ISO 27001: Controles de Segurança (A.5 a A.9)

1. Introdução aos Controles da ISO 27001

A ISO/IEC 27001 organiza seus controles em 14 domínios (Anexo A da norma), cobrindo desde políticas e governança até segurança física, comunicações, continuidade de negócios e conformidade.

Nesta aula, aprofundaremos os controles A.5 a A.9, que estão na base de qualquer Sistema de Gestão de Segurança da Informação (SGSI). Eles tratam de políticas, organização, pessoas, ativos e acesso, ou seja, os elementos mais fundamentais para garantir proteção consistente.

A.5 – Políticas de Segurança da Informação

Finalidade: garantir que haja diretrizes formais que orientem todas as ações de segurança da informação na organização.

Requisitos principais:

- A política deve ser aprovada pela direção da empresa.
- Precisa ser comunicada a todos os colaboradores.
- Deve ser revisada periodicamente, geralmente a cada 12 meses ou quando houver mudanças significativas no ambiente.

A.5 – Políticas de Segurança da Informação

Conteúdo esperado de uma política:

- Objetivos da segurança da informação.
- Definição de responsabilidades.
- Regras gerais para proteção de dados e uso de recursos.
- Direcionamento para documentos complementares (ex.: política de senhas, política de backup).

Exemplo prático: uma universidade que define regras claras para o uso de e-mails institucionais e para o armazenamento de documentos acadêmicos em nuvem.

A.6 – Organização da Segurança da Informação

Finalidade: definir responsabilidades e garantir que a gestão da segurança não fique restrita a apenas uma pessoa ou área.

Principais pontos:

- Papéis e responsabilidades: todos devem saber quais são suas atribuições em relação à segurança (ex.: administradores de sistema, gestores de dados, usuários finais).
- Segregação de funções: reduzir riscos de fraude ou abuso. Ex.: quem aprova pagamentos não deve ser a mesma pessoa que executa as transações.

A.6 – Organização da Segurança da Informação

- Relacionamento com terceiros: fornecedores e parceiros também devem seguir diretrizes de segurança (contratos com cláusulas de confidencialidade e requisitos de proteção).

Exemplo prático: uma empresa de e-commerce que terceiriza o datacenter exige do provedor certificação ISO 27001 e auditorias regulares de conformidade.

A.7 – Segurança em Recursos Humanos

Finalidade: proteger informações em todo o ciclo de vida do vínculo empregatício — antes, durante e após a contratação.

Fases principais:

- Pré-contratação: checagem de antecedentes, inclusão de cláusulas de confidencialidade nos contratos.
- Durante o vínculo: treinamentos periódicos, campanhas de conscientização, regras claras de conduta digital.

A.7 – Segurança em Recursos Humanos

- Pós-desligamento: revogação imediata de acessos, devolução de equipamentos, manutenção de cláusulas de sigilo.
- Importância: a falha humana ainda é uma das principais causas de incidentes de segurança (ex.: phishing, engenharia social).

Exemplo prático: em um hospital, novos funcionários assinam termo de confidencialidade sobre dados de pacientes e recebem treinamento obrigatório em LGPD.

A.8 – Gestão de Ativos

Finalidade: assegurar que todos os ativos de informação sejam identificados, inventariados, classificados e protegidos.

Etapas principais:

- Inventário de ativos: lista atualizada de equipamentos, sistemas, bancos de dados, documentos e até conhecimento humano.
- Classificação da informação: categorização de acordo com criticidade (ex.: público, interno, confidencial, restrito).

A.8 – Gestão de Ativos

- Proprietário do ativo: cada ativo deve ter um responsável que decide como ele pode ser usado, compartilhado e protegido.
- Benefícios: permite priorizar controles de acordo com a importância dos ativos para o negócio.

Exemplo prático: uma startup mantém inventário dos notebooks fornecidos a funcionários, com regras para uso e devolução.

A.9 – Controle de Acesso

Finalidade: restringir o acesso às informações apenas a pessoas autorizadas, conforme suas responsabilidades.

Principais medidas:

- Política de controle de acesso: documento que define princípios gerais, como “mínimo privilégio” e “necessidade de saber”.
- Autenticação: métodos que garantem a identidade do usuário (senhas fortes, tokens, biometria, autenticação multifator).

A.9 – Controle de Acesso

- Autorização: concessão de permissões conforme a função do colaborador.
- Revisão periódica de acessos: checar regularmente se usuários ainda precisam das permissões concedidas.
- Gestão de contas privilegiadas: controles especiais para administradores e superusuários.

Exemplo prático: em um banco, um analista de crédito pode acessar informações financeiras de clientes, mas não consegue alterar registros no sistema principal.

Elaborando uma Política de Segurança

Com base no cenário definido na Aula 04 e nas referências da Aula 03 (PSI) e da ISO 27001 (Aula 04 e Aula 05), cada grupo deverá:

1. Escolher um cenário trabalhado anteriormente (hospital, banco, startup, universidade etc.).

2. Elaborar uma Política de Segurança da Informação cobrindo os seguintes pontos:

- Objetivo da política: por que ela existe e o que busca proteger.
- Escopo de aplicação: quem deve segui-la (funcionários, terceirizados, fornecedores).
- Responsabilidades: papéis das áreas de TI, gestores e usuários.
- Controles mínimos obrigatórios: aplicar conceitos dos domínios A.5 a A.9 (políticas, organização, RH, ativos, acessos).
- Regras práticas para usuários: uso de senhas, acesso a sistemas, cuidados com documentos e dispositivos.

3. Entregar a política em 1 a 2 páginas, com linguagem clara, objetiva e compreensível até para quem não é da área de TI.

4. Preparar um breve resumo para apresentar em sala, destacando como a política escolhida ajuda a reduzir riscos no cenário selecionado.