ANMCS
unitate aflată în SUPRAVEGHEREA

SJUB
SPITALUL JUDETEAN DE URGENTA BACAU
Bacău, Str. Spiru Haret, nr. 2, Cod Poştal: 600114, CUI: 4278728
Tel. 0234.534.000 Fax: 0234.537.571 E-mail:office@spitaluljudeteanbacau.ro,
registratura@spitaljudbc.ro, relatiipublice@spitaluljudeteanbacau.r
www.spitaluljudeteanbacau.ro Nr._____Din:_____

SE APROBĂ,
MANAGER

BIBLIOGRAFIE ŞI TEMATICĂ
pentru concursul de ocupare a postului contractual vacant de conducere, pe durată nedeterminată, de Şef Serviciu Informatică, Evaluare şi Statistică Medicală
Spitalul Judeţean de Urgenţă Bacău

I. BIBLIOGRAFIE

A. Legislaţie şi reglementări aplicabile

L1. Constituţia României, republicată – prevederile referitoare la egalitatea în drepturi, viaţa intimă şi privată, dreptul la informaţie şi protecţia sănătăţii.

L2. Legea nr. 53/2003 – Codul muncii, republicată, cu modificările şi completările ulterioare – drepturile şi obligaţiile angajatorului şi salariaţilor, raporturile de muncă, formarea profesională şi răspunderea disciplinară.

L3. Ordinul Secretariatului General al Guvernului nr. 600/2018 privind aprobarea Codului controlului intern managerial al entităţilor publice, cu modificările şi completările ulterioare – standardele referitoare la atribuţii şi responsabilităţi, obiective, planificare, monitorizarea performanţelor, managementul riscurilor, proceduri, continuitatea activităţii, informare şi comunicare şi gestionarea documentelor.

L4. Legea nr. 544/2001 privind liberul acces la informaţiile de interes public, cu modificările şi completările ulterioare – principiile accesului la informaţii şi categoriile de informaţii exceptate de la accesul liber.

L5. Legea nr. 95/2006 privind reforma în domeniul sănătăţii, republicată, cu modificările şi completările ulterioare – Titlul VII „Spitalele", prevederile privind organizarea, funcţionarea şi conducerea spitalelor.

L6. Regulamentul (UE) 2016/679 privind protecţia datelor cu caracter personal – în special art. 5, 6, 9, 24, 25, 28 şi 32–34, referitoare la principiile prelucrării, datele privind sănătatea, responsabilităţile operatorului şi persoanelor împuternicite, măsurile de securitate şi încălcările securităţii datelor.

L7. Legea nr. 46/2003 privind drepturile pacientului, cu modificările şi completările ulterioare – prevederile privind confidenţialitatea informaţiilor medicale.

L8. Ordonanţa de urgenţă a Guvernului nr. 155/2024 privind instituirea unui cadru pentru securitatea cibernetică a reţelelor şi sistemelor informatice din spaţiul cibernetic naţional civil, aprobată cu modificări şi completări prin Legea nr. 124/2025, cu modificările şi completările ulterioare – prevederile privind domeniul de aplicare, managementul riscurilor de securitate cibernetică, măsurile de securitate şi gestionarea şi raportarea incidentelor.

L9. Ordinul comun al ministrului sănătății publice și al președintelui CNAS nr. 1.782/576/2006 privind înregistrarea și raportarea statistică a pacienților care primesc servicii medicale în regim de spitalizare continuă și spitalizare de zi, cu modificările și completările ulterioare – prevederile privind documentarea, colectarea și raportarea datelor medicale.

L10. Ordinul președintelui CNAS nr. 516/2023 privind aprobarea regulilor de confirmare din punctul de vedere al datelor clinice și medicale la nivel de pacient pentru cazurile spitalizate în regim de spitalizare continuă și de zi, precum și a metodologiei de evaluare a cazurilor neconfirmate pentru care se solicită reconfirmarea, cu modificările și completările ulterioare – regulile de confirmare și metodologia de evaluare a cazurilor neconfirmate.

B. Bibliografie tehnică de specialitate

T1. Andrew S. Tanenbaum, David J. Wetherall – *Computer Networks*, ediția a 5-a, Pearson – capitolele referitoare la arhitectura rețelelor, legătura de date, nivelul rețea, nivelul transport și protocoalele de aplicație.

T2. Microsoft Learn – *Active Directory Domain Services – Training*, modulele:

- Introduction to AD DS;
- Manage AD DS domain controllers and FSMO roles;
- Implement Group Policy Objects.

https://learn.microsoft.com/en-us/training/paths/active-directory-domain-services/

T3. Microsoft Learn – *Active Directory Domain Services overview* – structura și funcționarea AD DS, domenii, controlere de domeniu, autentificare, autorizare și replicare.
https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview

T4. Microsoft Learn – *What is Dynamic Host Configuration Protocol (DHCP) Server in Windows Server?* – funcționarea DHCP, alocarea adreselor IP, integrarea cu DNS și disponibilitatea serviciului.
https://learn.microsoft.com/en-us/windows-server/networking/technologies/dhcp/dhcp-top

T5. Canonical – *Ubuntu Server Documentation*, secțiunile:

- Security: User management, Firewalls, OpenSSH;
- Networking: DNS, DHCP, configurarea și diagnosticarea serviciilor;
- Managing software: Package management, Automatic updates;
- Data and storage: Backups and version control.

https://ubuntu.com/server/docs/

T6. Microsoft Learn – *Virtualization documentation*, secțiunile:

- Hyper-V overview;
- Hyper-V hosts;
- Virtual machines;
- Virtual networking.

https://learn.microsoft.com/windows-server/virtualization/

T7. Fortinet – *FortiGate/FortiOS Administration Guide*, versiunea 7.4, secțiunile introductive privind:

- Firewall policy;
- VPN și controlul traficului;
- Logging and monitoring.

https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/656084/firewall-policy

T8. PostgreSQL Global Development Group – *PostgreSQL 18 Documentation*, Tutorial, capitolul 2 – *The SQL Language*, subcapitolele 2.1–2.8: concepte, tabele, interogări, JOIN, agregare și actualizarea datelor.
https://www.postgresql.org/docs/18/tutorial-sql.html

T9. Microsoft Learn – *Back up and restore of SQL Server databases*, secțiunile privind strategiile de backup și restaurare, protejarea copiilor de siguranță și testarea restaurării.

https://learn.microsoft.com/en-us/sql/relational-databases/backup-restore/back-up-and-restore-of-sql-server-databases

T10. National Institute of Standards and Technology (NIST) – *The NIST Cybersecurity Framework (CSF) 2.0*, 2024 – prezentarea cadrului și cele șase funcții: Govern, Identify, Protect, Detect, Respond și Recover.
https://www.nist.gov/publications/nist-cybersecurity-framework-csf-20

T11. NIST Special Publication 800-61, Revision 3, 2025 – *Incident Response Recommendations and Considerations for Cybersecurity Risk Management* – principiile pregătirii, detectării, gestionării și recuperării în urma incidentelor de securitate.
https://csrc.nist.gov/pubs/sp/800/61/r3/final

T12. NIST Special Publication 800-34, Revision 1, actualizată în 2010 – *Contingency Planning Guide for Federal Information Systems* – secțiunile referitoare la analiza impactului, strategiile de recuperare, elaborarea și testarea planurilor de continuitate.
https://csrc.nist.gov/pubs/sp/800/34/r1/upd1/final

T13. HL7 International – *FHIR Release 4, Overview* – principiile schimbului electronic de informații medicale și conceptul de resursă FHIR.
https://www.hl7.org/fhir/R4/overview.html

T14. National Electrical Manufacturers Association (NEMA) – *DICOM Standard, PS3.1 – Introduction and Overview*, ediția 2026c – capitolele 5 și 6 privind modelul general de comunicație și structura standardului DICOM.
https://dicom.nema.org/Medical/dicom/2026c/output/chtml/part01/PS3.1.html

C. Precizări privind bibliografia tehnică

Documentațiile tehnice oficiale se utilizează exclusiv pentru capitolele și subiectele expres menționate.

Referințele la Microsoft, Canonical, Fortinet și PostgreSQL au rolul de a fundamenta competențe tehnice generale, relevante pentru administrarea sistemelor informatice, și nu instituie cerințe de certificare sau de experiență profesională cu un anumit producător.

Nu se solicită memorarea comenzilor specifice unor versiuni de firmware, a particularităților unor modele comerciale de echipamente sau cunoașterea configurațiilor interne ale spitalului.

Documentațiile NIST, HL7 și DICOM se utilizează la nivelul conceptelor și principiilor expres menționate în tematică. Aceste referințe tehnice nu constituie, prin simpla includere în bibliografie, obligații legale suplimentare.

II. TEMATICĂ

1. Legislație, organizare instituțională și management

1.1. Principiile constituționale relevante pentru exercitarea atribuțiilor într-o instituție publică.

1.2. Drepturile și obligațiile angajatorului și salariaților; organizarea activității și răspunderea profesională.

1.3. Organizarea și funcționarea spitalelor publice; responsabilități de conducere și coordonare.

1.4. Controlul intern managerial: stabilirea obiectivelor, planificarea activităților, managementul riscurilor, proceduri și monitorizarea performanțelor.

1.5. Accesul la informațiile de interes public și protejarea informațiilor exceptate de la comunicare.

Bibliografie: L1–L5.

2. Arhitectura sistemelor de calcul și a infrastructurii informatice

2.1. Componentele hardware și software ale sistemelor de calcul.

2.2. Arhitectura sistemelor de tip client–server.

2.3. Rolul serverelor, stațiilor de lucru, sistemelor de stocare și echipamentelor de comunicații.

2.4. Principiile disponibilității, redundanței, scalabilității și monitorizării infrastructurii.

Bibliografie: T1, T5, T6.

3. Rețele de calculatoare și protocoale de comunicație

3.1. Topologii de rețea, medii de transmisie și echipamente de comunicații: switch, router, firewall și punct de acces.

3.2. Modelele OSI și TCP/IP; rolul principalelor niveluri și protocoale.

3.3. Adresarea IPv4/IPv6, subrețele, gateway, rutare și comutare.

3.4. VLAN, segmentarea logică a rețelelor și comunicațiile între segmente.

3.5. Serviciile și protocoalele DNS, DHCP, TCP, UDP, HTTP/HTTPS, SSH și TLS.

3.6. Conexiuni VPN și principiile securizării comunicațiilor între sedii și pentru accesul la distanță.

3.7. Diagnosticarea incidentelor de conectivitate și monitorizarea performanței rețelei.

Bibliografie: T1, T4, T5, T7.

4. Sisteme de operare Windows Server și Active Directory

4.1. Instalarea, configurarea, administrarea și securizarea sistemelor Windows Server.

4.2. Arhitectura Active Directory Domain Services: domenii, păduri, controlere de domeniu, unități organizaționale, utilizatori și grupuri.

4.3. Autentificare, autorizare și administrarea drepturilor de acces.

4.4. Group Policy Objects (GPO): rol, aplicare și administrare.

4.5. Rolurile FSMO și principiile replicării între controlerele de domeniu.

4.6. Integrarea serviciilor DNS și DHCP în infrastructura Windows.

4.7. Monitorizarea, diagnosticarea, actualizarea și recuperarea serviciilor de domeniu.

Bibliografie: T2–T4.

5. Sisteme de operare Linux și administrarea serviciilor

5.1. Arhitectura și administrarea de bază a sistemelor Linux Server.

5.2. Utilizatori, grupuri, permisiuni și controlul accesului.

5.3. Administrarea serviciilor, pachetelor software și actualizărilor.

5.4. Configurarea serviciilor și interfețelor de rețea.

5.5. Accesul administrativ securizat prin SSH și utilizarea firewall-ului local.

5.6. Monitorizare, jurnalizare, diagnosticare și proceduri de backup.

Bibliografie: T5.

6. Securitatea rețelelor și administrarea echipamentelor de protecție

6.1. Principiile securizării rețelelor informatice.

6.2. Rolul firewall-ului în controlul comunicațiilor.

6.3. Politici de filtrare a traficului și reguli de acces între segmente de rețea.

6.4. Segmentarea zonelor cu cerințe diferite de securitate, inclusiv rețelele administrative, medicale și de management.

6.5. Principiile VPN și ale administrării securizate a echipamentelor de comunicații.

6.6. Jurnalizarea, monitorizarea traficului și identificarea evenimentelor de securitate.

6.7. Principiile protecției antivirus/antimalware, ale controlului accesului și ale managementului vulnerabilităților.

Bibliografie: T1, T7, T10.

7. Virtualizare, sisteme de stocare și disponibilitate

7.1. Principiile virtualizării serverelor; hypervisor, mașină virtuală, gazdă fizică și resurse alocate.

7.2. Beneficiile și riscurile consolidării serverelor prin virtualizare.

7.3. Noțiuni privind sistemele RAID, NAS, SAN și protocoalele uzuale de acces la stocare.

7.4. Noțiuni privind clusterizarea, redundanța componentelor și disponibilitatea ridicată.

7.5. Monitorizarea resurselor, capacității și performanțelor.

7.6. Diferențele dintre snapshot, replicare și backup.

Bibliografie: T5, T6, T9, T12.

8. Administrarea bazelor de date

8.1. Concepte privind bazele de date relaționale: tabele, relații, chei și integritate referențială.

8.2. Interogări SQL: SELECT, JOIN, filtrare și agregare.
8.3. Administrarea drepturilor de acces la date.
8.4. Integritatea, consistența și disponibilitatea datelor.
8.5. Strategii de backup și restaurare a bazelor de date.
8.6. Monitorizarea și diagnosticarea problemelor uzuale de performanță și disponibilitate.
Bibliografie: T8, T9.
9. Securitate cibernetică și protecția datelor
9.1. Principiile confidențialității, integrității și disponibilității informațiilor.
9.2. Identificarea și evaluarea riscurilor de securitate cibernetică.
9.3. Controlul accesului, privilegiul minim și autentificarea multifactor.
9.4. Principiile protecției împotriva malware și ransomware.
9.5. Gestionarea vulnerabilităților și actualizărilor de securitate.
9.6. Detectarea, analiza, tratarea și documentarea incidentelor de securitate cibernetică.
9.7. Cadrul normativ privind securitatea cibernetică aplicabil entităților din sectorul sănătății.
9.8. Principiile prelucrării datelor cu caracter personal și măsurile de securitate aplicabile datelor privind sănătatea.
Bibliografie: L6–L8, T10, T11.
10. Backup, continuitatea activității și recuperarea în caz de dezastru
10.1. Identificarea sistemelor și serviciilor informatice critice.
10.2. Analiza impactului întreruperii serviciilor informatice asupra activității instituției.
10.3. Strategii de backup: copii complete, incrementale și diferențiale; separarea și protejarea copiilor de siguranță.
10.4. Planificarea și verificarea restaurării datelor și serviciilor.
10.5. Conceptele Recovery Time Objective (RTO) și Recovery Point Objective (RPO).
10.6. Principiile planificării continuității activității și ale recuperării în caz de dezastru (BCP/DRP).
10.7. Rolul infrastructurilor redundante și al centrelor de date secundare în asigurarea continuității serviciilor.
Bibliografie: L3, T9, T10, T12.
11. Sisteme informatice medicale și interoperabilitate
11.1. Rolul sistemelor informatice în activitatea unui spital.
11.2. Arhitectura funcțională a unui sistem informatic integrat de spital (HIS).
11.3. Rolul sistemelor PACS și al sistemelor informatice asociate imagisticii medicale.
11.4. Principiile schimbului de date între aplicațiile informatice medicale.
11.5. Noțiuni privind standardele HL7/FHIR și DICOM.
11.6. Asigurarea disponibilității, integrității, confidențialității și trasabilității datelor medicale.
11.7. Colaborarea dintre serviciul informatic, personalul medical și furnizorii aplicațiilor pentru menținerea funcționării sistemelor informatice.
Bibliografie: L6, L7, T10, T13, T14.
12. Evaluare și statistică medicală
12.1. Organizarea procesului de colectare și raportare a datelor privind activitatea medicală.
12.2. Documentele și seturile de date utilizate pentru raportarea activității de spitalizare continuă și de zi.
12.3. Principiile sistemului DRG și rolul datelor clinice și administrative în clasificarea cazurilor.
12.4. Verificarea integrității, completitudinii și corectitudinii datelor colectate.
12.5. Identificarea și tratarea erorilor de raportare și a cazurilor neconfirmate.
12.6. Indicatorii statistici și de activitate utilizați pentru monitorizarea performanțelor spitalului.
12.7. Securitatea, confidențialitatea și trasabilitatea datelor medicale utilizate în raportări.
Bibliografie: L5–L7, L9, L10.
13. Managementul serviciului informatic
13.1. Organizarea activităților unui serviciu informatic și repartizarea responsabilităților.

13.2. Planificarea activităților de administrare, mentenanță și suport tehnic.

13.3. Managementul incidentelor, problemelor și schimbărilor din infrastructura IT.

13.4. Administrarea și evidența activelor hardware și software.

13.5. Elaborarea și actualizarea procedurilor operaționale și a documentației tehnice.

13.6. Stabilirea priorităților de intervenție în funcție de impactul asupra activităților medicale și administrative.

13.7. Coordonarea colaborării tehnice cu furnizorii și fundamentarea necesarului de modernizare a infrastructurii informatice.

13.8. Monitorizarea indicatorilor de performanță ai serviciului și raportarea către conducerea spitalului.

Bibliografie: L2, L3, L5, T10–T12.

ÎNTOCMIT
DIRECTOR MEDICAL