Anexa 10 la nr._____ din _____*(după aprobarea conducătorului instituţiei se va completa olograf numărul şi data documentaţiei de securitate)*

-MODEL-

Lista vulnerabilităţilor asociate ameninţărilor,
la adresa securităţii *SIC [DENUMIRE SISTEM]*

(coloana nivelului de risc se va completa fiind avut în vedere nivelul riscului calculat în funcţie de probabilitatea de producere a unui eveniment nedorit şi impactul acestui eveniment asupra securităţii SIC [DENUMIRE SISTEM]. Determinarea nivelului riscului pentru fiecare eveniment nedorit care poate avea impact asupra SIC [DENUMIRE SISTEM] sau asupra informaţiilor, se realizează după implementarea măsurilor de securitate din ANEXA 11, cu ajutorul matricei nivelului de risc din ANEXA 5.)

Vulnerabilitatea	Ameninţarea	Valori afectate	Nivel risc
Existenţa de materiale inflamabile	Incendiu	Hardware Date	
Lipsa fişierelor de backup	Cutremur Incendiu Inundaţie Interferenţe electronice Temperaturi extreme şi umiditate Fluctuaţii ale tensiunii de alimentare Căderi ale tensiunii de alimentare Erori de transfer Utilizare software neautorizat Modificări neautorizate ale software-ului Virusare Utilizare software fără licenţă Nefuncţionarea instalaţiilor auxiliare	Software	
Interfaţa de utilizator complicată	Erori umane neintenţionate	Date	
Managementul necorespunzător al configuraţiei	Disfuncţionalităţi tehnice Sabotaj Furt şi fraudă Erori umane neintenţionate Erori de programare	Hardware Software Date	
Întreţinere defectuoasă a instalaţiilor auxiliare	Disfuncţionalităţi tehnice	Hardware	
Control inadecvat al distribuţiei de software	Utilizare software neautorizat Virusare Utilizare software fără licenţă	Date Software	
Instruire necorespunzătoare a	Virusare	Software	

Vulnerabilitatea	Ameninţarea	Valori afectate	Nivel risc
personalului privind protecţia antivirus		Date	
Măsuri inadecvate privind monitorizarea condiţiilor de mediu	Temperaturi şi umiditate extreme	Hardware Software Date	
Neraportarea funcţionării defectuoase a software-ului	Modificări neautorizate ale software-ului Virusare	Software Date	
Drepturi neautorizate de acces	Sabotaj	Software	
Configurarea necorespunzătoare a facilităţilor de securitate ale aplicaţiilor	Distrugeri intenţionate ale datelor, sabotaj Furt şi fraudă Virusare Falsificarea identităţii	Date	
Sistem de operare configurat necorespunzător	Virusare Modificări neautorizate ale software-ului Distrugeri intenţionate ale datelor, sabotaj Falsificarea identităţii	Software Date	
Măsuri de securitate implementate necorespunzător	Refuzul serviciului Modificări neautorizate ale software-ului Distrugeri intenţionate ale datelor, sabotaj Furt şi fraudă Virusare Falsificarea identităţii	Software Date	
Pregătire de specialitate necorespunzătoare a personalului SIC	Erori umane neintenţionate	Hardware Software Date	
Absenţa unui inventar al resurselor sistemului	Acces neautorizat la resurse	Hardware Date	
Absenţa sistemului automat de stingere a incendiilor	Incendiu	Hardware Software Date	
Absenţa comunicării între compartimentul Resurse Umane al instituţiei şi administratorii sistemului privind personalul SIC care a	Distrugeri intenţionate ale datelor, sabotaj Distrugeri intenţionate, furturi ale echipamentelor Virusare	Software Date	

Vulnerabilitatea	Ameninţarea	Valori afectate	Nivel risc
părăsit instituţia, pentru actualizarea permisiunilor de acces			
Absenţa mecanismelor de identificare şi autentificare	Falsificarea identităţii	Hardware Software	
Securitate fizică precară	Incendiu Distrugeri intenţionate ale datelor, sabotaj Distrugeri intenţionate, furturi ale echipamentelor Furt şi fraudă Acces neautorizat la resurse Falsificarea identităţii	Hardware Date	
Accesul neautorizat la resursele hardware	Distrugeri intenţionate, furturi ale echipamentelor Utilizare software neautorizat	Hardware Date	
Neprotejarea parolelor de către utilizatori	Distrugeri intenţionate ale datelor, sabotaj Utilizare software neautorizat Falsificarea identităţii	Hardware Software	
Absenţa politicilor conform cărora orice cerere de acces la informaţii este permisă numai după verificarea identităţii solicitantului	Inginerie sociala Distrugeri intenţionate ale datelor, sabotaj	Hardware Software Date	
Lipsa politicii privind utilizarea numai a software-ului licenţiat	Utilizare software fără licenţă Virusare	Software	
Lipsa politicii de restricţionare a informaţiilor transmise telefonic	Inginerie socială	Software Date	
Absenţa actualizării regulate a software-ului antivirus	Virusare	Software Date	
Lipsa restricţiilor de timp pentru accesul utilizatorilor	Falsificarea identităţii	Date	
Lipsa mesajelor de atenţionare a utilizatorilor	Erori umane neintenţionate Disfuncţionalităţi tehnice	Software Hardware	
Lipsa/nefuncţionarea echipamentelor de asigurare a microclimatului	Temperaturi extreme	Software Date Hardware Personal SIC	

Vulnerabilitatea	Ameninţarea	Valori afectate	Nivel risc
Localizarea SIC într-o zonă susceptibilă de dezastre naturale	Cutremur Incendiu Inundaţie	Software Date Hardware Personal SIC	
Lipsa echipamentelor de protecţie împotriva fluctuaţiilor tensiunii de alimentare	Fluctuaţii ale tensiunii de alimentare	Software Date Hardware	
Lipsa planurilor de continuare a activităţii sau a procedurilor de recuperare/refacere a informaţiilor	Cutremur Incendiu Inundaţie Interferenţe electronice Temperatură şi umiditate extremă Fluctuaţii ale tensiunii de alimentare Disfuncţionalităţi tehnice Erori de transfer Distrugeri intenţionate ale datelor, sabotaj Distrugeri intenţionate, furturi ale echipamentelor Furt şi fraudă Căderi ale tensiunii de alimentare	Software Date Hardware	
Lipsa surselor neîntreruptibile de alimentare cu energie electrică	Căderi ale tensiunii de alimentare	Hardware Date	
Nerespectarea procedurilor operaţionale de acces la sistem	Furt şi fraudă	Date Software	
Nerespectarea procedurilor privind transferul de date prin intermediul mediilor de stocare neînregistrate	Furt şi fraudă Pierderea, furtul documentelor sau a mediilor de stocare	Date	
Deficienţele sau absenţa unui sistem de audit	Disfuncţionalităţi tehnice Furt şi fraudă Erori umane neintenţionate	Software Date	
Necriptarea parolelor	Falsificarea identităţii	Hardware Software	
Utilizarea unor echipamente portabile în reţea	Acces neautorizat la resurse	Date	
...	...	...	...