## DECLARAÇÃO DE APLICABILIDADE

HISTÓRICO DE VERSÕES

|  |  |  |
| --- | --- | --- |
| Data | Edição n.º | Conteúdo |
| 22/12/2021 | 1.0 | Redação Inicial |
| 10/01/2022 | 2.0 | Clarificação dos documentos associados ao método de implementação |
|  |  |  |
|  |  |  |
|  |  |  |

|  |  |
| --- | --- |
| Elaborado por: | Aprovado por: |
| Assinado Por: Rui Alexandre Borba Vitorino (8190479)  Bruno Miguel do Carmo Vieira (8190724)  Gilberto Jorge Da Mota Gomes (8210227)  Data da Assinatura: 10/01/2022 12:20:44 GMT +01:00 Motivo: Aprovo o documento | Assinado Por: AAAAA BBBBB CCCCC DDDDD  (Presidente do Conselho de Administração  Data da Assinatura: 10/01/2021 12:45:04 GMT +01:00  Motivo: Aprovo este documento |

Aviso Legal

**Copyright** **Mercado da Boneca SA - R. Prof. Joaquim Barros Leite, 4610-108 Felgueiras, Portugal**

É expressamente proibida a reprodução, total ou parcial, do conteúdo deste documento, sem prévia autorização escrita emitida pela Mercado da Boneca SA - R. Prof. Joaquim Barros Leite, 4610-108 Felgueiras, Portugal.

Qualquer dúvida ou pedido de informação relativamente ao conteúdo deste documento deverá ser dirigido suporte@mercadodaboneca.pt

# Introdução

A finalidade deste documento é definir quais os controlos que são adequados para implementação na Mercado da Boneca, quais são os objetivos desses controlos e como eles são implementados, além de aprovar os riscos residuais e aprovar formalmente a implementação desses controlos.

Este documento inclui todos os controlos relacionados no Anexo A da norma ISO 27001. Os controlos são aplicáveis a todo o âmbito do Sistema de Gestão da Segurança da Informação (SGSI).

Este documento é aplicável a todos os colaboradores da Mercado da Boneca abrangidos no âmbito do SGSI.

# Aplicabilidade dos controlos

Os seguintes controles do Anexo A da ISO 27001 são aplicáveis:

**Motivo para a seleção/não seleção** - com base nos resultados de avaliação de riscos e das obrigações contratuais e legais

**Método de implementação** - especifique o documento e o controlo técnico ou descreva o processo. Deixe em branco se o controlo for marcado como inaplicável. Se não houver documentos relevantes para o controlo, faça uma breve descrição do processo.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ID | Controlos de acordo com  a norma ISO/IEC 27001 | | Aplicável  Sim/Não | Motivo para a  seleção/não seleção | | | | Método de  implementação | |
| A.5 | **Políticas de segurança da informação** | | | | | | | | |
| **A.5.1** | **Diretrizes da gestão para a segurança da informação**  Objetivos: Proporcionar diretrizes e apoio da gestão para a segurança da informação, de acordo com os requisitos do negócios, leis e regulamentações relevantes. | | | | | | | | |
| A.5.1.1 | Políticas para a  segurança da informação | | Sim | Serve como base para o estabelecimento de procedimentos e responsabilidades que garantem a segurança da informação. Ponto de partida para a gestão dos riscos da segurança da informação. | | | | PQSI - Política Qualidade e Segurança Informação  PSI - Princípios Segurança  Informação | da de da  de da |
| A.5.1.2 | Revisão das políticas para a segurança da informação | | Sim |
| **A.6** | **Organização da segurança da informação** | | | | | | | | |
| **A.6.1** | **Organização interna**  Objetivos: Estabelecer um modelo de refª de gestão para iniciar e controlar a implementação e operação de segurança da informação dentro da organização | | | | | | | | |
| A.6.1.1 | Papéis e  responsabilidades da segurança da informação | | Sim | Necessidade controlo da  informação. | de | assegurar segurança | o da | MF - Manual Funções | de |
| A.6.1.2 | Segregação de funções | | Sim | Princípio básico de um sistema de controlo interno que consiste na separação de funções potencialmente conflituantes, nomeadamente de autorização, aprovação, execução, controlo e  contabilização das operações. | | | | MF - Manual de Funções  Controlo dos Documentos e Registos | |
| A.6.1.3 | Contacto autoridades competentes | com | Sim | A Mercado da Boneca mantem contacto regular com autoridades competentes, como sejam o GNS – Gabinete Nacional de Segurança. | | | | Relatórios Auditorias; Documentação trocada. | de |
| A.6.1.4 | Contactos com grupos  de interesse especial | | Sim |
| A.6.1.5 | Segurança da informação na gestão de projeto | | Sim | Necessidade de segurança da informação associada ao desenvolvimento de novos  projetos. | | | | Plano de projeto; Relatórios implementação. | De |
| **A.6.2** | **Dispositivos móveis e teletrabalho**  Objetivos: Assegurar a segurança no teletrabalho e na utilização de dispositivos móveis | | | | | | | | |
| A.6.2.1 | Política de dispositivos móveis | | Sim | Necessidade de controlo de utilização de dispositivos móveis dentro da rede da empresa. | | | | Os riscos e controlos são identificados durante a avaliação e o tratamento de riscos e documentados no [RAR - Relatório de  avaliação de riscos]. | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ID | Controlos de acordo com  a norma ISO/IEC 27001 | | Aplicável  Sim/Não | Motivo para a  seleção/não seleção | | | Método de  Implementação | |
| A.6.2.2 | Teletrabalho | | Sim | COVID-19 | | | - | |
| **A.7** | **Segurança na gestão de recursos humanos** | | | | | | | |
| **A.7.1** | **Antes da relação contratual**  Objetivos: Assegurar que os colaboradores e prestadores de serviço compreendem as suas responsabilidades, e que são adequados para as funções para as quais estão a ser considerados | | | | | | | |
| A.7.1.1 | Verificação de credenciais e referências | | Sim | Necessidade aumentar o nível de controlo na admissão de novos colaboradores. | | | PQ Gestão Recursos Humanos, MF - manual  funções. | de  de |
| A.7.1.2 | Termos e condições da relação contratual | | Sim | Necessidade de responsabilidades colaboradores e  serviços. | assegurar  prestadores | as dos de | Contrato de trabalho, Gestão de Recursos Humanos | |
| **A.7.2** | **Durante a relação contratual**  Objetivos: Assegurar que os colaboradores e prestadores estão conscientes e cumprem as suas responsabilidades de segurança da informação | | | | | | | |
| A.7.2.1 | Responsabilidade gestão | da | Sim | Assegurar que as políticas estabelecidas pela organização são cumpridas. | | | MF - Manual  funções. Contrato confidencialidade | de de |
| A.7.2.2 | Consciencialização,  educação e formação em segurança da informação | | Sim | Ações de formação | |
| A.7.2.3 | Procedimento disciplinar | | Sim | PQSI - Política Qualidade e Segurança Informação  PSI - Princípios Segurança  Informação | da de da  de da |
| **A.7.3** | **Cessação e alteração da relação contratual**  Objetivos: Proteger os interesses da organização na cessação e alteração da relação contratual | | | | | | | |
| A.7.3.1 | Responsabilidades na cessação ou alteração da  relação contratual | | Sim | Clausulas de confidencialidade após cessação de contrato. | | | Gestão de Recursos Humanos  Contrato de trabalho. | |
| A.8 | **Gestão de ativos** | |  |  | | |  | |
| **A.8.1** | **Responsabilidade pelos ativos**  Objetivos: Identificar os ativos da organização e definir responsabilidades de proteção apropriadas | | | | | | | |
| A.8.1.1 | Inventário de ativos | | Sim | Identificação dos ativos associados com a informação e os recursos de processamento de informação. | | | Tabela avaliação de riscos | de |
| A.8.1.2 | Responsabilidade pelos  ativos | | Sim | Necessidade de atribuição de  responsável dos ativos. | | |
| A.8.1.3 | Utilização aceitável  ativos | de | Sim | Carência de controlo de meios de  utilização aceitáveis dos ativos da | | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ID | Controlos de acordo com  a norma ISO/IEC 27001 | | | | | Aplicável  Sim/Não | Motivo para a  seleção/não seleção | | | | Método de  implementação | | |
|  |  | | | | |  | empresa. | | | |  | | |
| A.8.1.4 | Devolução de ativos | | | | | Sim | Colaboradores e utilizadores externos usufruem dos ativos da empresa e devem devolver os mesmos no fim do contrato ou prestação de serviço. | | | | Gestão Recursos Humanos | | de |
| **A.8.2** | **Classificação da informação**  Objetivos: Assegurar que a informação recebe um nível adequado de proteção, de acordo com a sua importância para a organização | | | | | | | | | | | | |
| A.8.2.1 | Classificação informação | | |  | da | Sim | Atribuição de um nível de valor, importância, e sensibilidade à  informação da empresa. | | | | Controlo dos Documentos e Registos,  PQSI - Política da Qualidade e de  Segurança da Informação  PSI - Princípios de Segurança de  Informação | | |
| A.8.2.2 | Etiquetagem  informação | | |  | da | Sim | Criação de procedimento para a  classificação da informação. | | | |
| A.8.2.3 | Manuseamento ativos | | |  | de | Sim | Colaboradores e entidades externas apenas acedem à informação autorizada de acordo com a classificação da informação. | | | |
| **A.8.3** | **Manuseamento de suportes de dados**  Objetivos: Prevenir a divulgação não autorizada, modificação, remoção ou eliminação da informação armazenada em suportes de dados | | | | | | | | | | | | |
| A.8.3.1 | Gestão de suportes de  dados amovíveis | | | | | Sim | Necessidade de controlo de utilização, eliminação e transporte de suportes de dados amovíveis da empresa. | | | | PQSI - Política Qualidade e Segurança Informação  PSI - Princípios  Segurança Informação | | da de da  de da |
| A.8.3.2 | Eliminação de suportes  de dados | | | | | Sim |
| A.8.3.3 | Transporte de suportes de dados | | | | | Sim |
| **A.9** | **Controlo de acessos** | | | | |  |  | | | |  | | |
| **A.9.1** | **Requisitos de negócio para controlo de acesso**  Objetivos: Limitar o acesso à informação e aos recursos de processamento de informação | | | | | | | | | | | | |
| A.9.1.1 | Política de controlo de  acessos | | | | | Sim | Necessidade conformidade acessos à rede. | de de | assegurar controlo | a nos | PSEG -  Segurança | Plano | De |
| A.9.1.2 | Acesso a redes  serviços de rede | | | e | a | Sim |
| **A.9.2** | **Gestão de acesso de utilizadores**  Objetivos: Assegurar o acesso de utilizadores autorizados e prevenir o acesso não autorizado a sistemas e serviços | | | | | | | | | | | | |
| A.9.2.1 | Registo e cancelamento  de utilizador | | | | | Sim | Necessidade de implementar um processo formal de controlo e registo de utilizadores. | | | | PSEG -  Segurança | Plano | De |
| A.9.2.2 | Disponibilização de  acesso aos utilizadores | | | | | Sim |
| A.9.2.3 | Gestão | de | direitos | | de | Sim |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ID | Controlos de acordo com  a norma ISO/IEC 27001 | | Aplicável  Sim/Não | Motivo para a  seleção/não seleção | | Método de  implementação | | |
|  | acesso privilegiado | |  |  | |  | | |
| A.9.2.4 | Gestão da secreta autenticação  utilizadores | informação  para de | Sim |
| A.9.2.5 | Revisão de direitos de  acesso de utilizadores | | Sim |
| A.9.2.6 | Remoção ou ajuste de  direitos de acesso | | Sim |
| **A.9.3** | **Responsabilidades dos utilizadores**  Objetivos: Tornar os utilizadores responsáveis pela proteção da sua informação de autenticação | | | | | | | |
| A.9.3.1 | Utilização de informação secreta para  autenticação | | Sim | Necessidade de aumento no nível  de segurança no acesso a informação secreta. | | PSEG -  Segurança | Plano | de |
| **A.9.4** | **Controlo de acesso a sistemas e aplicações**  Objetivos: Prevenir o acesso não autorizado a sistemas e aplicações | | | | | | | |
| A.9.4.1 | Restrição de acesso à | | Sim |  | |  |  |  |
| informação | |  | |  |  |  |
| A.9.4.2 | Procedimentos seguros  de início de sessão | | Sim | Necessidade de aumento no nível de segurança no acesso a informação secreta. | | PSEG -  Segurança | Plano | de |
| A.9.4.3 | Sistema de  senhas | gestão de | Sim |
| A.9.4.4 | Utilização de programas | | Sim |  | |  |  |  |
| utilitários privilegiados | |  | |  |  |  |
|  |  | |  |  |  | Código fonte reside | | |
|  |  | |  |  |  | apenas nos servidores | | |
| A.9.4.5 | Controlo de acesso ao código fonte de  programas | | Sim | Garantia de integridade propriedade intelectual | e | de desenvolvimento e armazenamento  centralizado, que | | |
|  |  | |  |  |  | possuem controle de | | |
|  |  | |  |  |  | acessos. | | |
| **A.10** | **Criptografia** | |  |  | |  | | |
| **A.10.1** | **Controlo criptográficos**  Objetivos: Assegurar a utilização adequada e eficaz de criptografia para proteger a confidencialidade, autenticidade e/ou integridade | | | | | | | |
|  |  | |  |  |  | MF - Manual de | | |
| A.10.1.1 | Política sobre a utilização de controlos  criptográficos | | Sim | Garantia de confidencialidade integridade da informação | e | Funções;  PCS - Política de Cópias de Segurança; | | |
|  |  | |  |  |  | Outros. | | |
| A.10.1.2 | Gestão de chaves | | Sim | Garantia de acesso à informação | | PCS - Política de Cópias de Segurança;  Outros. | | |
| **A.11** | **Segurança fisíca e ambiental** | | | | | | | |
| **A.11.1** | **Áreas seguras** | | | | | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ID | Controlos de acordo com  a norma ISO/IEC 27001 | Aplicável  Sim/Não | Motivo para a  seleção/não seleção | Método de  Implementação |
|  | Objetivos: Prevenir o acesso físico não autorizado, os danos e as interferências na informação e nos  recursos de processamento de informação da organização | | | |
| A.11.1.1 | Perímetro de segurança  física | Sim | Necessidade de assegurar a segurança física e ambiental na Mercado da Boneca. | PSEG - Plano de Segurança;  Controlo dos Documentos e Registos |
| A.11.1.2 | Controlo de entrada  física | Sim |
| A.11.1.3 | Segurança em  escritórios, salas e instalações | Sim |
| A.11.1.4 | Proteção contra ameaças externas e  ambientais | Sim |
| A.11.1.5 | Trabalhar em áreas  seguras | Sim |
| A.11.1.6 | Áreas de carga e  descarga | Sim |
| **A.11.2** | **Equipamento**  Objetivos: Prevenir a perda, dano, furto ou comprometimento de ativos e interrupção das operações da organização | | | |
| A.11.2.1 | Colocação e proteção de  equipamentos | Sim | Necessidade de salvaguardar a proteção dos equipamentos e da sua informação. | PSEG - Plano de Segurança;  PQSI - Política da Qualidade e de  Segurança da Informação  PSI - Princípios de Segurança de Informação |
| A.11.2.2 | Serviços básicos de  suporte | Sim |
| A.11.2.3 | Segurança da cablagem | Sim |
| A.11.2.4 | Manutenção de  equipamentos | Sim |
| A.11.2.5 | Remoção de ativos | Sim |
| A.11.2.6 | Segurança de equipamentos e ativos  fora das instalações | Sim |
| A.11.2.7 | Eliminação e reutilização seguras de  equipamentos | Sim |
| A.11.2.8 | Equipamento de utilizador não vigiado | Sim | Necessidade de salvaguardar a proteção dos equipamentos e da sua informação. |
| A.11.2.9 | Política de secretária limpa e ecrã limpo | Sim |
| **A.12** | **Segurança de operações** |  |  |  |
| **A.12.1** | **Procedimentos e responsabilidades operacionais**  Objetivos: Assegurar a operação correta e segura dos recursos de processamento de informação | | | |
| A.12.1.1 | Procedimentos de operação documentados | Sim | Necessidade de assegurar a operação correta e segura de todo | Procedimentos operacionais para a |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ID | Controlos de acordo com  a norma ISO/IEC 27001 | Aplicável  Sim/Não | Motivo para a  seleção/não seleção | Método de  implementação |
| A.12.1.2 | Gestão de alterações | Sim | o processamento de informação. | gestão de TI;  PSEG - Plano de Segurança |
| A.12.1.3 | Gestão da capacidade | Sim |
| A.12.1.4 | Separação entre  ambientes de desenvolvimento, teste e de produção | Sim |
| **A.12.2** | **Proteção contra código malicioso**  Objetivos: Assegurar que a informação e os recursos de processamento de informação estão protegidos contra código malicioso | | | |
| A.12.2.1 | Controlo contra código malicioso | Sim | Necessidade de assegurar que a informação e os recursos de processamento de informação estão protegidos contra código  malicioso. | PSEG - Plano de Segurança |
| **A.12.3** | **Salvaguarda de dados**  Objetivos: Proteger contra a perda de dados | | | |
| A.12.3.1 | Salvaguarda de informação | Sim | Necessidade de fazer backup para proteger a informação | PQSI - Política da Qualidade e de  Segurança da Informação  PSI - Princípios de  Segurança de Informação |
| **A.12.4** | **Registos de eventos e monitorização**  Objetivos: Registar eventos e gerar evidências | | | |
| A.12.4.1 | Registos de eventos | Sim | Necessidade de registar e monitorizar eventos. | Logs  Gestão de  Incidentes de Sistemas de Informação |
| A.12.4.2 | Proteção da informação  registada | Sim | Política de Cópias de Segurança; PSEG - Plano de  Segurança; Logs;  HMAC (ADSS). |
| A.12.4.3 | Registos de  administrador e de operador | Sim |
| A.12.4.4 | Sincronização de relógio | Sim | Sincronização com Observatório Astronómico de Lisboa  e NTP Server |
| **A.12.5** | **Controlo de software em sistemas de produção**  Objetivos: Assegurar a integridade dos sistemas de produção | | | |
| A.12.5.1 | Instalação de software  nos sistemas de | Sim | Necessidade de assegurar a  integridade dos sistemas de | Instrução de trabalho |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ID | Controlos de acordo com  a norma ISO/IEC 27001 | Aplicável  Sim/Não | Motivo para a  seleção/não seleção | Método de  implementação |
|  | produção |  | produção. |  |
| **A.12.6** | **Gestão de vulnerabilidades técnicas**  Objetivos: Prevenir a exploração de vulnerabilidades técnicas | | | |
| A.12.6.1 | Gestão de  vulnerabilidades técnicas | Sim | Necessidade de minimizar as vulnerabilidades técnicas e controlo da instalação de software. | Tabela de ativos |
| A.12.6.2 | Restrições sobre a  instalação de software | Sim | Instrução de trabalho |
| **A.12.7** | **Considerações para auditorias a sistemas de informação**  Objetivos: Minimizar o impacto das atividades de auditoria nos sistemas de produção | | | |
| A.12.7.1 | Controlos de auditoria nos sistemas de informação | Sim | Auditoria de verificação aos sistemas de informação. | Checklist para auditorias periódicas |
| **A.13** | **Segurança de comunicações** | | |  |
| **A.13.1** | **Gestão da segurança da rede**  Objetivos: Assegurar a proteção da informação nas redes e nos recursos de processamento de informação | | | |
| A.13.1.1 | Controlos de rede | Sim | As redes devem ser controladas para proteger a informação | PSEG - Plano de Segurança |
| A.13.1.2 | Segurança de serviços de  rede | Sim |
| A.13.1.3 | Segregação de redes | Sim |
| **A.13.2** | **Transferência de informação**  Objetivos: Manter a segurança da informação transferida dentro da organização e para qualquer entidade externa | | | |
| A.13.2.1 | Políticas e  procedimentos de  transferência de informação | Sim | Necessidade de regular a transferência da informação. | PSEG - Plano de Segurança |
| A.13.2.2 | Acordos sobre transferência de  informação | Sim | Necessidade de controlar a transferência da informação entre  entidades | Contratos |
| A.13.2.3 | Mensagens eletrónicas | Sim | Necessidade de proteger a informação contida dentro de mensagens eletrónicas de forma apropriada. | PQSI - Política da Qualidade e de  Segurança da Informação  PSI - Princípios de Segurança de Informação  Acordos de  confidencialidade e contratos |
| A.13.2.4 | Acordos de  confidencialidade ou de não divulgação | Sim | Necessidade de restringir ou reservar a divulgação da informação confidencial. |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ID | Controlos de acordo com  a norma ISO/IEC 27001 | Aplicável  Sim/Não | Motivo para a  seleção/não seleção | Método de  implementação |
| **A.14** | **Aquisição, desenvolvimento e manutenção de sistemas** | | |  |
| **A.14.1** | **Requisitos de segurança de sistemas de informação**  Objetivos: Assegurar que a segurança da informação é uma parte integrante dos sistemas de informações ao longo do todo o seu ciclo de vida. Isto inclui também os requisitos para sistemas de informação que prestam serviços através de redes públicas | | | |
| A.14.1.1 | Especificação e análise de requisitos de segurança de informação | Sim | Necessidade de assegurar que a segurança da informação é uma parte integrante dos sistemas de informação ao longo do seu ciclo de vida. | Antivírus, Firewall, uso de criptografia  PSEG - Plano de Segurança |
| A.14.1.2 | Proteger serviços aplicacionais nas redes públicas | Sim |
| A.14.1.3 | Proteger transações de serviços aplicacionais | Sim |
| **A.14.2** | **Segurança no desenvolvimento e nos processos de suporte**  Objetivos: Assegurar que a segurança da informação é concebida e implementada no âmbito do ciclo de vida do desenvolvimento de sistemas de informação | | | |
| A.14.2.1 | Política de  desenvolvimento seguro | Sim | Necessidade de assegurar a segurança da informação no desenvolvimento e manutenções dos sistemas | Plano de projeto; Relatórios de  implementação. |
| A.14.2.2 | Procedimento de  controlo de alterações aos sistemas | Sim | PSEG - Plano de Segurança |
| A.14.2.3 | Revisão técnica de aplicações após alterações na plataforma  de produção | Sim |
| A.14.2.4 | Restrições sobre  alterações em pacotes de software | Sim |
| A.14.2.5 | Princípios de engenharia de sistemas seguros | Sim | Plano de projeto; Relatórios de  implementação. |
| A.14.2.6 | Ambiente de  desenvolvimento seguro | Sim | Desenvolvimento feito em ambiente similar  ao de produção |
| A.14.2.7 | Desenvolvimento subcontratado | Não | Não é prática da empresa a subcontratação de  desenvolvimento | -- |
| A.14.2.8 | Testes de segurança de  sistemas | Sim | Necessidade de assegurar a segurança da informação no desenvolvimento e manutenções  dos sistemas | Plano de projeto; Relatórios de implementação. |
| A.14.2.9 | Testes de aceitação de  sistemas | Sim |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ID | Controlos de acordo com  a norma ISO/IEC 27001 | Aplicável  Sim/Não | Motivo para a  seleção/não seleção | Método de  implementação |
| **A.14.3** | **Dados de teste**  Objetivos: Assegurar a proteção dos dados usados para testes | | | |
| A.14.3.1 | Proteção de dados de teste | Sim | Necessidade de assegurar a segurança da informação | Desenvolvimento feito em ambiente similar  ao de produção |
| **A.15** | **Relações com fornecedores** | | | |
| **A.15.1** | **Segurança da informação nas relações com os fornecedores**  Objetivos: Assegurar a proteção dos ativos da organização que estão a cessíveis aos fornecedores | | | |
| A.15.1.1 | Política da segurança da informação para as relações com fornecedores | Sim | Necessidade de assegurar que a informação e os ativos estão seguros nas relações com os fornecedores. | Contrato de  confidencialidade |
| A.15.1.2 | Endereçar a segurança nos acordos com os fornecedores | Sim |
| A.15.1.3 | Cadeia de fornecimento de tecnologias de informação e  comunicação | Sim |
| **A.15.2** | **Gestão da entrega de serviços pelos fornecedores**  Objetivos: Manter o nível acordado de segurança da informação e de disponibilidade de serviços, alinhado com os acordos com os fornecedores | | | |
| A.15.2.1 | Monitorizar e rever  serviços de fornecedores | Sim | A fim de manter o nível acordado de segurança da informação e de disponibilidade de serviços, necessitamos de uma forma de monitorizar as relações com os fornecedores, bem como adquirir produtos e equipamentos  homologados | Onde aplicável, são preferidos produtos e/ou fornecedores credenciados / homologados  Gestão de Compras |
| A.15.2.2 | Gerir alterações aos serviços de fornecedores | Sim |
| **A.16** | **Gestão de incidentes de segurança da informação** | | | |
| **A.16.1** | **Gestão de incidentes de segurança da informação e melhorias**  Objetivos: Assegurar uma abordagem consistente e eficaz à gestão de incidentes de segurança da informação, incluindo a comunicação de eventos e pontos fracos de segurança | | | |
| A.16.1.1 | Responsabilidades e  procedimentos | Sim | Necessidade de assegurar uma abordagem consistente eficaz de gestão de incidentes de segurança da informação, incluindo a comunicação de eventos e possíveis pontos fracos de segurança detetados. | Gestão de Incidentes de Sistemas de Informação |
| A.16.1.2 | Reportar eventos de  segurança de informação | Sim |
| A.16.1.3 | Reportar pontos fracos  de segurança de informação | Sim |
| A.16.1.4 | Avaliação e decisão sobre eventos de  segurança de informação | Sim |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ID | Controlos de acordo com  a norma ISO/IEC 27001 | Aplicável  Sim/Não | Motivo para a  seleção/não seleção | Método de  implementação |
| A.16.1.5 | Resposta a incidentes de  segurança de informação | Sim |  |  |
| A.16.1.6 | Aprender com os incidentes de segurança  de informação | Sim |
| A.16.1.7 | Recolha de evidências | Sim |
| **A.17** | **Aspetos de segurança da informação na gestão da continuidade do negócio** | | | |
| **A.17.1** | **Continuidade de segurança da informação**  Objetivos: A continuidade de segurança da informação deve ser contemplada nos sistemas de gestão da continuidade do negócio da organização | | | |
| A.17.1.1 | Planeamento da  continuidade da segurança da informação | Sim | Planeamento e estruturação dos controlos, normas, políticas, processos e procedimentos da  segurança da informação | DA - Declaração de aplicabilidade,  PCN - procedimento de continuidade do negócio |
| A.17.1.2 | Implementação da  continuidade da segurança da informação | Sim | Implementação dos controlos, normas, políticas, processos e procedimentos da segurança da  informação |
| A.17.1.3 | Verificar, rever e avaliar a continuidade da segurança da informação | Sim | Necessidade de reavaliação constante da segurança da informação. | PCN - Procedimentos de continuidade do negócio.  Teste de simulação; Checklist para  auditorias periódicas, |
| **A.17.2** | **Redundâncias**  Objetivos: Assegurar a disponibilidade dos recursos de processamento da informação | | | |
| A.17.2.1 | Disponibilidade dos recursos de  processamento da informação | Sim | Necessidade planeamento e implementação de estratégias de continuidade do negócio. | Checklist para auditorias periódicas, PCN - procedimento de continuidade do  negócio. |
| **A.18** | **Conformidade** | | | |
| **A.18.1** | **Conformidade com requisitos legais e contratuais**  Objetivos: Evitar violações de obrigações legais, estatutárias, regulamentares ou contratuais relacionadas com a segurança da informação e de quaisquer requisitos de segurança | | | |
| A.18.1.1 | Identificação da legislação aplicável e de  requisitos contratuais | Sim | Necessidade de evitar violações legais, estruturais, regulamentares ou contratuais relacionadas com a segurança da informação e de quaisquer requisitos de segurança. | Legislação e normas aplicáveis  (Lista de documentos de origem externa) |
| A.18.1.2 | Direitos de propriedade  intelectual | Sim |
| A.18.1.3 | Proteção de registos | Sim |
| A.18.1.4 | Privacidade e proteção  de dados pessoais | Sim |
| A.18.1.5 | Regulamentação de | Sim |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ID | Controlos de acordo com  a norma ISO/IEC 27001 | Aplicável  Sim/Não | Motivo para a  seleção/não seleção | Método de  Implementação |
|  | controlos criptográficos |  |  |  |
| **A.18.2** | **Revisões de segurança da informação**  Objetivos: Assegurar que a segurança da informação é implementada e operada de acordo com as políticas e procedimentos organizacionais | | | |
| A.18.2.1 | Revisão independente  de segurança da informação | Sim | Necessidade de assegurar que a segurança da informação é implementada e operada de acordo com as políticas e procedimentos organizacionais. | Revisão anual do SGQSI,  Checklist para auditorias periódicas, PCN - Procedimento de continuidade do negócio. |
| A.18.2.2 | Conformidade com as políticas e normas de  segurança | Sim |
| A.18.2.3 | Revisão da  conformidade técnica | Sim |