise crítica dos direitos de acesso de usuário**
- Controle
  - Convém que os proprietários de ativos **analisem criticamente os direitos de acesso dos usuários, a intervalos regulares**.

- Diretrizes para implementação
  - Convém que a análise crítica dos direitos de acesso considere a seguinte orientação:
    - os direitos de acesso de usuários sejam revisados em **intervalos regulares** e depois de quaisquer **mudanças**, como promoção, remanejamento ou encerramento do contrato.

9. Controle de Acesso

- **9.2.6 Retirada ou ajuste dos direitos de acesso**
- Controle
  - Convém que os direitos de acesso de todos os funcionários e partes externas às informações e aos recursos de processamento da informação sejam **retirados logo após o encerramento de suas atividades**, contratos ou acordos, ou ajustados após a mudança destas atividades.

- Diretrizes para implementação
  - Convém que, após o encerramento das atividades, os direitos de acesso da pessoa aos ativos associados com os sistemas de informação e serviços sejam removidos ou suspensos.

9. Controle de Acesso

- **9.3 Responsabilidades dos usuários**
  - Objetivo: Tornar os usuários responsáveis pela proteção das suas informações de autenticação.
- **9.3.1 Uso da informação de autenticação secreta**
- Controle
  - Convém que os usuários sejam orientados a seguir as práticas da organização quanto ao uso da informação de autenticação secreta.
- Diretrizes para implementação
  - Convém que todos os usuários sejam informados para:
    - manter a **confidencialidade** da informação de autenticação secreta;
    - **evitar manter anotada** a informação de autenticação secreta (por exemplo, papel, arquivos ou dispositivos móveis), a menos que ela possa ser armazenada de forma segura;
    - alterar a informação de autenticação secreta, sempre que existir qualquer indicação de possível comprometimento do sistema ou da própria senha;
    - quando as senhas são usadas como informação de autenticação secreta, selecionar senhas de qualidade, com um tamanho mínimo, que sejam:
      - fáceis de lembrar;
      - não vulneráveis a **ataque de dicionário** (por exemplo, não consistir em palavras inclusas no dicionário);
      - isentas de caracteres idênticos consecutivos, todos numéricos ou todos alfabéticos sucessivos;
      - caso a senha seja **temporária**, ela deve ser mudada no primeiro acesso (*log-on*).

9. Controle de Acesso

- **9.4 Controle de acesso ao sistema e à aplicação**
  - Objetivo: Prevenir o acesso não autorizado aos sistemas e aplicações.

- **9.4.1 Restrição de acesso à informação**
- Controle
  - Convém que o acesso à informação e às funções dos sistemas de aplicações seja restrito, de acordo com a política de controle de acesso.

- Diretrizes para implementação
  - Convém que restrições para o acesso sejam baseadas nos requisitos das aplicações individuais do negócio e de acordo com a política de controle de acesso definida.

9. Controle de Acesso

- **9.4.2 Procedimentos seguros de entrada no sistema (*log-on*)**
- Controle
  - Convém que, onde aplicável pela política de controle de acesso, o acesso aos sistemas e aplicações sejam controlados por um **procedimento seguro** de entrada no sistema **(*log-on*).**
- Diretrizes para implementação
  - Convém que uma técnica de autenticação adequada seja escolhida para validar a identificação alegada de um usuário.
  - Onde é requerida a verificação de identidade e uma forte autenticação, convém que métodos alternativos de autenticação para as senhas, como **meios criptográficos, *smart cards*, *tokens* ou biometria**, sejam usados.
  - Convém que o procedimento de entrada (*log-on*) revele o **mínimo de informações sobre o sistema ou aplicação**, de forma a evitar o fornecimento de informações desnecessárias a um usuário não autorizado. Convém que um procedimento de *log-on*:
    - não **mostre identificadores de sistema ou de aplicação** até que o processo tenha sido concluído com sucesso;
    - mostre um aviso geral informando que o computador seja acessado somente por usuários autorizados;
    - não forneça mensagens de ajuda durante o procedimento *log-on* que poderiam auxiliar um usuário não autorizado;
    - valide informações de entrada no sistema **somente** quando **todos os dados** de entrada **estiverem completos**. Caso ocorra uma condição de erro, o sistema não indique qual parte do dado de entrada está correta ou incorreta;
    - **proteja** contra **tentativas forçadas** de entrada no sistema (*log-on*);
    - **registre tentativas** de acesso ao sistema, sem sucesso e bem-sucedida;
    - **não mostre a senha que está sendo informada**;
    - **encerre sessões inativas** após um período definido de inatividade.

9. Controle de Acesso

- **9.4.3 Sistema de gerenciamento de senha**
- Controle
  - Convém que sistemas para gerenciamento de senhas sejam interativos e assegurem **senhas de qualidade**.

- Diretrizes para implementação
  - Convém que o sistema de gerenciamento de senha:
    - obrigue o uso individual de ID de usuário e senha para manter responsabilidades;
    - permita que os usuários **selecionem e modifiquem suas próprias senhas**, incluindo um procedimento de confirmação para evitar erros;
    - obrigue a escolha de **senhas de qualidade**;
    - obrigue os usuários a **mudarem** as suas senhas temporárias no **primeiro acesso** ao sistema;
    - force as mudanças de senha a **intervalos regulares**, conforme necessário;
    - mantenha um registro das **senhas anteriores utilizadas** e **bloqueie a reutilização**;
    - **não mostre as senhas na tela** quando **forem digitadas**;
    - armazene e transmita as senhas de forma **protegida**.

9. Controle de Acesso

- **9.4.4 Uso de programas utilitários privilegiados**
- Controle
  - Convém que o uso de programas utilitários que podem ser capazes de sobrepor os controles dos sistemas e aplicações seja restrito e estritamente controlado.

9. Controle de Acesso

- **9.4.5 Controle de acesso ao código-fonte de programas**
- Controle
  - Convém que o acesso ao **código-fonte** de programa seja **restrito**.

- Diretrizes para implementação
  - Convém que o acesso ao código-fonte de programas e de itens associados seja **estritamente controlado**, com a finalidade de prevenir a introdução de funcionalidade não autorizada e para evitar mudanças não intencionais, bem como para manter a confidencialidade de propriedade intelectual valiosa.

10. Criptografia

- **10.1 Controles criptográficos**
  - Objetivo: Assegurar o uso efetivo e adequado da criptografia para proteger a confidencialidade, autenticidade e/ou a integridade da informação.
- **10.1.1 Política para o uso de controles criptográficos**
- Controle
  - Convém que seja desenvolvida e implementada uma **política sobre o uso de controles criptográficos** para a proteção da informação.
- Diretrizes para implementação
  - Quando do desenvolvimento de uma política para criptografia, convém que sejam considerados:
    - a **abordagem da direção** quanto ao uso de controles criptográficos em toda a organização, incluindo os princípios gerais sob os quais as informações de negócio sejam protegidas;
    - a identificação **do nível requerido de proteção** com base em uma **avaliação de risco**, levando em consideração o tipo, a força e a qualidade do algoritmo de criptografia requerido;
    - o uso de **criptografia** para a proteção de **informações sensíveis** transportadas em dispositivos móveis, mídias removíveis ou através de linhas de comunicação.

10. Criptografia

- **10.1.2 Gerenciamento de chaves**
- Controle
  - Convém que uma **política sobre o uso, proteção e tempo de vida das chaves criptográficas** seja desenvolvida e implementada ao longo de todo o seu ciclo de vida.

- Diretrizes para implementação
  - Convém que a política inclua **requisitos para o gerenciamento de chaves criptográficas** ao longo de todo o seu **ciclo de vida**, incluindo a geração, armazenamento, arquivo, recuperação, distribuição, retirada e destruição das chaves.

11. Segurança física e do ambiente

- **11.1 Áreas seguras**
  - Objetivo: **Prevenir o acesso físico não autorizado**, **danos** e **interferências** com os recursos de processamento das informações e nas informações da organização.
- **11.1.1 Perímetro de segurança física**
- Controle
  - Convém que **perímetros de segurança sejam definidos** e usados para proteger tanto as instalações de processamento da informação como as áreas que contenham informações **críticas ou sensíveis**.
- Diretrizes para implementação
  - Convém que as seguintes diretrizes sejam consideradas e implementadas, onde apropriado, para os perímetros de segurança física:
    - convém que seja implantada uma **área de recepção**, ou um outro meio para controlar o acesso físico ao local ou ao edifício; convém que o acesso aos locais ou edifícios fique restrito somente ao **pessoal autorizado**;
    - convém que sejam construídas **barreiras físicas**, onde aplicável, para **impedir o acesso físico não autorizado**;
    - convém que **sistemas de detecção de intrusos** sejam **instalados** e **testados** em **intervalos regulares**.

11. Segurança física e do ambiente

- **11.1.2 Controles de entrada física**
- Controle
  - Convém que as áreas seguras sejam protegidas por controles apropriados de entrada para assegurar que somente **pessoas autorizadas** tenham **acesso permitido**.
- Diretrizes para implementação
  - Convém que sejam levadas em consideração as seguintes diretrizes:
    - convém que a **data e a hora da entrada e saída** de **visitantes** sejam registradas, e **todos os visitantes sejam supervisionados**, a não ser que o seu acesso tenha sido previamente aprovado; convém que as permissões de acesso só sejam concedidas para finalidades específicas e autorizadas;
    - convém que o acesso às áreas em que são processadas ou armazenadas informações sensíveis seja **restrito apenas ao pessoal autorizado** pela implementação de controles de acesso apropriados, por exemplo, mecanismos de **autenticação de dois fatores**, como, **cartões de controle de acesso e PIN (*personal identifi cation number*);**
    - convém que seja exigido que todos os funcionários, fornecedores e partes externas, e todos os visitantes, tenham alguma **forma visível de identificação**;
    - às partes externas que realizam serviços de suporte, convém que seja concedido **acesso restrito** às áreas seguras ou as instalações de processamento da informação sensíveis, somente quando necessário; convém que este acesso seja **autorizado e monitorado**.

11. Segurança física e do ambiente

- **11.1.3 Segurança em escritórios, salas e instalações**
- Controle
  - Convém que seja projetada e aplicada **segurança física para escritórios, salas e instalações**.

- Diretrizes para implementação
  - Convém que as instalações-chave sejam localizadas de maneira a evitar o acesso do público.

11. Segurança física e do ambiente

- **11.1.4 Proteção contra ameaças externas e do meio ambiente**
- Controle
  - Convém que seja projetada e aplicada **proteção física** contra **desastres naturais, ataques maliciosos ou acidentes**.

- Diretrizes para implementação
  - Convém que **orientações de especialistas** sejam obtidas sobre como evitar danos oriundos de fogo, inundação, terremoto, explosão, manifestações civis e outras formas de **desastre natural** ou provocado pela natureza.

11. Segurança física e do ambiente

- **11.1.5 Trabalhando em áreas seguras**
- Controle
  - Convém que sejam projetados e aplicados procedimentos para o trabalho em áreas seguras.

- Diretrizes para implementação
  - Convém que sejam levadas em consideração as seguintes diretrizes:
    - o pessoal só tenha **conhecimento da existência de áreas seguras** ou das atividades nelas realizadas, **se for necessário**;
    - seja **evitado o trabalho não supervisionado em áreas seguras**;
    - **não seja permitido** o uso de **máquinas fotográficas, gravadores de vídeo ou áudio ou de outros equipamentos de gravação, como câmeras em dispositivos móveis**, salvo se for autorizado.

11. Segurança física e do ambiente

- **11.1.6 Áreas de entrega e de carregamento**
- Controle
  - Convém que pontos de acesso, como áreas de entrega e de carregamento e outros pontos em que pessoas não autorizadas possam entrar nas instalações, sejam **controlados** e, se possível, **isolados** das instalações de processamento da informação, **para evitar o acesso não autorizado**.

11. Segurança física e do ambiente

- **11.2 Equipamento**
  - Objetivo: Impedir perdas, danos, furto, ou comprometimento de ativos e interrupção das operações da organização.

- **11.2.1 Localização e proteção do equipamento**
- Controle
  - Convém que os equipamentos sejam **protegidos** e colocados em **locais para reduzir os riscos de ameaças e perigos do meio ambiente**, bem como as oportunidades de **acesso não autorizado**.

11. Segurança física e do ambiente

- **11.2.2 Utilidades**
- Controle
  - Convém que os equipamentos sejam **protegidos contra falta de energia elétrica e outras interrupções** causadas por falhas das utilidades.

- **11.2.3 Segurança do cabeamento**
- Controle
  - Convém que o **cabeamento de energia e de telecomunicações** que transporta dado ou dá suporte aos serviços de informações seja **protegido** contra **interceptação, interferência ou danos**.

- **11.2.4 Manutenção dos equipamentos**
- Controle
  - Convém que os equipamentos tenham uma **manutenção correta** para assegurar a sua **contínua integridade e disponibilidade**.

11. Segurança física e do ambiente

- **11.2.5 Remoção de ativos**
- Controle
  - Convém que equipamentos, informações ou *software* **não sejam retirados do local sem autorização prévia**.

- **11.2.6 Segurança de equipamentos e ativos fora das dependências da organização**
- Controle
  - Convém que sejam tomadas medidas de segurança para ativos que operem fora do local, levando em conta os diferentes riscos decorrentes do fato de se trabalhar fora das dependências da organização.

- **11.2.7 Reutilização ou descarte seguro de equipamentos**
- Controle
  - Convém que todos os equipamentos que contenham mídias de armazenamento de dados **sejam examinados antes da reutilização**, para assegurar que todos os dados sensíveis e *software* licenciados tenham **sido removidos ou sobregravados com segurança**.

11. Segurança física e do ambiente

- **11.2.8 Equipamento de usuário sem monitoração**
- Controle
  - Convém que os usuários assegurem que os **equipamentos não monitorados** tenham **proteção adequada**.

- **11.2.9 Política de mesa limpa e tela limpa**
- Controle
  - Convém que sejam adotadas uma **política de mesa limpa** para papéis e mídias de armazenamento removíveis e uma **política de tela limpa** para os recursos de processamento da informação.
- Diretrizes para implementação
  - convém que as informações do negócio sensíveis ou críticas, por exemplo, em papel ou em mídia de armazenamento eletrônicas, sejam guardadas em **lugar seguro** (idealmente em um cofre, armário ou outras formas de mobília de segurança), quando não em uso, especialmente quando o escritório estiver desocupado;
  - convém que os computadores e terminais sejam mantidos desligados ou protegidos com mecanismo de travamento de tela e teclados controlados por **senha, *token* ou mecanismo de autenticação similar**, quando sem monitoração, e protegidos por **tecla de bloqueio, senhas ou outros controles, quando não usados**;
  - convém que seja **evitado o uso não autorizado de fotocopiadoras** e de outra tecnologia de reprodução;
  - convém que os documentos que contêm **informação sensível ou classificada** sejam **removidos de impressoras imediatamente**.

12. Segurança nas operações

- **12.1 Responsabilidades e procedimentos operacionais**
  - Objetivo: Garantir a operação segura e correta dos recursos de processamento da informação.

- **12.1.1 Documentação dos procedimentos de operação**
- Controle
  - Convém que os procedimentos de operação sejam **documentados** e **disponibilizados** para **todos os usuários que necessitem deles**.

- Diretrizes para implementação
  - Convém que os procedimentos documentados sejam preparados para as atividades operacionais associadas a recursos de processamento de comunicação e informações, como procedimentos de inicialização e desligamento de computadores, geração de cópias de segurança (*backup*), manutenção de equipamentos, tratamento de mídias, segurança e gestão do tratamento das correspondências e das salas de computadores.

12. Segurança nas operações

- **12.1.2 Gestão de mudanças**
- Controle
  - Convém que mudanças na organização, nos processos do negócio, nos recursos de processamento da informação e nos sistemas que afetam a segurança da informação, sejam **controladas**.

- **12.1.3 Gestão de capacidade**
- Controle
  - Convém que a utilização dos recursos seja **monitorada** e **ajustada**, e que as projeções sejam feitas para **necessidades de capacidade futura** para garantir o **desempenho** requerido do sistema.

12. Segurança nas operações

- **12.1.4 Separação dos ambientes de desenvolvimento, teste e produção**
- Controle
  - Convém que ambientes de desenvolvimento, teste e produção sejam **separados** para **reduzir os riscos de acessos ou modificações não autorizadas no ambiente de produção**.

- Diretrizes para implementação
  - Convém que o nível de separação dos ambientes de produção, testes e desenvolvimento, que é necessário para prevenir problemas operacionais, seja identificado e os controles apropriados sejam implementados.

12. Segurança nas operações

- **12.2 Proteção contra *malware***
  - Objetivo: Assegurar que as informações e os recursos de processamento da informação estão protegidos contra *malware*.

- **12.2.1 Controles contra *malware***
- Controle
  - Convém que sejam implementados controles de **detecção, prevenção e recuperação** para proteger contra *malware*, combinados com um adequado programa de conscientização do usuário.
- Diretrizes para implementação
  - Convém que a proteção contra *malware* seja baseada em ***software* de detecção e resposta a *malware***, na **conscientização da segurança da informação**, no **controle de acesso** adequado e nos **controles de gerenciamento de mudanças**. Recomenda-se que os seguintes controles sejam considerados:
    - estabelecer uma **política** formal proibindo o uso de *software* não autorizados;
    - implementar **controles para prevenir ou detectar o uso de *software* não autorizado** (por exemplo, *whitelisting*, ou seja, uma lista de *software* permitidos.

12. Segurança nas operações

- **12.3 Cópias de segurança**
  - Objetivo: Proteger contra a perda de dados.
- **12.3.1 Cópias de segurança das informações**
- Controle
  - Convém que cópias de segurança das informações, dos *software* e das imagens do sistema sejam **efetuadas e testadas regularmente** conforme a **política de geração de cópias de segurança** definida.
- Diretrizes para implementação
  - Convém que a política de *backup* seja **estabelecida** para definir os requisitos da organização relativos às cópias de segurança das informações, dos *software* e dos sistemas.
  - Convém que a política de *backup* defina os requisitos para proteção e retenção.
  - Quando da elaboração de um plano de *backup*, convém que os seguintes itens sejam levados em consideração:
    - convém que a **abrangência** (por exemplo, completa ou diferencial) e a **frequência** da geração das cópias de segurança reflitam os requisitos de negócio da organização, além dos **requisitos de segurança da informação** envolvidos e a **criticidade da informação** para a continuidade da operação da organização;
    - convém que as cópias de segurança sejam armazenadas em uma **localidade remota**, a uma distância suficiente para escapar dos danos de um desastre ocorrido no local principal;
    - convém que seja dado um **nível apropriado de proteção física e ambiental** das informações das cópias de segurança;
    - convém que as mídias de *backup* sejam **regularmente testadas** para garantir que elas sejam confiáveis no caso do uso emergencial;
    - em situações onde a confidencialidade é importante, convém que cópias de segurança sejam protegidas por **encriptação**.

12. Segurança nas operações

- **12.4 Registros e monitoramento**
  - Objetivo: Registrar eventos e gerar evidências.
- **12.4.1 Registros de eventos**
- Controle
  - Convém que **registros (*log*) de eventos das atividades do usuário**, exceções, falhas e eventos de segurança da informação sejam **produzidos**, **mantidos** e **analisados criticamente**, a **intervalos regulares**.

- **12.4.2 Proteção das informações dos registros de eventos (*logs*)**
- Controle
  - Convém que as informações dos registros de eventos (*log*) e os seus recursos sejam **protegidos contra acesso não autorizado e adulteração**.

12. Segurança nas operações

- **12.4.3 Registros de eventos (*log*) de administrador e operador**
- Controle
  - Convém que as atividades dos **administradores e operadores do sistema** sejam **registradas** e os registros (*logs*) **protegidos e analisados criticamente**, a intervalos regulares.

- **12.4.4 Sincronização dos relógios**
- Controle
  - Convém que os relógios de todos os sistemas de processamento de informações relevantes, dentro da organização ou do domínio de segurança, sejam sincronizados com uma **única fonte de tempo precisa**.

12. Segurança nas operações

- **12.5 Controle de *software* operacional**
  - Objetivo: Assegurar a integridade dos sistemas operacionais.

- **12.5.1 Instalação de *software* nos sistemas operacionais**
- Controle
  - Convém que **procedimentos** para **controlar a instalação de *software*** em sistemas operacionais sejam implementados.

12. Segurança nas operações

- **12.6 Gestão de vulnerabilidades técnicas**
  - Objetivo: Prevenir a exploração de vulnerabilidades técnicas.
- **12.6.1 Gestão de vulnerabilidades técnicas**
- Controle
  - Convém que informações sobre **vulnerabilidades técnicas** dos sistemas de informação em uso sejam obtidas em tempo hábil; convém que a exposição da organização a estas vulnerabilidades seja **avaliada** e que sejam tomadas as **medidas apropriadas** para lidar com os riscos associados.
- Diretrizes para implementação
  - Um **inventário completo** e atualizado dos ativos de informação é um **pré-requisito** para uma **gestão efetiva de vulnerabilidade técnica**. Informação especifica para o apoio à gestão de vulnerabilidade técnica inclui o fornecedor de *software*, o número da versão, o *status* atual de desenvolvimento (por exemplo, quais *software* estão instalados e em quais sistemas), e a(s) pessoa(s) na organização responsável(is) pelos *software*.

12. Segurança nas operações

- **12.6 Gestão de vulnerabilidades técnicas (continuação)**
- Diretrizes para implementação (continuação)
  - Convém que **seja tomada ação apropriada**, no **devido tempo**, como resposta às potenciais vulnerabilidades técnicas identificadas;
  - Convém que a organização **defina e estabeleça as funções e responsabilidades associadas à gestão de vulnerabilidades técnicas**, incluindo o **monitoramento de vulnerabilidades, a avaliação de risco de vulnerabilidades, correções, acompanhamento dos ativos e qualquer responsabilidade de coordenação** requerida;
  - Convém que os **recursos de informação** a serem usados para identificar vulnerabilidades técnicas relevantes e para manter a conscientização sobre eles sejam identificados;
  - Convém que seja definido **um prazo** para a reação a notificações de potenciais vulnerabilidades técnicas relevantes;
  - Uma vez que uma vulnerabilidade técnica potencial tenha sido identificada, convém que a organização **avalie os riscos associados e as ações a serem tomadas**; tais ações podem requerer o uso de emendas de correções (*patches*) nos sistemas vulneráveis e/ou a aplicação de outros controles;

12. Segurança nas operações

- **12.6 Gestão de vulnerabilidades técnicas (continuação)**
- Diretrizes para implementação (continuação)
  - Se uma **correção for disponibilizada**, convém que **sejam avaliados os riscos associados à sua instalação** (convém que os riscos associados à vulnerabilidade sejam comparados com os riscos de instalação da correção);
  - Convém que as **emendas (*patches*) sejam testadas e avaliadas antes de serem instaladas**, para assegurar a efetividade; quando não existir a disponibilidade de uma correção, convém considerar o uso de outros controles, como:
    - a **desativação de serviços** ou relacionados à vulnerabilidade;
    - a adaptação ou a agregação de controles de acesso, por exemplo, *firewalls*;
    - o aumento do **monitoramento para detectar ou prevenir ataques**;
    - o aumento da **conscientização** sobre a vulnerabilidade;
  - Convém que seja mantido um **registro de auditoria** de todos os procedimentos realizados;
  - Convém que processo de gestão de vulnerabilidades técnicas seja **monitorado e avaliado regularmente;**
  - Recomenda-se contemplar em primeiro lugar os sistemas de **altos riscos**;
  - Convém que um processo de gestão de vulnerabilidade técnica eficaz **esteja alinhado com as atividades de gestão de incidentes.**
- Informações adicionais
  - A gestão de vulnerabilidades técnicas pode ser vista como uma subfunção da gestão de mudanças e, como tal, pode aproveitar os procedimentos e processos da gestão de mudanças.

12. Segurança nas operações

- **12.6.2 Restrições quanto à instalação de *software***
- Controle
  - Convém que sejam estabelecidas e implementadas **regras** definindo critérios para a **instalação de *software* pelos usuários**.

- Diretrizes para implementação
  - Convém que a organização defina e crie uma **política** mandatória e restrita sobre quais os tipos de *software* os usuários podem instalar.
  - Convém que o princípio do **privilégio mínimo** seja aplicado. Se certos privilégios forem concedidos, os usuários podem ter a capacidade de instalar *software*. Convém que a **organização identifique quais os tipos de *software* são permitidos instalar** (por exemplo, atualização e segurança de *patches* ao *software* existente), e quais **tipos de instalações são proibidas** (por exemplo, *software* que é usado somente para fins pessoais e *software* cuja possibilidade de ser potencialmente malicioso, é desconhecida ou suspeita).

12. Segurança nas operações

- **12.7 Considerações quanto à auditoria de sistemas da informação**
  - Objetivo: Minimizar o impacto das atividades de auditoria nos sistemas operacionais.

- **12.7.1 Controles de auditoria de sistemas de informação**
- Controle
  - Convém que as atividades e requisitos de auditoria envolvendo a verificação nos sistemas operacionais sejam cuidadosamente planejados e acordados para minimizar interrupção dos processos do negócio.

13. Segurança nas comunicações

- **13.1 Gerenciamento da segurança em redes**
  - Objetivo: Assegurar a proteção das informações em redes e dos recursos de processamento da informação que as apoiam.

- **13.1.1 Controles de redes**
- Controle
  - Convém que as redes sejam gerenciadas e controladas para proteger as informações nos sistemas e aplicações.

- Diretrizes para implementação
  - Convém que controles sejam implementados para garantir a segurança da informação nestas redes, e a proteção dos serviços a elas conectadas, contra acesso não autorizado.

13. Segurança nas comunicações

- **13.1.2 Segurança dos serviços de rede**
- Controle
  - Convém que mecanismos de segurança, níveis de serviço e requisitos de gerenciamento de todos os serviços de rede sejam identificados e incluídos em qualquer **acordo de serviços de rede**, tanto para serviços de rede providos internamente como para terceirizados.

- Diretrizes para implementação
  - Convém que a **capacidade** do provedor dos serviços de rede para gerenciar os serviços acordados de maneira segura seja determinada e monitorados regularmente.

13. Segurança nas comunicações

- **13.1.3 Segregação de redes**
- Controle
  - Convém que grupos de serviços de informação, usuários e sistemas de informação sejam **segregados em redes**.

- Diretrizes para implementação
  - Um método de controlar a segurança da informação em grandes redes é **dividir em diferentes domínios de redes**. A segregação pode ser feita tanto usando diferentes redes físicas quanto usando diferentes redes lógicas (por exemplo, VPN).
  - Convém que o critério para segregação de redes em domínios e o acesso permitido através dos *gateways* seja baseado em uma avaliação dos requisitos de segurança da informação de cada domínio. Convém que a avaliação seja feita de acordo com a **política de controle de acesso**, os **requisitos de acesso**, o **valor e a classificação da informação processada**.

13. Segurança nas comunicações

- **13.2 Transferência de informação**
  - Objetivo: Manter a segurança da informação transferida dentro da organização e com quaisquer entidades externas.

- **13.2.1 Políticas e procedimentos para transferência de informações**
- Controle
  - Convém que **políticas, procedimentos e controles de transferências formais** sejam estabelecidos para proteger a transferência de informações, por meio do uso de todos os tipos de recursos de comunicação.

- **13.2.2 Acordos para transferência de informações**
- Controle
  - Convém que sejam estabelecidos **acordos para transferência segura de informações** do negócio entre a organização e as partes externas.

13. Segurança nas comunicações

- **13.2.3 Mensagens eletrônicas**
- Controle
  - Convém que as informações que trafegam em mensagens eletrônicas sejam adequadamente protegidas.

- **13.2.4 Acordos de confidencialidade e não divulgação**
- Controle
  - Convém que os requisitos para confidencialidade ou acordos de não divulgação que reflitam as necessidades da organização para a proteção da informação sejam identificados, analisados criticamente e documentados.
- Diretrizes para implementação
  - Convém que os **acordos de confidencialidade e de não divulgação** considerem os requisitos para proteger as **informações confidenciais**. Acordos de confidencialidade ou não divulgação são aplicáveis às partes externas ou aos funcionários da organização. Convém que os seguintes elementos sejam considerados:
    - uma **definição da informação a ser protegida** (por exemplo, informação confidencial);
    - o **tempo de duração** esperado de um acordo, incluindo situações onde a confidencialidade tenha que ser mantida indefinidamente;
    - uso **permitido** da informação confidencial;
    - **ações** esperadas a serem tomadas no **caso de uma violação deste acordo**.

14. Aquisição, desenvolvimento e manutenção de sistemas

- **14.1 Requisitos de segurança de sistemas de informação**
  - Objetivo: Garantir que a segurança da informação seja parte **integrante** de todo o **ciclo de vida** dos **sistemas de informação**. Isto também inclui os requisitos para sistemas de informação que fornecem serviços sobre as redes públicas.

- **14.1.1 Análise e especificação dos requisitos de segurança da informação**
- Controle
  - Convém que os requisitos relacionados à segurança da informação sejam **incluídos nos requisitos para novos sistemas de informação** ou melhorias dos sistemas de informação existentes.

- Informações adicionais
  - A **ISO/IEC 27005** e a **ISO 31000** fornecem diretrizes sobre o uso de processos de gestão de riscos, para identificar controles que atendam aos requisitos de segurança da informação.

14. Aquisição, desenvolvimento e manutenção de sistemas

- **14.1.2 Serviços de aplicação seguros em redes públicas**
- Controle
  - Convém que as informações envolvidas nos serviços de aplicação que transitam sobre redes públicas sejam protegidas de atividades fraudulentas, disputas contratuais e divulgação e modificações não autorizadas.

- **14.1.3 Protegendo as transações nos aplicativos de serviços**
- Controle
  - Convém que informações envolvidas em transações nos aplicativos de serviços sejam protegidas para prevenir transmissões incompletas, erros de roteamento, alteração não autorizada da mensagem, divulgação não autorizada, duplicação ou reapresentação da mensagem não autorizada.

14. Aquisição, desenvolvimento e manutenção de sistemas

- **14.2 Segurança em processos de desenvolvimento e de suporte**
  - Objetivo: Garantir que a **segurança da informação** esteja **projetada e implementada** no **ciclo de vida de desenvolvimento dos sistemas de informação**.

- **14.2.1 Política de desenvolvimento seguro**
- Controle
  - Convém que **regras** para o desenvolvimento de sistemas e *software* sejam estabelecidas e aplicadas aos desenvolvimentos realizados dentro da organização.

- **14.2.2 Procedimentos para controle de mudanças de sistemas**
- Controle
  - Convém que as **mudanças** em sistemas no ciclo de vida de desenvolvimento sejam **controladas** utilizando **procedimentos formais** de controle de mudanças.

14. Aquisição, desenvolvimento e manutenção de sistemas

- **14.2.3 Análise crítica técnica das aplicações após mudanças nas plataformas operacionais**
- Controle
  - Quando plataformas operacionais forem modificadas, convém que as aplicações críticas de negócio sejam **analisadas criticamente e testadas** para garantir que não haverá qualquer impacto adverso na operação da organização ou na segurança.

- **14.2.4 Restrições sobre mudanças em pacotes de *software***
- Controle
  - Convém que modificações em pacotes de *software* sejam desencorajadas e estejam limitadas às mudanças necessárias, e todas as **mudanças sejam estritamente controladas**.

- **14.2.5 Princípios para projetar sistemas seguros**
- Controle
  - Convém que **princípios para projetar sistemas seguros sejam estabelecidos, documentados, mantidos e aplicados** para qualquer implementação de sistemas de informação.

14. Aquisição, desenvolvimento e manutenção de sistemas

- **14.2.6 Ambiente seguro para desenvolvimento**
- Controle
  - Convém que as organizações estabeleçam e protejam adequadamente ambientes seguros de desenvolvimento, para os esforços de integração e desenvolvimento de sistemas, que cubram todo o ciclo de vida de desenvolvimento de sistema.

- **14.2.7 Desenvolvimento terceirizado**
- Controle
  - Convém que a organização **supervisione** e **monitore** as atividades de desenvolvimento de **sistemas terceirizado**.

14. Aquisição, desenvolvimento e manutenção de sistemas

- **14.2.8 Teste de segurança do sistema**
- Controle
  - Convém que os **testes das funcionalidades de segurança** sejam realizados durante o desenvolvimento de sistemas.

- **14.2.9 Teste de aceitação de sistemas**
- Controle
  - Convém que programas de **testes de aceitação** e **critérios relacionados** sejam estabelecidos para **novos sistemas de informação, atualizações e novas versões**.

14. Aquisição, desenvolvimento e manutenção de sistemas

- **14.3 Dados para teste**
  - Objetivo: Assegurar a proteção dos dados usados para teste.

- **14.3.1 Proteção dos dados para teste**
- Controle
  - Convém que os **dados de teste** sejam selecionados com cuidado, **protegidos** e **controlados**.

- Diretrizes para implementação
  - Convém que seja **evitado**, para **propósitos de teste**, o uso de bancos de dados operacionais que contenham **informação de identificação pessoal** ou qualquer outra **informação confidencial**. Se a informação de identificação pessoal ou outras informações sensíveis forem utilizadas com o propósito de teste, convém que todos os detalhes e conteúdos sejam **protegidos contra remoção ou modificação**.

15. Relacionamento na cadeia de suprimento

- **15.1 Segurança da informação na cadeia de suprimento**
  - Objetivo: Garantir a proteção dos ativos da organização que que são acessados pelos fornecedores.

- **15.1.1 Política de segurança da informação no relacionamento com os fornecedores**
- Controle
  - Convém que os requisitos de segurança da informação para mitigar os riscos associados com o acesso dos fornecedores aos ativos da organização sejam acordados com o fornecedor e documentados.

15. Relacionamento na cadeia de suprimento

- **15.1.2 Identificando segurança da informação nos acordos com fornecedores**
- Controle
  - Convém que todos os requisitos de segurança da informação relevantes sejam **estabelecidos e acordados com cada fornecedor** que possa acessar, processar, armazenar, comunicar ou prover componentes de infraestrutura de TI para as informações da organização.

- **15.1.3 Cadeia de suprimento na tecnologia da informação e comunicação**
- Controle
  - Convém que acordos com fornecedores incluam **requisitos** para contemplar os **riscos de segurança da informação** associados à cadeia de suprimento de produtos e serviços de tecnologia da informação e comunicação.

15. Relacionamento na cadeia de suprimento

- **15.2 Gerenciamento da entrega do serviço do fornecedor**
  - Objetivo: Manter um **nível acordado** de segurança da informação e de entrega de serviços em consonância com os acordos com fornecedores.

- **15.2.1 Monitoramento e análise crítica de serviços com fornecedores**
- Controle
  - Convém que as organizações **monitorem, analisem criticamente e auditem**, a intervalos **regulares**, a entrega dos **serviços executados pelos fornecedores**.

- **15.2.2 Gerenciamento de mudanças para serviços com fornecedores**
- Controle
  - Convém que mudanças no provisionamento dos serviços pelos fornecedores, incluindo manutenção e melhoria das políticas de segurança da informação, dos procedimentos e controles existentes, sejam gerenciadas, levando-se em conta a **criticidade das informações do negócio**, **dos sistemas e processos envolvidos, e a reavaliação de riscos.**

16. Gestão de incidentes de segurança da informação

- **16.1 Gestão de incidentes de segurança da informação e melhorias**
  - Objetivo: Assegurar um enfoque **consistente** e **efetivo** para gerenciar os **incidentes de segurança da informação**, incluindo a **comunicação** sobre fragilidades e eventos de segurança da informação.

- **16.1.1 Responsabilidades e procedimentos**
- Controle
  - Convém que responsabilidades e procedimentos de gestão sejam estabelecidos para assegurar **respostas rápidas, efetivas e ordenadas aos incidentes de segurança da informação**.

- Informações adicionais
  - Diretriz detalhada em gestão de incidentes de segurança da informação é fornecida na **ISO/IEC 27035**.

16. Gestão de incidentes de segurança da informação

- **16.1.2 Notificação de eventos de segurança da informação**
- Controle
  - Convém que os eventos de segurança da informação sejam relatados por meio dos canais de gestão, o mais rapidamente possível.

- Diretrizes para implementação
  - Convém que todos os funcionários e partes externas sejam alertados sobre sua **responsabilidade de notificar qualquer evento de segurança da informação** o **mais rapidamente possível**. Convém que eles também estejam cientes do procedimento para notificar os eventos de segurança da informação e do **ponto de contato**, ao qual os eventos devem ser notificados.

16. Gestão de incidentes de segurança da informação

- **16.1.3 Notificando fragilidades de segurança da informação**
- Controle
  - Convém que os funcionários e partes externas que usam os sistemas e serviços de informação da organização sejam instruídos a **notificar e registrar quaisquer fragilidades de segurança da informação**, observada ou suspeita, nos sistemas ou serviços.

- Diretrizes para implementação
  - Convém que todos os funcionários e partes externas notifiquem essas questões para o ponto de contato, o mais rápido possivel, de forma a prevenir incidentes de segurança da informação.

16. Gestão de incidentes de segurança da informação

- **16.1.4 Avaliação e decisão dos eventos de segurança da informação**
- Controle
  - Convém que os eventos de segurança da informação sejam avaliados e seja decidido se eles são classificados como incidentes de segurança da informação.

- **16.1.5 Resposta aos incidentes de segurança da informação**
- Controle
  - Convém que incidentes de segurança da informação sejam **reportados** de acordo com **procedimentos documentados**.

- Diretrizes para implementação
  - Convém que incidentes de segurança da informação sejam **reportados** para um ponto de contato definido e outras pessoas relevantes da organização, ou ainda, partes externas.

16. Gestão de incidentes de segurança da informação

- **16.1.6 Aprendendo com os incidentes de segurança da informação**
- Controle
  - Convém que os conhecimentos obtidos da análise e resolução dos incidentes de segurança da informação sejam usados para reduzir a probabilidade ou o impacto de incidentes futuros.

- **16.1.7 Coleta de evidências**
- Controle
  - Convém que a organização defina e aplique procedimentos para a **identificação, coleta, aquisição e preservação das informações, as quais podem servir como evidências**.

- Informações adicionais
  - A **ISO/IEC 27037** fornece diretrizes para identificação, coleta, aquisição e preservação de evidências digitais.

17. Aspectos da segurança da informação na gestão da continuidade do negócio

- **17.1 Continuidade da segurança da informação**
  - Objetivo: Convém que a **continuidade da segurança da informação** seja contemplada nos sistemas de gestão da continuidade do negócio da organização

- **17.1.1 Planejando a continuidade da segurança da informação**
- Controle
  - Convém que a organização determine seus requisitos para a segurança da informação e a continuidade da gestão da segurança da informação em situações adversas, por exemplo, durante uma crise ou desastre.

17. Aspectos da segurança da informação na gestão da continuidade do negócio

- **17.1.2 Implementando a continuidade da segurança da informação**
- Controle
  - Convém que a organização **estabeleça, documente, implemente e mantenha processos**, **procedimentos e controles** para assegurar o nível requerido de **continuidade para a segurança da informação**, durante uma situação adversa.

- **17.1.3 Verificação, análise crítica e avaliação da continuidade da segurança da informação**
- Controle
  - Convém que a organização verifique os **controles de continuidade da segurança da informação**, estabelecidos e implementados, a **intervalos regulares**, para garantir que eles sejam **válidos e eficazes em situações adversas**.

17. Aspectos da segurança da informação na gestão da continuidade do negócio

- **17.2 Redundâncias**
  - Objetivo: Assegurar a **disponibilidade** dos recursos de processamento da informação.

- **17.2.1 Disponibilidade dos recursos de processamento da informação**
- Controle
  - Convém que os recursos de processamento da informação sejam implementados com **redundância** suficiente para atender aos **requisitos de disponibilidade**.

18. Conformidade

- **18.1 Conformidade com requisitos legais e contratuais**
  - Objetivo: Evitar violação de quaisquer obrigações legais, estatutárias, regulamentares ou contratuais relacionadas à segurança da informação e de quaisquer requisitos de segurança.

- **18.1.1 Identificação da legislação aplicável e de requisitos contratuais**
- Controle
  - Convém que todos os **requisitos legislativos estatutários, regulamentares e contratuais** pertinentes e o enfoque da organização para atender a esses requisitos sejam explicitamente **identificados**, **documentados** e **mantidos atualizados** para cada sistema de informação da organização.

18. Conformidade

- **18.1.2 Direitos de propriedade intelectual**
- Controle
  - Convém que procedimentos apropriados sejam implementados para garantir a **conformidade** com os **requisitos legislativos, regulamentares e contratuais** relacionados aos direitos de propriedade intelectual, e sobre o uso de produtos de *software* proprietários.

- **18.1.3 Proteção de registros**
- Controle
  - Convém que registros sejam **protegidos** contra **perda, destruição, falsificação, acesso não autorizado e liberação não autorizada**, de acordo com os requisitos regulamentares, estatutários, contratuais e do negócio.

18. Conformidade

- **18.1.4 Proteção e privacidade de informações de identificação pessoal**
- Controle
  - Convém que a **privacidade e a proteção dos dados pessoais** sejam asseguradas conforme requerido por **legislação e regulamentação** pertinente, quando aplicável.

- Diretrizes para implementação
  - Convém que uma **política** de dados da organização para proteção e privacidade da informação de identificação pessoal seja desenvolvida e implementada. Esta política deve ser **comunicada a todas as pessoas** envolvidas no **processamento de informação de identificação pessoal**.

- Informações adicionais
  - A **ISO/IEC 29100** fornece uma estrutura de alto nível para a proteção da informação de identificação pessoal, no âmbito dos sistemas de tecnologia da comunicação e informação.

18. Conformidade

- **18.1.5 Regulamentação de controles de criptografia**
- Controle
  - Convém que controles de criptografia sejam usados em conformidade com todas as leis, acordos, legislação e regulamentações pertinentes.

18. Conformidade

- **18.2 Análise crítica da segurança da informação**
  - Objetivo: Assegurar que a segurança da informação esteja implementada e operada de acordo com as políticas e procedimentos da organização.

- **18.2.1 Análise crítica independente da segurança da informação**
- Controle
  - Convém que o enfoque da organização para gerenciar a segurança da informação e a sua implementação seja **analisado criticamente**, de forma **independente**, a **intervalos planejados**, ou quando ocorrerem **mudanças significativas**.

18. Conformidade

- **18.2.2 Conformidade com as políticas e procedimentos de segurança da informação**
- Controle
  - Convém que os gestores analisem criticamente, a **intervalos regulares**, a **conformidade** dos **procedimentos** e do processamento da informação, dentro das suas áreas de responsabilidade, com as **normas e políticas de segurança** e quaisquer **outros requisitos de segurança da informação**.

- **18.2.3 Análise crítica da conformidade técnica**
- Controle
  - Convém que os sistemas de informação sejam analisados criticamente, a intervalos regulares, para verificar a **conformidade** com as **normas e políticas de segurança da informação** da organização.

Referências bibliográficas

- ISO/IEC 27001 Tecnologia da informação - Técnicas de segurança – Sistema de Gestão da segurança da informação - Requisitos.
- ISO/IEC 27002 Tecnologia da informação - Técnicas de segurança - Código de prática para controles de segurança da informação.