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 | A ser implementada | |  |  |  |  |  |  |  |
| A.6.1.2 |  | |  |  | | | |  | |
| A.6.1.3 |  |  |  |  | | | |  | de |
| A.6.1.4 |  | |  |
| A.6.1.5 |  | |  |  | | | |  | De |
| **A.6.2** | **Dispositivos móveis e teletrabalho**  Objetivos: Assegurar a segurança no teletrabalho e na utilização de dispositivos móveis | | | | | | | | |
| A.6.2.1 |  | |  |  | | | |  | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 |  | |  |  | | | - | |
| **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 |  | |  |  | | |  |  |
| A.7.1.2 |  | |  |  |  |  |  | |
| **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 |  |  |  |  | | |  |  |
| A.7.2.2 |  | |  |  | |
| A.7.2.3 |  | |  |  |  |
| **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 |  | |  |  | | |  | |
| 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 de avaliação de riscos |  |
| A.8.1.2 | Responsabilidade pelos ativos | | Sim | Necessidade de atribuição de responsável dos ativos. | | |
| A.8.1.3 | Utilização aceitável de ativos |  | Sim | Carência de controlo de meios de utilização aceitáveis dos ativos da empresa | | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ID | Controlos de acordo com  a norma ISO/IEC 27001 | | | | | Aplicável  Sim/Não | Motivo para a  seleção/não seleção | | | | Método de  implementação | | |
|  |  | | | | |  |  | | | |  | | |
| A.8.1.4 | Devolução de ativos | | | | | Sim | Colaboradores e utilizadores externos que usufruam dos ativos da empresa e dever os mesmos no fim do contrato ou prestação de serviço. | | | | Gestão de Recursos Humanos | |  |
| **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 |  | | |  |  |  |  | | | |  | | |
| A.8.2.2 |  | | |  |  |  |  | | | |
| A.8.2.3 |  | | |  |  |  |  | | | |
| **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 |  | | | | |  |  | | | |  | |  |
| A.8.3.2 |  | | | | |  |
| A.8.3.3 |  | | | | |  |
| **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 de assegurar a conformidade de controlo nos acessos à rede. |  |  |  | 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 física 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 |  |  |  |  |
| A.11.1.2 |  |  |
| A.11.1.3 |  |  |
| A.11.1.4 |  |  |
| A.11.1.5 |  |  |
| A.11.1.6 |  |  |
| **A.11.2** | **Equipamento**  Objetivos: Prevenir a perda, dano, furto ou comprometimento de ativos e interrupção das operações da organização | | | |
| A.11.2.1 |  |  |  |  |
| A.11.2.2 |  |  |
| A.11.2.3 |  |  |
| A.11.2.4 |  |  |
| A.11.2.5 |  |  |
| A.11.2.6 |  |  |
| A.11.2.7 |  |  |
| A.11.2.8 |  |  |  |
| A.11.2.9 |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **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 |  |  |  |  |
| 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 |  |  |  |  |
| A.12.1.3 |  |  |
| A.12.1.4 |  |  |
| **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 |  |  |  |  |
| **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 |  |  |  |  |
| A.12.4.2 |  |  |  |
| A.12.4.3 |  |  |
| A.12.4.4 |  |  |  |
| **A.12.5** | **Controlo de software em sistemas de produção**  Objetivos: Assegurar a integridade dos sistemas de produção | | | |
| A.12.5.1 |  |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ID | Controlos de acordo com  a norma ISO/IEC 27001 | Aplicável  Sim/Não | Motivo para a  seleção/não seleção | Método de  implementação |
| **A.12.6** | **Gestão de vulnerabilidades técnicas**  Objetivos: Prevenir a exploração de vulnerabilidades técnicas | | | |
| A.12.6.1 |  |  |  |  |
| A.12.6.2 |  |  |  |
| **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 |  |  |  |  |
| **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 |  |  |  |  |
| A.13.1.2 |  |  |
| A.13.1.3 |  |  |
| **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 |  |  |  |  |
| A.13.2.2 |  |  |  |  |
| A.13.2.3 |  |  |  |  |
| A.13.2.4 |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 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 |  |  |  |  |
| A.14.1.2 |  |  |
| A.14.1.3 |  |  |
| **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 |  |  |  |  |
| A.14.2.2 |  |  |  |
| A.14.2.3 |  |  |
| A.14.2.4 |  |  |
| A.14.2.5 |  |  |  |
| A.14.2.6 |  |  |  |
| A.14.2.7 |  |  |  |  |
| A.14.2.8 |  |  |  |  |
| A.14.2.9 |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 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 |  |  |  |  |
| **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 |  |  |  |  |
| A.15.1.2 |  |  |
| A.15.1.3 |  |  |
| **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 |  |  |  |  |
| A.15.2.2 |  |  |
| **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 |  |  |  |  |
| A.16.1.2 |  |  |
| A.16.1.3 |  |  |
| A.16.1.4 |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 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 |  |  |  |  |
| A.16.1.6 |  |  |
| A.16.1.7 |  |  |
| **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 |  |  |  |  |
| A.17.1.2 |  |  |  |
| A.17.1.3 |  |  |  |  |
| **A.17.2** | **Redundâncias**  Objetivos: Assegurar a disponibilidade dos recursos de processamento da informação | | | |
| A.17.2.1 |  |  |  |  |
| **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 |  |  |  |  |
| A.18.1.2 |  |  |
| A.18.1.3 |  |  |
| A.18.1.4 |  |  |
| A.18.1.5 |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ID | Controlos de acordo com  a norma ISO/IEC 27001 | Aplicável  Sim/Não | Motivo para a  seleção/não seleção | Método de  Implementação |
|  |  |  |  |  |
| **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 |  |  |  |  |
| A.18.2.2 |  |  |
| A.18.2.3 |  |  |