



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)

## 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 +01:00 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

Conteúdo

[1. Introdução: 5](#_Toc93252852)

[2. Âmbito 5](#_Toc93252853)

[3. Políticas de Cópia de segurança 5](#_Toc93252854)

[4. Responsável pelas cópias de segurança 5](#_Toc93252855)

[5. Periodicidade 5](#_Toc93252856)

[6. Aplicação de cópias de segurança 6](#_Toc93252857)

[7. Cópias de segurança externas 6](#_Toc93252858)

[8. Ações disciplinares 6](#_Toc93252859)

[POLÍTICA DE PASSWORDS 7](#_Toc93252860)

[9. Referências 8](#_Toc93252861)

# 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

* 1. A frequência e a extensão das cópias de segurança devem ser de acordo com a importância da informação e o risco aceitável, conforme determinado pelo proprietário dos dados.
  2. 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.
  3. Deverá ser implementado um processo de verificação do êxito das cópias de segurança eletrónicas.
  4. As cópias de segurança devem ser periodicamente testadas para assegurar que os dados contidos são recuperáveis.
  5. Os suportes das cópias de segurança, se aplicável, devem conter no mínimo os seguintes 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, um servidor para efeitos de cópias de segurança. A solução escolhida pela Mercado da Boneca foi alvo de análise, tendo optado pelo backuppc, solução de alta performance open-source.

Conforme o equipamento alvo de cópia de segurança, será especificado em documento anexo 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 de privilégios 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:

* 1. 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.
  2. O utilizador não pode comunicar a sua password a terceiros.
  3. 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.).
  4. 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.
  5. 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, ...).
  6. 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"'
  1. O armazenamento das passwords é efetuado em modo não reversível.
  2. As passwords são gravadas centralmente de forma encriptada, sendo do conhecimento exclusivo de cada utilizador.
  3. As passwords deverão transitar entre o sistema central de autenticação e as aplicações sempre encriptadas ou protegidas por protocolos seguros.
  4. 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.
  5. A equipa técnica do Departamento de Sistemas de Informação da Mercado da Boneca SA nunca solicita ao utilizador a indicação da password.
  6. 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

# 10.1 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

<https://hightable.io/backup-policy/>

<https://www.ibm.com/docs/en/aix/7.2?topic=concepts-backup-policies>

<https://nationalcybersecuritysociety.org/wp-content/uploads/2019/10/Backup-Policy-Template.pdf>

<https://docs.microsoft.com/en-us/azure/backup/guidance-best-practices>

<https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_backup.html>

<https://www.computerweekly.com/podcast/Whats-new-in-ISO-27001-2103-for-storage-and-backup>