**Referat de aprobare**
**referitor la proiectul de Normă privind guvernanța și securitatea sistemelor de tehnologia informațiilor și a comunicațiilor**

## I. Sumar

Proiectul de *Normă privind guvernanța și securitatea sistemelor de tehnologia informațiilor și a comunicațiilor*, supus consultării publice, are la bază Ghidul EIOPA BoS-20/600 privind guvernanța și securitatea în domeniul tehnologiei informațiilor și a comunicațiilor (TIC).

## II. Expunere de motive

Proiectul de normă abordează următoarele aspecte:

*1. Responsabilitatea conducerii societăților*

Conducerii societăților îi revine responsabilitatea pentru stabilirea și punerea în practică a strategiei TIC și a strategiei privind continuitatea activităților TIC, pentru instruirea personalului, pentru aprobarea raportului de managementul riscului TIC și pentru adoptarea de decizii pe baza acestuia.

*2. Guvernanța sistemelor TIC, inclusiv în ceea ce privește externalizarea*

Elaborarea de politici și proceduri are drept scop aplicarea în mod corect a strategiilor adoptate prin configurarea sistemelor TIC în funcție de obiectivele privind securitatea cibernetică, de dependențele existente și prin stabilirea unor criterii privind achiziționarea sau dezvoltarea internă a sistemelor TIC.

*3. Procesul de management al riscului TIC*

Nivelul toleranței la riscurile TIC se stabilește în concordanță cu strategia de risc adoptată și în funcție de acesta se stabilesc modalitățile de identificare, evaluare, gestionare, minimizare și raportare a riscurilor respective.

*4. Managementul operațiunilor TIC*

Stabilirea clară a modalităților în care sistemele și serviciile TIC sunt derulate, monitorizate și controlate permite identificarea promptă a fiecărui element TIC în ceea ce privește proprietarul, localizarea și clasificarea acestuia din punctul de vedere al securității cibernetice. De asemenea, este necesar a se stabili criterii adecvate și praguri de semnificație pentru încadrarea evenimentelor drept incidente și mecanisme de avertizare timpurie pentru detectarea în timp util a incidentelor.

*5. Securitatea cibernetică*

Politicile privind securitatea cibernetică stabilesc principii și reguli pentru a se asigura respectarea confidențialității, integralității și disponibilității activelor TIC și prevăd desemnarea persoanelor cărora li se alocă atribuțiile funcției de securitate cibernetică, funcție independentă de funcțiile operaționale și de cele de dezvoltare a sistemelor TIC.

*6. Securitatea tehnică și fizică*

Procedurile privind securitatea tehnică asigură managementul identității utilizatorilor care au acces la sistemele TIC, iar cele privind securitatea fizică prevăd condițiile în care este permis accesul fizic la sistemele TIC, măsurile pentru prevenirea accesului neautorizat în sediu și măsurile pentru prevenirea deteriorării sistemelor TIC din cauze externe, independente de factorul uman.

*7. Planurile pentru asigurarea continuității activității*

Planurile respective prevăd realizarea unor analize de impact pe bază de scenarii pentru a evalua efectele cantitative și calitative ale unor disfuncționalități severe, modalitatea de reacție și de recuperare a sistemelor TIC și a serviciilor TIC astfel încât să se minimizeze efectele negative asupra activității.

*8. Monitorizarea securității cibernetice și a planurilor pentru asigurarea continuității activității*

Securitatea cibernetică și planurile pentru asigurarea continuității activității se monitorizează și periodic se efectuează teste și se elaborează un raport pe baza căruia se adoptă decizii și se instituie mecanisme de control.

*9. Dezvoltarea internă a sistemelor TIC sau achiziționarea acestora*

Politicile referitoare la dezvoltarea internă a sistemelor TIC sau achiziționarea acestora au drept scop menținerea sistemelor respective astfel încât acestea să respecte cerințele de securitate cibernetică privind confidențialitatea, integralitatea și disponibilitatea informațiilor.

Societățile au la dispoziție o perioadă care se încheie la 31 decembrie 2021 pentru a revizui sistemul de guvernanță instituit, politicile, procedurile și contractele de externalizare în vederea efectuării modificărilor necesare pentru conformarea cu noile prevederi.