Termos e Condições de Housing de Equipamentos

> **Os termos e condições abaixo indicados aplicam-se às seguintes Instituições:**
> - Departamento de Engenharia Eletrotécnica e de Computadores da Universidade de Coimbra (DEEC)
> - Instituto de Sistemas e Robótica - Pólo de Coimbra (ISR)
> - Instituto de Telecomunicações - Pólo de Coimbra (IT)
> - Instituto de Engenharia de Sistemas e Computadores de Coimbra (INESCC)

Está disponível o serviço de housing & Colocation no Datacenter comum DEEC/ISR/IT/INESCC. Este serviço consiste na colocação (colocation) do servidor ou outro equipamento informático com acesso à rede neste espaço.

Sendo que o servidor é fornecido pelo cliente, será este também configurado, administrado e mantido (hardware e software) pelo mesmo. Desta forma, o seu proprietário poderá instalar o software que desejar, bem como configurá-lo minuciosamente.

O espaço dedicado a este serviço possui ligações redundantes ao core da rede e ligação a UPS (limitado a equipamentos sem GPU para efeitos de computação) e é fisicamente seguro, pelo que novos pedidos carecem de verificação de disponibilidade.

Benefícios e Características

- Energia – Acesso a UPS (limitado a equipamentos sem GPU para efeitos de computação) , garantindo maior segurança eléctrica e estabilidade dos equipamentos
- Controlo de Temperatura – Sistema HVAC (Controlo de Temperatura e Humidade) permite ter um controlo constante da temperatura e humidade relativa
- Ligação a core da rede – Ligação directa ao core da rede para maior estabilidade, velocidade de acesso superior e baixa latência entre as aplicações e os utilizadores
- Segurança – Espaço com acesso limitado permite maior segurança dos equipamentos

Responsabilidades do Proprietário

- Instalação (podendo ser pedido o nosso apoio)
- Parametrização de rede (podendo ser pedido o nosso apoio ou solicitados os dados necessários)
- Configuração de sistema base, contas/acessos, camada aplicacional e serviços
- Manutenção
- Operação
- Cópias de Segurança
- Actualizações de Software
- Resolução de Problemas
- Licenciamento

Boas Práticas

- Controlo de Acessos
  - Utilizar contas individuais, nunca contas partilhadas
  - Aplicar o princípio do menor privilégio (acesso apenas ao necessário) - conta de administração separada das contas de utilizador regular
  - Utilizar as melhores práticas na utilização de passwords
    - Utilizar passwords baseadas em palavras - https://www.keepersecurity.com/features/passphrase-generator/
    - Não conter informação pessoal ou institucional
    - NUNCA reutilizar palavras-passe de outros serviços
    - Ativar autenticação de 2 fatores (2FA) sempre que possível
    - Utilizar gestor de passwords para facilitar a utilização das boas práticas acima indicadas - recomendamos https://bitwarden.com/
  - Separar permissões de leitura, escrita e administração adequadas apenas ao estritamente necessário
  - Rever permissões regularmente
- Organização e Estrutura
  - Utilizar pastas bem estruturadas conforme cada necessidade específica
  - Evitar armazenar dados pessoais fora de locais autorizados
  - Rever permissões de sistema de ficheiros regularmente
- Acesso Remoto
  - Acesso a interfaces de administração apenas mediante VPN institucional
  - Acesso a linha de comandos deve estar desativado sempre que possível ou mediante VPN institucional se estritamente necessário e apenas utilizando chaves criptográficas
  - Evitar acesso directo via Internet sem firewall a qualquer serviço não estritamente necessário
  - Desactivar serviços e portas não utilizados
- Actualizações e Manutenção
  - Manter o sistema operativo actualizado

    - Aplicar actualizações de segurança assim que disponíveis
    - Remover serviços obsoletos ou não utilizados
- Cópias de Segurança (Backups)
    - Garantir que existem backups automáticos
    - Seguir a regra 3-2-1: 3 cópias dos dados, em 2 tipos de suporte diferentes, 1 cópia fora do sistema principal
    - Testar periodicamente a reposição de backups

Riscos associados ao uso inadequado de sistemas

- Perda de dados irreproduzíveis
- Violação de dados pessoais
- Comprometimento de credenciais
- Interrupção de serviços instalados
- Acesso não autorizado a informação sensível

Anomalias e Problemas

Por razões de segurança, em caso de detecção de anomalias (vírus, software malicioso, mau funcionamento de software, etc.), quebras de segurança (contas atacadas, etc.) ou qualquer outro problema que tenha potencial impacto na restante infra-estrutura, o equipamento será imediatamente desligado da rede e/ou energia e entregue ao proprietário para correcção das situações identificadas.

Disposições finais

A instituição pode atualizar este regulamento periodicamente para responder a necessidades técnicas ou legais emergentes.

Revision #3
Created 2026-01-30 13:30:33 UTC by Francisco Maia
Updated 2026-02-03 19:10:08 UTC by Francisco Maia