ESCOLA SUPERIOR DE TECNOLOGIA E GESTÃO

P.PORTO

Sistema de Segurança e Gestão da Informação

Trabalho Prático 2

Docente: Prof.ª Aida Maria Calheiros Cepa Carneiro

Grupo RGB

Alunos:

Rui Alexandre Borba Vitorino (8190479)

Bruno Miguel do Carmo Vieira (8190724)

Gilberto Gomes (8210227)

Índice

Objetivo

Definir uma metodologia de identificação, avaliação e tratamento de riscos da informação na organização. A avaliação de riscos aplica-se a todo o Sistema de Gestão da Segurança da informação (SGSI), isto é, a todos os ativos de informações que são usados na organização ou que podem ter um impacto sobre a segurança da informação da organização.

Definições

Ativo – qualquer coisa que tenha valor para a organização.
Pode-se dizer que é tudo aquilo que por si só é importante (informação) ou cujo seu papel pode afetar a segurança da informação (preservação da confidencialidade, integridade e disponibilidade).

Segurança da informação – preservação da confidencialidade, integridade e disponibilidade da informação; adicionalmente, outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confiabilidade, podem também estar envolvidas.

Confidencialidade – propriedade de que a informação não esteja disponível ou revelada a indivíduos, entidades ou processos não autorizados.

Integridade – propriedade de salvaguarda da totalidade e exatidão dos ativos.

Disponibilidade – propriedade de estar acessível e utilizável a pedido de uma entidade autorizada.

Ameaça – causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização.

Vulnerabilidade – fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças.

Evento de segurança da informação – uma ocorrência identificada de um estado de sistema, serviço ou rede, indicando uma possível violação da política de segurança da informação ou falha de controlos, ou uma situação previamente desconhecida, que possa ser relevante para a segurança da informação.

Incidente de segurança da informação – um simples ou uma série de eventos de segurança da informação indesejados ou inesperados, que tenham uma grande probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação.

Sistema de gestão da segurança da informação (SGSI) – a parte do sistema de gestão global, baseado na abordagem de riscos do negócio, para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar a segurança da informação.

Nota: O sistema de gestão inclui estrutura organizacional, políticas, atividades de planeamento, responsabilidades, práticas, procedimentos, processos e recursos.

Risco residual – risco remanescente após o tratamento de riscos.

Aceitação do risco – decisão de aceitar um risco.

Análise de riscos – uso sistemático de informações para identificar fontes e estimar o risco.

Análise/avaliação de riscos – processo completo de análise e avaliação de riscos.

Avaliação de riscos – processo de comparar o risco estimado com critérios de risco predefinidos para determinar a importância do risco.

Gestão de riscos – atividades coordenadas para direcionar e controlar uma organização no que se refere a riscos.
Nota: *A gestão de riscos geralmente inclui a análise/avaliação de riscos, o tratamento de riscos, a aceitação de riscos e a comunicação de riscos*.

Tratamento do risco – processo de seleção e implementação de medidas para modificar um risco.

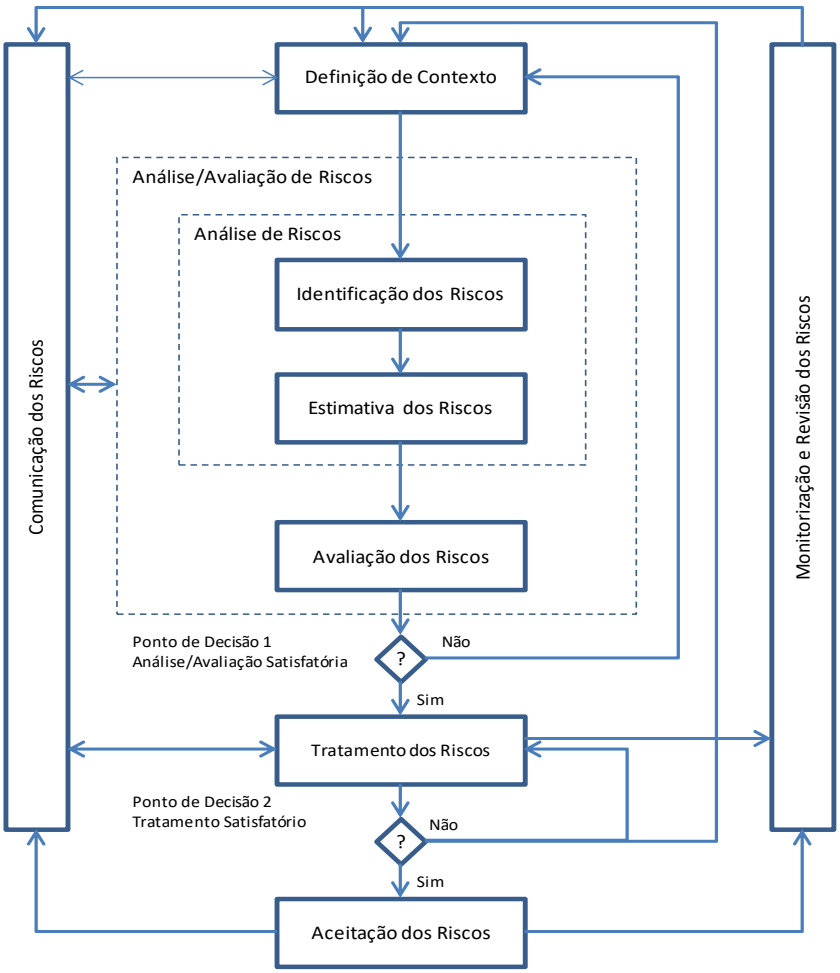
Declaração de aplicabilidade – declaração documentada que descreve os objetivos de controlo e controles que são pertinentes e aplicáveis ao SGSI da organização.
Nota: Os objetivos de controlo e controles estão baseados nos resultados e conclusões dos processos de análise/avaliação de riscos e tratamento de risco, dos requisitos legais ou regulamentares, obrigações contratuais e os requisitos de negócio da organização para a segurança da informação.

Metodologia de Gestão de risco

A definição de uma boa metodologia de gestão de risco tem que contribuir para:

- A identificação de riscos;
- A análise/avaliação de riscos em termos das suas consequências para o negócio e da probabilidade da sua ocorrência;
- Que a probabilidade e a consequência dos riscos sejam comunicadas e entendidas;
- O estabelecimento de prioridades no tratamento de riscos;
- Que seja dada prioridade a ações que reduzam a ocorrência de riscos;
- Que todos os interessados sejam envolvidos nas decisões de gestão de risco e estejam informados do estado da gestão dos mesmos;
- A monitorização de eficácia do tratamento de risco;
- A revisão e monitorização periódicas dos riscos e do processo de gestão dos mesmos;
- A captura de informação que permita melhorar a abordagem de gestão de risco;
- A sensibilização de gestores e colaboradores para os riscos e as ações tomadas no sentido de os mitigar.

Os riscos devem ser geridos de acordo com o processo ilustrado na figura.



Análise e Avaliação dos Riscos

A análise e avaliação dos riscos é coordenada pelo CISO (Chief Information Security Officer) e por um elemento do Comité da Segurança da Informação, sendo utilizada para tal a Tabela de Avaliação de Riscos.

Identificação dos Ativos

A primeira etapa da avaliação de riscos é a identificação de todos os ativos de informação, isto é, de todos os ativos que podem afetar a confidencialidade, integridade e disponibilidade das informações na organização. Os ativos podem incluir documentos em papel ou formato eletrónico, aplicativos e bases de dados, pessoas, equipamentos de informação e comunicação, serviços internos e externos. Ao identificar os ativos, também é preciso identificar os seus "proprietários", as pessoas ou a unidade organizacional responsável para cada ativo, diferenciando-os por categorias de ativos.

Identificação dos Riscos

Na identificação dos riscos deve ter-se em conta as ameaças, vulnerabilidades e consequências associadas a cada ativo.

Deve-se ter o cuidado de avaliar que cada ativo pode estar associado a diversas ameaças e cada ameaça pode estar associada a diversas vulnerabilidades.

Estimativa dos Riscos

Nesta fase, deve proceder-se à estimativa dos riscos que afetam a atividade da organização, avaliando-se para cada Risco, a Probabilidade e o Impacto:

O grau de impacto determinado deverá ter em consideração, as potenciais consequências da perda de confidencialidade, integridade e/ou disponibilidade do ativo e os controlos que já se encontram implementados e que possam contribuir para a redução do mesmo.

		Impacto			
		Baixo Aceitável (atividade acessória) [1]	**Médio** Tolerável (coima grave) [2]	**Alto** Indesejável (grave & reputação) [3]	**Muito Alto** Intolerável (+ grave & reputação) [4]
Probabilidade (nível de maturidade)	**Muito Provável** Risco irá ocorrer uma vez que o controlo é inexistente [4]	4 - Médio	8 - Elevado	12 - Elevado	16 - Crítico
	Provável Risco irá ocorrer uma vez que a maturidade é **muito baixa** [3]	3 - Baixo	6 - Médio	9 - Elevado	12 – Elevado
	Possível Risco poderá ocorrer uma vez que a maturidade é **baixa** [2]	2 – Baixo	4 - Médio	6 - Médio	8 - Elevado
	Improvável Risco improvável uma vez que a maturidade é **média ou alta** [1]	1 - Baixo	2 - Baixo	3 - Médio	4 - Médio

Os controlos de segurança existentes devem ser inseridos na coluna da Tabela de avaliação de riscos.

Nível de Risco Final = Probabilidade * Impacto

Avaliação dos Riscos

Após se ter uma lista de todos os riscos estimados que ameaçam os ativos da organização, é necessário compará-los com os critérios previamente definidos para:

- Avaliação de risco: Que definem as várias categorias de riscos que se pretendem diferenciar e podem ser utilizadas para definir prioridades de tratamento dos mesmos;
- Aceitação de risco: Que definem as circunstâncias em que um determinado risco é considerado suficientemente negligenciável para não requerer qualquer tipo de tratamento.

Assim, é possível tomar decisões sobre ações a tomar, nomeadamente sobre quais os riscos que requerem ação e respetivas prioridades.

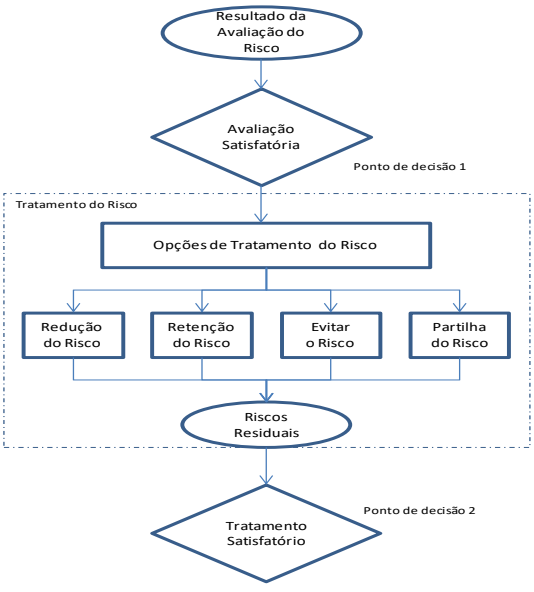
Contudo, nesta fase é também especialmente importante avaliar se há ou não confiança nos critérios definidos e na estimativa de riscos efetuada, principalmente durante as primeiras aplicações da metodologia. Caso haja dúvidas sobre a sua eficácia/adequação, devem efetuar-se os ajustes necessários e repetir a sua aplicação.
Assim, no final desta fase surge uma lista de riscos priorizada de acordo com os critérios adotados.

Categoria	Nível de Risco	Descrição
Crítico	16	São inaceitáveis, devem ter um tratamento prioritário imediato
Elevado	[8-12]	São inaceitáveis, devem ter um tratamento prioritário.
Médio	[4-6]	Poderão ser aceitáveis mediante formalização por parte da Administração. Caso contrário, requerem a existência de um plano de tratamento.
Baixo	≤3	São considerados aceitáveis, carecendo apenas de registo e não requerendo ações específicas de tratamento.

Tratamento dos Riscos

Agora é necessário decidir o que fazer em relação a cada um deles, levando em consideração:

- A prioridade de cada um dos riscos;
- As opções de tratamento possíveis;
- Os benefícios esperados de cada uma das opções de tratamento existentes;
- O custo da implementação das opções de tratamento existentes, sendo que:
  - Se deve efetuar um esforço para reduzir o mais possível as consequências adversas dos riscos existentes;
  - Quando grandes reduções de risco podem ser conseguidas a um custo reduzido, essas opções devem ser implementadas;
  - Devem ser considerados riscos que, embora raros, possam ter consequências graves, e que justifiquem a adoção de tratamentos que não seriam justificáveis por critérios meramente económicos (por exemplo, a existência dos controlos de continuidade de negócio);
  - Deve haver uma reflexão documentada sobre a não implementação de opções cujo custo seja considerado excessivo quando comparado com os benefícios esperados;



O resultado deverá ser formalizado num "Plano de Tratamento do Risco".

Após a definição do referido plano, determina-se os níveis residuais de risco, o que envolve uma atualização da apreciação de risco, considerando os efeitos dos vários tratamentos previstos. Caso o nível de risco residual ainda seja superior ao nível considerado aceitável, dever-se-á proceder a uma nova iteração do processo de tratamento de risco antes de se poder efetuar a aceitação.

Redução do Risco

Esta opção de tratamento passa pela adoção de uma seleção de controlos que permitam obter níveis de risco residual considerados aceitáveis.

Nota: No caso da opção pela Redução do Risco – seleção de controlos de segurança, é necessário avaliar o novo valor do impacto e a probabilidade na Tabela de tratamento de riscos, que resultará em um novo valor de risco após a implementação dos controlos.

Retenção do Risco

Esta opção corresponde à decisão de aceitar um determinado risco, não tomando qualquer medida no sentido de o reduzir. Esta opção deve ser utilizada, caso o respetivo risco se encontre dentro dos critérios de aceitação definidos pela organização ou em situações em que não há nenhuma ação que possa evitar, reduzir ou transferir o risco (por exemplo, risco de alterações legislativas que impactem negativamente o negócio).

Para além disso, as consequências (legais, financeiras, etc.) de uma decisão deste tipo deverão ser cuidadosamente avaliadas, carecendo da aprovação da Gerência.

Evitar o Risco

Quando um risco ou o custo da implementação do respetivo controlo é demasiadamente elevado, pode equacionar-se, descontinuar uma determinada atividade do negócio (p.e. deixando de comercializar um produto cuja qualidade não se consegue controlar), ou alterar as condições em que a mesma é levada a cabo (p.e. retirando ativos de locais propícios a furto, etc.).

Partilha do Risco

Partilha do risco com terceiros mais capazes de o gerir de forma eficaz. Um exemplo deste tipo de tratamento será a subscrição de um seguro que cubra as consequências previstas ou a contratação de um prestador de serviços em quem delegar determinado tipo de atividades. Contudo, dado que daí podem advir novos riscos (franquias de prémios de seguro, risco de falha do prestador de serviços, etc..) ou a alteração de riscos já identificados, poderão ser necessárias medidas adicionais de tratamento de risco. Para além disso, a utilização deste tipo de opção carece de uma análise de risco ao parceiro envolvido.

Frequência da avaliação e do tratamento de riscos

A avaliação deve ser realizada pelo menos uma vez por ano ou com mais frequência em caso de alterações organizacionais importantes, alterações significativas na tecnologia, no objetivo dos negócios, alterações legais ou regulamentares, etc.

Aceitação dos Riscos

Após a elaboração do Plano de Tratamento, os Riscos Residuais, têm que ser aprovados pelo Conselho de Administração, e tem que se obter a aprovação dos responsáveis pelos riscos e a aceitação dos riscos residuais.

A aplicabilidade ou não aplicabilidade dos controles de segurança do Anexo A da norma ISO/IEC 27001, deve ser documentada na Declaração de Aplicabilidade. O Conselho de Administração deve aceitar todos os riscos residuais na Declaração de Aplicabilidade.

Análise de riscos

A análise de riscos segue em documento anexo, denominado RGB_AnaliseDeRiscos.

AVALIAÇÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO

ID Risco	Risco (Ameaça)	Fonte de Ameaça	Tipo de Ameaça	Motivo	Preocupação			Resultado (Ataque ou Incidente)	Probabilidade	Impacto	Nível de Risco	Categoria
					afidencialidade	Integridade	isponibilidade					
10	Roubo ou perda de documentos físicos com informação confidencial	• Pessoal interno; • Pessoal externo.	Humana	• Causar danos de forma intencional à Organização; • Uso de informação para propósitos financeiros; • Uso da informação para propósitos pessoais.	■			• Danos ao nível da imagem exterior da Organização; • Roubo ou perda de informação: informação crítica ou confidencial que pode tornar-se pública ou ser utilizada por terceiros.	2	3	6	Médio
11	Envio não autorizado de informação de negócio	• Pessoal interno	Humana	• Causar danos de forma intencional à Organização; • Uso de informação para propósitos financeiros; • Uso da informação para propósitos pessoais.	■			• Danos ao nível da imagem exterior da Organização; • Extravio ou perda de informação: informação crítica ou confidencial que pode tornar-se pública ou ser utilizada por terceiros.	3	4	12	Alto
12	Tempo excessivo de resolução em caso de falha técnica a nível de hardware, software ou componentes de rede.	• Organização de TI; • Fornecedores externos.	Tecnologias	• Procedimentos com um âmbito de aplicação limitada; • Monitorização e controlo de incidentes com um âmbito limitado e assente largamente e intervenção humana e manual; • Insuficiências ao nível dos contratos e controlo dos fornecedores externos.			■	• Indisponibilidade de serviços críticos devido à falha de Sistemas de Informação.	2	2	4	Médio
13	Alterações da infraestrutura sem documentação	• Organização de TI; • Fornecedores externos.	Organizacional	• Os procedimentos não se encontram descritos de forma sistemática; • Insuficiência de práticas de testes, aquando de alterações; • Controlo de alterações insuficiente; • Insuficiente domínio de soluções mais complexas implementadas inicialmente por entidades externas.		■	■	• Indisponibilidade de serviços críticos devido à falha de Sistemas de Informação.	2	4	8	Alto

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 +01:00Motivo: 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

1. Introdução

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

Este documento inclui todos os controlos relacionados no Anexo A da normaISO 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.

2. 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 da Qualidade e de Segurança da Informação PSI - Princípios de Segurança da Informação
A.5.1.2	Revisão das políticaspara 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 - Plano De Segurança
A.9.1.2	Acesso a redes e a serviços de rede	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 - Plano De Segurança
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 informação secreta para autenticação de utilizadores	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 - Plano de Segurança
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 informação	Sim	Necessidade de aumento no nível de segurança no acesso a informação secreta.	PSEG - Plano de Segurança
A.9.4.2	Procedimentos seguros de início de sessão	Sim		
A.9.4.3	Sistema de gestão de senhas	Sim		
A.9.4.4	Utilização de programas utilitários privilegiados	Sim		
A.9.4.5	Controlo de acesso ao código fonte de programas	Sim	Garantia de integridade e propriedade intelectual	Código fonte reside apenas nos servidores 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			
A.10.1.1	Política sobre a utilização de controlos criptográficos	Sim	Garantia de confidencialidade e integridade da informação	MF - Manual de 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				

Política de cópias de segurança

Histórico de versões

Data	Edição n.º	Conteúdo
22/12/2021	1.0	Redação Inicial
10/01/2022	2.0	Alteração do ponto 7 de "7.Fornecedor de salvaguarde de cópias de segurança" para "Cópias de segurança Offsite"

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 +01:00Motivo: 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

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

Introdução

As cópias de segurança são uma exigência das empresas para permitir a recuperação de dados e aplicações no caso de eventos, tais como catástrofes naturais, falhas em discos rígidos, espionagem, erros na introdução de dados ou erros na operação do sistema.

Âmbito

O objetivo da definição da política de cópias de segurança, é o estabelecimento de regras para as cópias de segurança e respetivo arquivo eletrónicos e seu suporte.

Política de Cópia de segurança

A frequência e a extensão das cópias de segurança devem ser de acordo com aimportância da informação e o risco aceitável, conforme determinado peloproprietário dos dados.
Para cada sistema de Recursos de Informação da Mercado da Boneca, o processo de cópia de segurança e de recuperação de dados deverá ser documentado e revisto periodicamente.
Deverá ser implementado um processo de verificação do êxito das cópias de segurança eletrónicas.
As cópias de segurança devem ser periodicamente testadas para assegurar que os dados contidos são recuperáveis.
Os suportes das cópias de segurança, se aplicável, devem conter no mínimo osseguintes identificadores em etiquetas:

- Nome do sistema;
- Data da cópia de segurança;
- Relevância dos dados;

Responsável pelas cópias de segurança

Administrador de Segurança

Periodicidade

Semanalmente: cópia de segurança integral
Diariamente: cópia de segurança incremental

Aplicação de cópias de segurança

A Mercado da Boneca para implementar os fins acima descritos instalou na sua rede interna, umservidor para efeitos de cópias de segurança. A solução escolhida pela Mercado da Boneca foi alvo de análise, tendo optado pelo *backup*, solução de alta performance *Open-Source*.
Conforme o equipamento alvo de cópia de segurança, será especificado em documentoanexo os ficheiros a serem incluídos na cópia de segurança.

Cópias de segurança externas

De forma a aumentar o nível de segurança, a Mercado da Boneca mantém cópias de segurança em instalações exteriores.
O procedimento para efetuar cópias de segurança em instalações externas encontra-se no documento "CSO – Cópias de Segurança Offsite".

Ações disciplinares

A violação desta política poderá resultar em ação disciplinar, que podem incluir: a rescisão temporária ou efetiva do contrato; uma cessação das relações de trabalho no caso de contratantes ou consultores; demissão de estagiários e voluntários; suspensão ou expulsão, no caso de um estudante. Além disso, os indivíduos estão sujeitos à perda deprivilégios de acesso os Recursos de Informação da Mercado da Boneca, e processo civil e/ou penal.

Política de Passwords

A utilização da generalidade dos serviços e recursos eletrónicos disponíveis na Mercado da Boneca SA, necessita da atribuição ao utilizador de um código de utilizador e de uma password para autenticação e autorização de acesso, adiante denominados conta.

O utilizador será responsável pela segurança da conta e pela sua utilização, não devendo permitir a sua utilização por terceiros, nem em caso algum lhes dar conhecimento da sua password.

A política de passwords aplica-se a todos os utilizadores do IPB e rege-se pelas seguintes regras gerais:

Todas as contas atribuídas pela Mercado da Boneca SA são pessoais e intransmissíveis, sendo a garantia de identidade assegurada pela posse de uma chave secreta (palavra-passe, palavra-chave, senha de acesso ou password) detida por cada Utilizador.
O utilizador não pode comunicar a sua password a terceiros.
O utilizador não deve usar a password associada à conta da Mercado da Boneca SA para se registar noutros sistemas (ex: homebanking, FCT, Skype, Gmail, etc.).
Sempre que for necessária a autenticação e autorização de acesso, será usado um código de utilizador e password que cumpram os requisitos a seguir descritos, definidos em função do vínculo e perfil de uso que o utilizador mantém com a instituição.
Deve sempre evitar colocar senhas simples ou óbvias (p.e. igual ao código de utilizador, número de aluno ou de documentos de identificação, iniciais do nome, ...).
A password deve ser complexa e ter no mínimo:

- Para a generalidade dos utilizadores: 9 caracteres;
- Para utilizadores com responsabilidades de administração: 13 caracteres.

A sua composição exige a inclusão de 3 dos 4 seguintes conjuntos de caracteres:

- letras minúsculas (a...z)
- letras maiúsculas (A...Z)
- números: (0...9)
- caracteres especiais: |!#$%&()=.:,;*<>@

Não pode conter os seguintes caracteres (que são considerados inválidos por algumas aplicações):

- áàãâÁÀÃÂéèêÉÈÊíìîÍÌÎóòõôÓÒÕÔúùûÚÙÛçÇ+-ao"'

O armazenamento das passwords é efetuado em modo não reversível.

As passwords são gravadas centralmente de forma encriptada, sendo do conhecimento exclusivo de cada utilizador.

As passwords deverão transitar entre o sistema central de autenticação e as aplicações sempre encriptadas ou protegidas por protocolos seguros.

No caso de haver sistemas que, excecionalmente, não possam implementar as políticas de passwords definidas, os utilizadores terão obrigatoriamente de ser informados sobre as políticas locais implementadas.

A equipa técnica do Departamento de Sistemas de Informação da Mercado da Boneca SA nunca solicita ao utilizador a indicação da password.

Será disponibilizado um mecanismo do tipo self-service para a definição de novas passwords, que exige prova inequívoca de identidade do Utilizador.

Política de Controlo de Acessos

Acessos a instalações e sistemas

A segurança física tem como objetivo fornecer um ambiente seguro para as pessoas, equipamentos e informação. Sem segurança física adequada, os ativos podem ficar danificados e os controlos de segurança lógica podem ser ultrapassados. A segurança física tem o seu foco, em controlos e regras de forma a evitar o acesso de pessoas não autorizadas a áreas onde se encontram dados e informações críticas da empresa.

Para desenvolver uma boa política de segurança física a empresa deverá contemplar:

- Controlo do acesso físico.
- Formas de identificação.
- Registo de entradas e saídas.
- Identificação de áreas críticas (CPD, arquivos).
- Mecanismos de controlo (câmaras de vídeo, alarmes, fechaduras).
- Controlo de prestadores de serviço.

Como o avanço da tecnologia novas formas de proteção estão a ser implementadas de forma a garantir uma segurança mais eficaz, que nos proporciona proteção e vigilância 24 horas por dia, 7 dias por semana.

É importante analisar o modelo de negócio da Mercado da Boneca SA para definir a política de controlo de acesso físico, por forma a melhorar a segurança e sensibilizar os utilizadores para as regras implementadas.

Existe também um aspeto muito importante que é a identificação das áreas da empresa onde os prestadores de serviço têm que ter acesso (empresa de limpeza, prestador de serviços IT). Nesse contexto a segurança física deve ter um foco mais ativo porque as ameaças são muito maiores.

Acessos físicos

Pessoas Externas à Mercado da Boneca SA

1) O vigilante deverá fazer o registo de todas as pessoas externas à chegada, preenchendo os campos "Nome do Visitante/Entidade", "Motivo da Visita", "Data da Visita" e "Hora de Entrada" do Mod.RA1 Registos dos acessos.
2) As pessoas externas não devem circular livremente pelas instalações da Mercado da Boneca SA, sendo que deverão ser sempre acompanhadas por um colaborador.
3) Quando a pessoa externa abandonar a Mercado da Boneca SA, o vigilante regista a hora de saída da mesma no campo "Hora de Saída".
4) Os registos de entrada/saída dos visitantes serão **arquivados por 6 meses** para consulta sempre que necessário.

Colaboradores internos

1) Os colaboradores da Mercado da Boneca SA, incluindo os que estão ao abrigo de um estágio profissional, possuem um cartão de acesso fornecido pelo Departamento de Recursos Humanos, sendo da responsabilidade de cada um assegurar a adequada proteção. Este cartão dá acesso ao edifício, às salas de reunião, e às instalações da Mercado da Boneca SA.
2) No caso dos estagiários no âmbito de estágios de curta duração (exemplo: estágios curriculares), estes não possuem cartão de acesso e como tal deverão tocar à campainha e fazer o registo de entrada e saída diariamente no Mod.RA1Registos dos acessos.
3) Em caso de perda do cartão, cabe ao colaborador comunicar imediatamente ao DRH que procederá à inativação do mesmo. Se após 5 dias úteis o cartão não for encontrado, o colaborador deverá informar o DRH, que fará cancelamento do cartão. Os procedimentos de inativação ou cancelamento são realizados imediatamente pela DRH assim que recebem o pedido.
4) A emissão de novos cartões para novos colaboradores é solicitada ao DRH.
5) Quando um colaborador sai da empresa deverá entregar o cartão de acesso ao DRH no dia da sua saída.
6) Não é permitido a troca de cartões entre colaboradores.
7) A área da arrecadação está protegida por duas portas cuja chave tem duas cópias que são guardadas uma pelo assistente técnico da Comité da Segurança da Informação e outra pelo Responsável DSI.

Referências

(*Backup Policies - AWS Organizations*, n.d.; *Backup Policies - IBM Documentation*, n.d.; *Backup Policy - Complete Guide - High Table*, n.d.; *Data Backup Policy Template*, n.d.; *Guidance and Best Practices - Azure Backup | Microsoft Docs*, n.d.)

Backup policies - AWS Organizations. (n.d.). Retrieved January 17, 2022, from https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_backup.html

Backup policies - IBM Documentation. (n.d.). Retrieved January 17, 2022, from https://www.ibm.com/docs/en/aix/7.2?topic=concepts-backup-policies

Backup Policy - complete guide - High Table. (n.d.). Retrieved January 17, 2022, from https://hightable.io/backup-policy/

Data Backup Policy Template. (n.d.). Retrieved January 17, 2022, from https://webstore.ansi.org/Standards/ISO/ISO154892016?gclid=EAIaIQobChMIyqL2_d285AIVCRgMCh

Guidance and best practices - Azure Backup | Microsoft Docs. (n.d.). Retrieved January 17, 2022, from https://docs.microsoft.com/en-us/azure/backup/guidance-best-practices