Secció III. Altres disposicions i actes administratius

ADMINISTRACIÓ DE LA COMUNITAT AUTÒNOMA
CONSELLERIA D'ECONOMIA, HISENDA I INNOVACIÓ

374 ***Acord del Consell Rector de l'Institut d'Estadística de les Illes Balears pel qual s'aprova la política de seguretat de la informació de l'Institut***

D'acord amb l'article 30.32 de l'Estatut d'autonomia de les Illes Balears, la Comunitat Autònoma té competència exclusiva en les estadístiques d'interès per a la comunitat autònoma i en l'organització i gestió d'un sistema estadístic propi.

La Llei 3/2002, de 17 de maig, d'estadística de les Illes Balears, va crear, mitjançant l'article 32, l'Institut d'Estadística de les Illes Balears (IBESTAT) com a organisme autònom adscrit a la conselleria competent en matèria d'economia. Les funcions de l'Institut es recullen en l'article 34 de la Llei 3/2002 esmentada, les quals suposen assumir la planificació, la normalització, la coordinació i la gestió del sistema estadístic de les Illes Balears, així com dur a terme les activitats estadístiques que se li encomanin en els programes anuals d'estadística, i promoure la difusió de les estadístiques relatives a la comunitat autònoma de les Illes Balears.

D'altra banda, l'article 13 de la Llei 39/2015, d'1 d'octubre, del procediment administratiu comú de les administracions públiques, estableix els drets de les persones en les seves relacions amb les administracions públiques; concretament en la lletra *h)* estableix el dret a la seguretat i la confidencialitat de les dades que figurin en els fitxers, sistemes i aplicacions de les administracions públiques.

La Llei 40/2015, d'1 d'octubre, de règim jurídic del sector públic, ha ampliat l'àmbit d'aplicació de l'Esquema Nacional de Seguretat (ENS) a tot el sector públic, i estableix en l'article 3, relatiu als principis generals, la necessitat que les administracions públiques es relacionin entre si i amb els seus òrgans, organismes públics i entitats vinculats o dependents a través de mitjans electrònics, que garanteixin la interoperabilitat i la seguretat de les solucions i els sistemes adoptats per cadascuna i la protecció de les dades personals, i facilitin la prestació de serveis als interessats preferentment per aquests mitjans, i assenyala l'ENS com a instrument fonamental per assolir aquests objectius en l'article 156.
L'IBESTAT depèn dels sistemes basats en les tecnologies de la informació i la comunicació (TIC) per aconseguir els seus objectius. Aquests sistemes s'han d'administrar amb diligència, i s'han de prendre les mesures adequades per protegir-los contra danys accidentals o deliberats que puguin afectar la disponibilitat, la traçabilitat, l'autenticitat, la integritat o la confidencialitat de la informació tractada o dels serveis prestats. L'objectiu de la seguretat de la informació és garantir la qualitat de la informació i la prestació continuada dels serveis, actuant preventivament, supervisant l'activitat diària i reaccionant amb prestesa als incidents.

Els diferents departaments han de garantir que la seguretat de les TIC és una part integral de cada etapa del cicle de vida del sistema, des de la concepció fins a la retirada de servei, passant per les decisions de desenvolupament o adquisició i les activitats d'explotació. Els requisits de seguretat i les necessitats de finançament han de ser identificats i inclosos en la planificació, en la sol·licitud d'ofertes i en els plecs de licitació per a projectes de TIC. La informació i els serveis prestats estan sotmesos a amenaces i riscs provinents d'accions malintencionades o il·lícites, errors o fallades i accidents o desastres.

L'Esquema Nacional de Seguretat, regulat pel Reial decret 311/2022, de 3 de maig, determina la política de seguretat que s'ha d'aplicar en la utilització dels mitjans electrònics. L'ENS està constituït pels principis bàsics i els requisits mínims per a una protecció adequada de la informació. L'adequació ordenada a l'ENS requereix el tractament de les qüestions següents:

a) Preparar i aprovar la política de seguretat, incloent-hi la definició de rols i l'assignació de responsabilitats.
b) Categoritzar els sistemes atenent a la valoració de la informació manejada i dels serveis prestats.
c) Dur a terme l'anàlisi de riscs, incloent-hi la valoració de les mesures de seguretat existents.
d) Preparar i aprovar la declaració d'aplicabilitat de les mesures de l'annex II de l'ENS.
e) Elaborar un pla d'adequació per millorar la seguretat, sobre la base de les insuficiències detectades, que ha d'incloure terminis estimats d'execució.
f) Implantar, operar i monitorar les mesures de seguretat a través de la gestió continuada de la seguretat corresponent.
g) Auditar la seguretat.
h) Informar sobre l'estat de la seguretat.

D'acord amb l'article 12 del Reial decret 311/2022 esmentat, cada administració pública ha de disposar d'una política de seguretat formalment aprovada per l'òrgan competent. Així mateix, cada òrgan o entitat amb personalitat jurídica pròpia comprès en l'àmbit subjectiu de l'article 2 del Reial decret esmentat ha de disposar d'una política de seguretat formalment aprovada per l'òrgan competent.

La Comissió Directora de Seguretat de la Informació de la Comunitat Autònoma de les Illes Balears va emetre l'informe corresponent sobre

l'esborrany de la política de seguretat de l'IBESTAT en la sessió de 28 d'octubre de 2024, d'acord amb el Decret 97/2006, de 24 de novembre, pel qual es creen i es regulen les comissions per a la millora contínua de la seguretat de la informació en l'Administració de la Comunitat Autònoma de les Illes Balears.

Per tot això, el Consell Rector en la sessió del dia 17 de desembre de 2024 adopta el següent

Acord

Primer. Aprovar la política de seguretat de la informació de l'Institut d'Estadística de les Illes Balears, que s'incorpora com annex a aquest Acord.

Segon. Disposar que aquest Acord, juntament amb l'annex, es publiqui en el *Butlletí Oficial de les Illes Balears* i en el portal web de l'IBESTAT.

Tercer. Establir que aquest Acord produeixi efectes des de la data de la publicació en el *Butlletí Oficial de les Illes Balears*.

Palma, en la data de la signatura electrònica *(14 de gener de 2025)*

La secretària suplent del Consell Rector de l'IBESTAT
Laura Alomar Llorente

ANNEX
Política de seguretat de la informació de l'Institut d'Estadística de les Illes Balears

1. Objecte

1.1. Constitueix l'objecte d'aquest Acord fixar la política de seguretat de la informació (PSI) en l'àmbit de l'Institut d'Estadística de les Illes Balears (IBESTAT), així com establir el marc organitzatiu, operacional i tecnològic d'aquesta entitat.

1.2. La política de seguretat de la informació identifica responsabilitats i estableix principis i directrius per assolir una protecció apropiada i consistent dels serveis i actius d'informació gestionats per mitjà de les tecnologies de la informació i la comunicació (TIC).

1.3. La política de seguretat de la informació és l'instrument en què es basa l'IBESTAT per assolir els seus objectius emprant de manera segura els sistemes d'informació i les comunicacions. La seguretat, concebuda com a procés integral, comprèn tots els elements tècnics, humans, materials i organitzatius relacionats amb els sistemes d'informació i les comunicacions, i cal entendre-la no com un producte, sinó com un procés continu d'adaptació i millora, que ha de ser controlat, gestionat i monitorat amb la implantació de la cultura de la seguretat a l'IBESTAT.

2. Àmbit d'aplicació

2.1. La PSI és de compliment obligat per a totes les persones responsables de l'IBESTAT tant en el camp de la gestió com en el tècnic; també és de compliment obligat per a tot el personal que accedeixi tant als sistemes d'informació com a la mateixa informació que gestioni cada àrea, amb independència de quina sigui la destinació, l'adscripció o la relació amb l'àrea.

2.2. Aquesta política és d'aplicació i de compliment obligat per a totes les àrees i serveis de l'IBESTAT i també n'afecta tots els recursos i els processos inclosos en el Reial decret 311/2022, de 3 de maig, pel qual es regula l'Esquema Nacional de Seguretat, ja siguin interns o externs, vinculats a l'entitat a través de contractes o acords amb tercers.

2.3. Aquesta política s'ha d'aplicar als sistemes d'informació de l'IBESTAT que estan relacionats amb la prestació de serveis per mitjans electrònics a la ciutadania, amb el compliment de deures per mitjans electrònics o amb l'accés a la informació o al procediment administratiu i que es troben dins l'abast de l'Esquema Nacional de Seguretat (ENS).

3. Missió

L'IBESTAT és l'òrgan central d'estadística de la Comunitat Autònoma de les Illes Balears, creat per la Llei 3/2002, de 17 de maig, d'estadística de les Illes Balears. Entre les funcions que determinen la seva missió destaquen les següents:

a) Dur a terme les activitats estadístiques que li assignin els plans i els programes estadístics aprovats pel Govern de les Illes Balears,

amb independència tècnica i professional, atenent al fet insular i altres desagregacions territorials, i complint els principis establerts en el Codi de bones pràctiques de les estadístiques europees.
b) Coordinar l'activitat estadística autonòmica com a responsable de la promoció, la gestió i la coordinació del Sistema Estadístic de les Illes Balears (SESTIB). En aquest sentit, confecciona la proposta de plans i programes estadístics que aprovarà el Govern de les Illes Balears.
c) Establir tots els elements tècnics necessaris per desplegar l'article 30.32 de l'Estatut d'autonomia referent a la competència exclusiva en matèria estadística d'interès de la comunitat autònoma, d'acord amb la Llei d'estadística autonòmica esmentada i l'altra normativa estadística que la pugui afectar.

4. Objectius

4.1. Són objectius generals de l'IBESTAT els següents:

a) Establir un marc de gestió de la seguretat de la informació adequat al Reial decret 311/2022 i reconèixer així com a actius estratègics la informació i els sistemes que la suporten.
b) Establir les bases sobre les quals el personal de l'IBESTAT i la ciutadania poden accedir als serveis en un entorn de gestió segur, anticipant-ne les necessitats i preservant-ne els drets.
c) Protegir la informació d'un ventall ampli d'amenaces, amb la finalitat de garantir la continuïtat dels sistemes d'informació, minimitzar els riscs de dany i assegurar el compliment eficient dels objectius de l'IBESTAT.
d) Garantir el funcionament adequat de les activitats de control, monitoratge i manteniment de les infraestructures i les instal·lacions generals, necessàries per prestar serveis de manera adequada, així com de la informació derivada d'aquest funcionament.

4.2. Són objectius específics de l'IBESTAT els següents:

a) Contribuir des de la gestió de la seguretat de la informació al compliment de la missió i els objectius establerts per a l'IBESTAT.
b) Disposar de les mesures de control necessàries per complir els requisits legals que siguin d'aplicació com a conseqüència de l'activitat desenvolupada, especialment pel que fa a la protecció de dades de caràcter personal i a la prestació de serveis a través de mitjans electrònics.
c) Assegurar l'accés, la integritat, la confidencialitat, la disponibilitat, l'autenticitat i la traçabilitat de la informació i la prestació continuada dels serveis, actuant preventivament, supervisant l'activitat diària i reaccionant amb rapidesa als incidents.
d) Protegir els recursos d'informació de l'IBESTAT i la tecnologia emprada per processar-los contra amenaces, internes o externes, deliberades o accidentals, amb la finalitat d'assegurar el compliment de la confidencialitat, la integritat, la disponibilitat, la legalitat i la fiabilitat de la informació.

5. Revisió de la política de seguretat de la informació

5.1. El Comitè per a la Gestió i la Coordinació de la Seguretat de la Informació (d'ara endavant, Comitè) ha de proposar, revisar i difondre la PSI, amb el suport de la persona responsable de seguretat, que ha de vetlar activament per conservar-la, actualitzar-la i difondre-la entre totes les parts afectades.

5.2. La política de seguretat de la informació s'ha de revisar un cop l'any i sempre que hi hagi canvis rellevants en l'organització, amb la finalitat d'assegurar que s'adequa a l'estratègia i les necessitats de l'organització.

5.3. En cas de conflictes o diferents interpretacions d'aquesta política, la direcció de l'IBESTAT és l'òrgan competent per resoldre'ls.

6. Marc normatiu

S'agafa com a referència bàsica en matèria de seguretat de la informació la normativa relacionada amb el Codi del dret de la ciberseguretat establert pel Ministeri de la Presidència, Relacions amb les Corts i Memòria Democràtica, en què es detalla tota la normativa aplicable, entre les quals es troben les normatives següents, enunciades a títol informatiu no limitatiu:

— Reglament (UE) núm. 2016/679, del Parlament Europeu i del Consell, de 27 d'abril de 2016, relatiu a la protecció de les persones físiques pel que fa al tractament de dades personals i a la lliure circulació d'aquestes dades i pel qual es deroga la Directiva 95/46/CE (Reglament general de protecció de dades).
— Llei orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals.
— Llei 25/2007, de 18 d'octubre, de conservació de dades relatives a les comunicacions electròniques i a les xarxes públiques de comunicacions.
— Llei 37/2007, de 16 de novembre, sobre reutilització de la informació del sector públic.
— Llei 56/2007, de 28 de desembre, de mesures d'impuls de la societat de la informació.
— Llei 19/2013, de 9 de desembre, de transparència, accés a la informació pública i bon govern.
— Llei 39/2015, d'1 d'octubre, del procediment administratiu comú de les administracions públiques.

— Llei 40/2015, d'1 d'octubre, de règim jurídic del sector públic.
— Llei 9/2017, de 8 de novembre, de contractes del sector públic, per la qual es transposen a l'ordenament jurídic espanyol les directives del Parlament Europeu i del Consell 2014/23/UE i 2014/24/UE, de 26 de febrer de 2014.
— Llei 6/2020, d'11 de novembre, reguladora de determinats aspectes dels serveis electrònics de confiança.
— Llei 11/2022, de 28 de juny, general de telecomunicacions.
— Reial decret llei 14/2019, de 31 d'octubre, pel qual s'adopten mesures urgents per raons de seguretat pública en matèria d'administració digital, contractació del sector públic i telecomunicacions.
— Reial decret legislatiu 1/1996, de 12 d'abril, pel qual s'aprova el Text refós de la Llei de propietat intel·lectual.
— Reial decret legislatiu 5/2015, de 30 d'octubre, pel qual s'aprova el Text refós de la Llei de l'Estatut bàsic de l'empleat públic.
— Reial decret 1553/2005, de 23 de desembre, pel qual es regula el document nacional d'identitat i els seus certificats de signatura electrònica.
— Reial decret 4/2010, de 8 de gener, pel qual es regula l'Esquema Nacional d'Interoperabilitat en l'àmbit de l'administració electrònica.
— Reial decret 203/2021, de 30 de març, pel qual s'aprova el Reglament d'actuació i funcionament del sector públic per mitjans electrònics.
— Reial decret 311/2022, de 3 de maig, pel qual es regula l'Esquema Nacional de Seguretat en l'àmbit de l'administració electrònica.
— Resolució de 7 d'octubre de 2016 de la Secretaria d'Estat d'Administracions Públiques per la qual s'aprova la Instrucció tècnica de seguretat de l'informe de l'estat de la seguretat.
— Resolució de 13 d'octubre de 2016 de la Secretaria d'Estat d'Administracions Públiques per la qual s'aprova la Instrucció tècnica de seguretat de conformitat amb l'Esquema Nacional de Seguretat.
— Resolució de 27 de març de 2018 de la Secretaria d'Estat de Funció Pública per la qual s'aprova la Instrucció tècnica de seguretat de l'auditoria de la seguretat dels sistemes d'informació.
— Resolució de 13 d'abril de 2018 de la Secretaria d'Estat de Funció Pública per la qual s'aprova la Instrucció tècnica de seguretat de notificació d'incidents de seguretat.
— Llei 3/2002, de 17 de maig, d'estadística de les Illes Balears.
— Llei 7/2010, de 21 de juliol, del sector públic instrumental de la Comunitat Autònoma de les Illes Balears.
— Decret 128/2007, de 5 d'octubre, d'organització i funcionament de l'Institut d'Estadística de les Illes Balears.
— Decret 8/2021, de 9 de febrer, sobre la transparència i el dret d'accés a la informació pública.
— Decret 31/2023, de 22 de maig, pel qual s'estableix l'organització administrativa en matèria de transparència i es desenvolupa l'exercici del dret d'accés a la informació pública en l'Administració de la Comunitat Autònoma de les Illes Balears i en el seu sector públic instrumental.

7. Principis bàsics en matèria de seguretat de la informació

L'IBESTAT, per aconseguir el compliment de les previsions recollides en el Reial decret 311/2022, ha d'implementar les mesures de seguretat proporcionals a la naturalesa de la informació i els serveis que s'han de protegir i tenint en compte la categoria dels sistemes afectats.

Per això, s'han de tenir en compte els principis bàsics desglossats en el capítol 2 del Reial decret 311/2022:

a) Seguretat com a procés integral.
b) Gestió de la seguretat basada en els riscs.
c) Prevenció, detecció, resposta i conservació.
d) Existència de línies de defensa.
e) Vigilància contínua.
f) Reavaluació periòdica.
g) Diferenciació de responsabilitats.

8. Estructura de la documentació de seguretat

8.1. Sens perjudici del marc normatiu que preveu el punt 6 d'aquest annex, el cos jurídic específic de la PSI d'aquest organisme autònom que sigui de compliment obligat s'ha de desenvolupar en tres nivells, segons l'àmbit d'aplicació i el detall tècnic. Aquests nivells són els següents:

a) Primer nivell: marc comú i directrius bàsiques de la política de seguretat de la informació en l'àmbit de l'administració electrònica de la Comunitat Autònoma de les Illes Balears. Constitueixen aquest primer nivell l'Acord del Consell Rector de l'Institut d'Estadística de les Illes Balears pel qual s'aprova la política de seguretat de la informació de l'Institut i les disposicions, directrius i normes de seguretat generals dins l'àmbit d'aplicació de la PSI que defineix el punt 6 d'aquest annex.
b) Segon nivell: instruccions operatives de seguretat de la informació i instruccions de les TIC. Aquestes instruccions donen resposta, sense entrar en detalls d'implementació ni tecnològics, al que es pot fer i al que no es pot fer en relació amb un determinat tema des del punt de vista de la seguretat, què es considera un ús apropiat o inapropiat, o quines conseqüències es deriven de l'incompliment,

entre altres aspectes. Els documents relatius a aquest segon nivell els ha d'elaborar el Comitè i els ha d'aprovar la persona titular de la direcció de l'IBESTAT, a proposta de la persona responsable de seguretat.

c) Tercer nivell: instruccions tècniques de seguretat de les tecnologies de la informació i la comunicació (STIC). Són documents que donen resposta, incloent-hi detalls d'implementació i tecnològics, a la manera com es pot dur a terme una determinada tasca, respectant els principis de seguretat de l'organització i els processos interns establerts. Els documents relatius a aquest tercer nivell els ha d'elaborar el Comitè i els ha d'aprovar la persona titular de la direcció de l'IBESTAT, a proposta de la persona responsable de seguretat.

8.2. A més dels documents esmentats en l'apartat anterior, la documentació de seguretat del sistema pot disposar, sota el criteri de la persona responsable de seguretat, d'altres documents de caràcter no vinculant: recomanacions, bones pràctiques, informes, registres o evidències electròniques, entre altres aspectes.

9. Desenvolupament de la política de seguretat de la informació

Aquesta política de seguretat de la informació s'ha de desplegar mitjançant normativa de seguretat que tracti aspectes específics. La normativa de seguretat ha d'estar a disposició de tots els membres de l'organització que necessitin conèixer-la, en particular per als que utilitzin, operin o administrin els sistemes d'informació i les comunicacions.

Les normes i els procediments han de preveure, almenys, els aspectes següents:

a) Protecció de dades de caràcter personal: s'han d'implantar mesures tècniques i organitzatives que permetin complir els requisits normatius en aquesta matèria.

b) Gestió d'actius d'informació: els actius d'informació s'han d'inventariar, categoritzar i associar a un responsable.

c) Seguretat lligada als recursos humans: la seguretat lligada al personal és fonamental per reduir els riscs d'errors humans, robatoris, fraus o mal ús de les instal·lacions i els serveis, per la qual cosa s'han d'implantar els mecanismes que permetin als usuaris conèixer les seves responsabilitats i com complir-les.

d) Seguretat física: les instal·lacions de l'IBESTAT han de mantenir una correcta seguretat física per evitar els accessos no autoritzats, així com qualsevol altre tipus de dany o interferència externa.

e) Seguretat lògica: s'han d'establir mesures organitzatives i tècniques per controlar els accessos, protegir davant codis nocius, assegurar les comunicacions, fer còpies de seguretat, etc.

f) Gestió d'incidents de seguretat: s'han d'establir responsabilitats i procediments de gestió d'incidències per assegurar una resposta ràpida, eficaç i ordenada als esdeveniments en matèria de seguretat.

10. Gestió i accés a la documentació del sistema

10.1. L'IBESTAT desenvolupa la política de gestió i conservació dels documents electrònics que s'implementa mitjançant normes internes, procediments i instruccions tècniques.

10.2. S'ha de disposar d'un sistema per gestionar l'elaboració, l'aprovació, la conservació, l'estructura i l'accés, entre d'altres, dels documents del sistema de gestió de la seguretat aplicat sobre els sistemes d'informació.

11. Organització de la gestió de la PSI

11.1. L'organització de la seguretat queda establerta mitjançant la identificació i la definició de les diferents activitats i responsabilitats en matèria de gestió de la seguretat dels sistemes i la implantació d'una estructura que les suporti.

11.2. Totes i cadascuna de les persones usuàries dels sistemes d'informació de l'IBESTAT són responsables de la seguretat dels actius d'informació, per la qual cosa han de fer-ne sempre un ús correcte, d'acord amb les seves atribucions professionals.

11.3. Per respondre millor a incidents de seguretat, l'IBESTAT ha de mantenir relacions de cooperació en matèria de seguretat amb les autoritats competents, els proveïdors de serveis informàtics o de comunicació, així com amb organismes públics o privats dedicats a promoure la seguretat dels sistemes d'informació.

11.4. L'estructura organitzativa per gestionar la seguretat de la informació en l'àmbit descrit en aquesta PSI de l'IBESTAT està integrada pels òrgans i els agents següents:

a) Comitè per a la Gestió i la Coordinació de la Seguretat de la Informació.
b) Responsable de la informació.
c) Responsable del servei.
d) Responsable de seguretat.
e) Responsable del sistema.

12. Comitè per a la Gestió i la Coordinació de la Seguretat de la Informació

12.1. Es crea el Comitè per a la Gestió i la Coordinació de la Seguretat de la Informació com una comissió de treball integrada a l'IBESTAT, i està constituït pels membres següents:

a) Presidència: la persona responsable de la direcció de l'IBESTAT.
b) Secretaria: una persona de l'IBESTAT, amb vincle funcionarial, designada per la presidència, que actua amb veu i sense vot.
c) Vocalies: les persones titulars dels serveis de l'IBESTAT; la persona o l'òrgan designat delegat de protecció de dades, que actua amb independència i no pot participar en les decisions relatives als fins i als mitjans del tractament, i la persona que ocupi el lloc de feina de cap de la Secció I de l'especialitat d'informàtica de l'IBESTAT.

12.2. El Comitè s'ha de regir pel que disposa la Llei 40/2015 per als òrgans col·legiats pel que fa al règim de funcionament en tot allò que no estigui previst en aquest annex.

12.3. El Comitè s'ha de reunir amb caràcter ordinari cada any i amb caràcter extraordinari a proposta de la presidència. No es percebran indemnitzacions en concepte d'assistència a les reunions del Comitè.

12.4. Es pot acordar la constitució de grups de treball per analitzar, elaborar i executar treballs o activitats específiques, dins l'àmbit de les seves funcions. El Comitè ha de conèixer en les sessions del ple el resultats de les actuacions dels grups de treball.

12.5. Corresponen al Comitè les funcions següents:

a) Elaborar els esborranys de modificació i actualització de la PSI.
b) Analitzar els riscs i impulsar-ne l'avaluació.
c) Revisar l'informe anual d'anàlisi de riscs fet per la persona responsable de seguretat.
d) Impulsar l'actualització dels criteris i les directrius sobre seguretat de la informació.
e) Impulsar mesures per millorar i reforçar els sistemes de seguretat i control.
f) Impulsar la difusió i el compliment de la PSI, i promoure activitats de conscienciació i formació en matèria de seguretat per al personal de l'IBESTAT.
g) Elaborar els esborranys de directrius i normes de seguretat generals de l'IBESTAT, que han de complir el marc normatiu d'aquest annex.
h) Elaborar la normativa de seguretat de segon i tercer nivell.
i) Coordinar les decisions i les actuacions de la persona responsable de seguretat, i assessorar per resoldre els possibles conflictes sota el criteri de garantir la seguretat de les infraestructures tecnològiques compartides.
j) Impulsar els projectes per adequar-los al compliment de l'Esquema Nacional de Seguretat.
k) Compartir experiències d'èxit en matèria de seguretat entre els membres del Comitè per vetlar pel compliment de la PSI i la normativa que la desplega.
l) Coordinar totes les activitats relacionades amb la seguretat dels sistemes d'informació.
m) Vetlar perquè la seguretat de la informació sigui part del procés de planificació de l'IBESTAT.
n) Qualsevol altra actuació en matèria de seguretat de la informació que no correspongui específicament a un altre agent.

13. Responsable de la informació

13.1. Les funcions de la persona responsable de la informació que estableix la normativa que regula l'Esquema Nacional de Seguretat corresponen a la direcció de l'IBESTAT.

13.2. Dins el seu àmbit d'actuació, ha de determinar els requisits de la informació tractada, establir les necessitats de seguretat de la informació i fer les valoracions de l'impacte que tindria un incident que n'afectàs la seguretat; a més, té la potestat de modificar el nivell de seguretat requerit.

13.3. Per desenvolupar aquestes funcions, ha de comptar amb la col·laboració de les persones gestores titulars de les unitats a càrrec seu amb rang de servei o equivalent.

14. Responsable del servei

14.1. La tasca de responsable del servei correspon als caps de servei per a les àrees de gestió de les quals són titulars, tal com estableix la normativa que regula l'Esquema Nacional de Seguretat. Concretament els serveis afectats són els següents:

- Producció Estadística
- Difusió Estadística
- Coordinació i Planificació Estadística

14.2. Dins el seu àmbit d'actuació, determina els requisits de seguretat dels serveis prestats.

15. Responsable de seguretat

15.1. Les funcions de la persona responsable de seguretat corresponen a la direcció de l'IBESTAT.

15.2. Determina les decisions per satisfer els requisits de seguretat de la informació i dels serveis, supervisa la implantació de les mesures necessàries per garantir la consecució dels requisits i informa sobre aquestes qüestions.

15.3. L'àmbit d'actuació del responsable de seguretat s'ha de limitar únicament i exclusiva als sistemes d'informació i als serveis de tecnologies de la informació i la comunicació que siguin competència i responsabilitat directa de l'IBESTAT.

15.4. Coordina de manera contínua el desenvolupament de la seguretat de la informació en l'àmbit d'aplicació d'aquest annex, a més d'exercir les funcions específiques següents:

a) Promoure la seguretat de la informació emprada i dels serveis electrònics dels sistemes d'informació.
b) Mantenir la documentació de seguretat actualitzada i organitzada en els sistemes de coneixement corporatius i gestionar els mecanismes per accedir-hi.
c) Proposar al Comitè la normativa de seguretat de segon i tercer nivell.
e) Promoure les activitats de conscienciació i informació en matèria de seguretat en el seu àmbit de responsabilitat.
f) Dur a terme la coordinació i el seguiment de la implantació dels projectes d'adequació a l'Esquema Nacional de Seguretat.
g) Elaborar, amb els responsables dels serveis, les preceptives anàlisis de risc, seleccionar les salvaguardes que s'han d'implantar, revisar el procés de gestió del risc i elevar un informe anual al Comitè.
h) Promoure auditories periòdiques per verificar el compliment de les obligacions en matèria de seguretat de la informació, analitzar els informes d'auditoria i elaborar les conclusions que s'han de presentar a les persones responsables del servei perquè, juntament amb la persona responsable de la informació, adoptin les mesures correctores adients.
i) Coordinar el procés de gestió de la seguretat.
j) Signar la declaració d'aplicabilitat, que comprèn l'aplicació de mesures de seguretat seleccionades per un sistema conforme a l'article 28 del Reial decret 311/2022.
k) Elaborar informes periòdics de seguretat que incloguin els incidents més rellevants de cada període.
l) Determinar la categoria de seguretat dels sistemes d'informació, segons el procediment descrit en l'annex 1 del Reial decret 311/2022, i les mesures de seguretat que s'han d'aplicar d'acord amb l'annex 2 d'aquest Reial decret.
m) Determinar la categoria de seguretat sobre la base de les valoracions que facin els responsables de la informació i del servei conforme a l'annex 1 del Reial decret 311/2022.

15.5. Per exercir les seves funcions, ha de comptar amb el suport del Comitè.

15.6. Atès que el responsable de seguretat recau sobre la direcció de l'IBESTAT, es prendran mesures compensatòries, consistents a dur a terme auditories periòdiques de seguretat o bé documentar i justificar les decisions preses pel Comitè per a la Gestió i la Coordinació de la Seguretat de la Informació.

16. Responsable del sistema

16.1. És responsable del sistema la persona titular del Servei d'Assistència Tècnica i Computacional de l'IBESTAT, atès que és la unitat administrativa que exerceix les competències en matèria de gestió de sistemes d'informació.

16.2. Les funcions de la persona responsable del sistema són les següents:

a) Implantar les mesures necessàries per garantir la seguretat del sistema durant tot el seu cicle de vida, seguint les indicacions de la persona responsable de seguretat.
b) Aprovar totes les modificacions substancials de qualsevol element del sistema.
c) Suspendre el maneig d'una determinada informació o la prestació d'un servei electrònic si és informada de deficiències greus de seguretat amb l'informe previ de la persona responsable d'aquesta informació o servei i de la persona responsable de seguretat. En cas de no arribar a un acord en aquest sentit, s'ha d'atenir al règim de resolució de conflictes previst en el punt 20 d'aquest annex.

17. Obligacions del personal

17.1. Tota persona que presti serveis a l'IBESTAT té l'obligació de conèixer i complir la PSI i la normativa de seguretat derivada, i és responsabilitat del Comitè disposar dels mitjans necessaris perquè la informació estigui disponible per a les persones afectades i comunicar aquesta disponibilitat.

17.2. Totes les persones que emprin o tenguin accés als sistemes tecnològics o d'informació tenen les obligacions següents:

a) Conèixer i respectar la PSI, així com les normes de seguretat i els procediments de seguretat que la despleguen i que l'afecten.
b) Assistir a les accions de conscienciació en matèria de seguretat de la informació que es duguin a terme.
c) Emprar els serveis i els sistemes d'informació, així com la informació que contenguin i a la qual tenguin accés, amb una finalitat professional d'acord amb les tasques encomanades en funció del lloc de treball i les finalitats i els propòsits que van motivar la concessió de l'accés.
d) Vetlar per la confidencialitat de la informació a la qual tenguin accés segons la classificació i les característiques d'aquesta.
e) Notificar actuacions o fets que puguin suposar una incidència de seguretat o evidenciïn una debilitat que pugui implicar incidents posteriors.
f) Col·laborar en la resolució d'incidents de seguretat i en la realització d'accions preventives quan sigui necessària la seva participació.
g) No dur a terme accions intencionades que perjudiquin la seguretat dels sistemes tecnològics o d'informació, ni la informació que contenen.

17.3. L'incompliment d'aquestes obligacions pot ser sancionat de conformitat amb la normativa disciplinària corresponent.

17.4. En cas de persones vinculades a entitats externes, l'ús de sistemes tecnològics o d'informació s'ha de limitar a les tasques o activitats circumscrites en els termes del contracte o acord que regula la relació entre aquesta entitat i l'IBESTAT.

18. Terceres parts

18.1. Quan es prestin serveis a altres organismes o es cedeixi informació a tercers:

a) Se'ls ha de fer participar de la PSI i de les normes de seguretat o procediments de seguretat relacionats amb el servei o la informació afectats.
b) S'han d'establir canals d'informació i coordinació entre les respectives persones responsables de gestió de la seguretat de la informació i establir procediments de seguretat per reaccionar davant els incidents que es puguin dur a terme.

18.2. Quan s'emprin serveis o es manegi informació d'altres organismes o entitats, s'han de procurar canals d'informació i coordinació en matèria de seguretat de la informació.

18.3. En els contractes d'implantació, manteniment o gestió de sistemes o aplicacions informàtiques, de prestació de serveis tecnològics, i també en el cas de contractes de prestació de serveis d'altre tipus que impliqui l'ús de serveis, aplicacions o sistemes informàtics interns, s'han de tenir en compte les mesures i les consideracions de seguretat de la informació que siguin d'aplicació, segons la legislació vigent en la matèria. També s'han de tenir en comptes les mesures i les consideracions de seguretat de la informació que resultin d'aplicació legal, en cas d'acord de cessió de sistemes, aplicacions o accés a serveis d'altres organismes o entitats.

18.4. Quan alguna part no pugui satisfer algun aspecte de la PSI, s'ha de requerir al Comitè un informe sobre els riscs en què es pot incórrer i la forma de tractar-los. En vista d'aquest informe, i abans que es faci efectiva la prestació, l'ús, l'accés o la gestió de què es tracti, les persones responsables de la informació o dels serveis afectats han de decidir sobre l'acceptació del risc residual.

18.5. En tot cas, s'ha de donar compliment tant a la normativa de l'Esquema Nacional de Seguretat com a la normativa en matèria de protecció de dades personals. És d'especial aplicació l'Esquema Nacional de Seguretat als sistemes d'informació de les entitats del sector privat, inclosa l'obligació de disposar de la política de seguretat, quan, d'acord amb la normativa aplicable, i en virtut d'una relació contractual, prestin serveis o proveeixin solucions a l'IBESTAT perquè aquest pugui exercir les seves competències i potestats administratives, de conformitat amb l'article 2.3 del Reial decret 311/2022.

19. Gestió de riscs

19.1. La gestió de riscs és un factor essencial per gestionar correctament la seguretat de la informació, i s'ha de dur a terme de manera contínua sobre els sistemes d'informació, conforme als principis de gestió de la seguretat basada en els riscs de l'article 7 i la reavaluació periòdica de l'article 10 del Reial decret 311/2022.

19.2. La persona responsable de seguretat és l'encarregada de l'anàlisi del risc dels sistemes d'informació gestionats per l'IBESTAT i de seleccionar les mesures que s'han d'implantar. L'informe de l'anàlisi de riscs amb les mesures que conté ha de ser analitzat i revisat pel Comitè.

19.3. Les persones responsables de la informació i del servei són les responsables dels riscs sobre la informació i sobre els serveis respectivament i, per tant, d'acceptar els riscs residuals calculats en l'anàlisi i de fer-ne el seguiment i el control.

19.4. El procés de gestió de riscs, que comprèn les fases de categorització dels sistemes, anàlisi de riscs i selecció de mesures de seguretat que s'han d'aplicar, que han de ser proporcionades als riscs i estar justificades, s'ha de revisar cada any.

19.5. En el cas de riscs que es derivin del tractament de dades personals, la persona responsable del tractament, assessorada per la persona delegada de protecció de dades, ha de dur a terme una anàlisi de riscs i, en els supòsits prevists en la normativa de protecció de dades, una avaluació d'impacte en la protecció de dades. En tot cas, aquestes mesures prevaldran en cas de resultar agreujades respecte de les previstes en el Reial decret 311/2022.

20. Resolució de conflictes

20.1. En cas de conflicte entre les persones responsables de l'estructura organitzativa de la PSI, aquest serà resolt per la persona superior jeràrquicament. Si no n'hi ha, serà resolt per la persona titular de la direcció de l'IBESTAT, un cop escoltat el Comitè.

20.2. En cas de conflicte entre les persones responsables que componen l'estructura organitzativa de la PSI i les definides en la normativa de protecció de dades de caràcter personal, prevaldrà la decisió que presenti un nivell d'exigència més gran respecte a la protecció de dades de caràcter personal segons determini la persona responsable del tractament.

21. Auditoria

21.1. Els sistemes d'informació propis de l'IBESTAT han de ser objecte d'una auditoria ordinària interna o externa que verifiqui el compliment dels requeriments de l'Esquema Nacional de Seguretat. Amb caràcter extraordinari s'ha de fer aquesta auditoria sempre que es duguin a terme modificacions substancials en el sistema d'informació que puguin repercutir en el compliment de les mesures de seguretat requerides.

21.2. Els informes d'auditoria han de restar a disposició del Comitè.

22. Formació i conscienciació

22.1. L'IBESTAT ha de desenvolupar activitats formatives específiques orientades a conscienciar i formar el personal d'aquest organisme autònom, així com difondre la PSI i desplegar-la normativament.

22.2. El Comitè i la persona responsable de seguretat s'han d'encarregar de promoure les activitats de formació i conscienciació en matèria de seguretat.