Manual de seguretat de la informació

20 de juny de 2025

Contingut

Historial de versions:

Versió	Autor	Aprovador	Estat	Motiu del problema/canvi	Data
v1	Negoci Clients Espanya	CEO Negoci Clients	Aprovat	• Primera versió	20/06/2025

1. Introducció

1.1. Finalitat

En aquest Manual de seguretat de la informació (també anomenat "Política de seguretat de la informació de Negoci Clients Espanya") s'estableixen les directrius generals de seguretat de la informació que Negoci Clients Espanya (d'ara endavant, "NCE") ha d'aplicar per protegir-se apropiadament contra amenaces que podrien afectar, en alguna mesura, la confidencialitat, integritat, disponibilitat, traçabilitat i autenticitat de la informació i ocasionar pèrdua o mal ús dels actius, dany de la seva imatge i reputació i/o interrupció dels processos que donen suport al negoci. Al seu torn, es defineixen els objectius de seguretat de la informació.

Mitjançant l'aprovació d'aquest manual, NCE manifiesta la seva determinació i compromís d'assolir un nivell de seguretat de la informació adequat a les seves necessitats que garanteixi la protecció dels actius de manera homogènia i la gestió adequada dels riscos aasociats. Així mateix, es compromet a la millora contínua del Sistema de Gestió de Seguretat de la Informació i al compliment dels objectius marcats i de tota la regulació que li és aplicable, tant interna com externa.

1.2. Àmbit d'aplicació

Aquest document és aplicable, amb caràcter obligatori, a tot el personal de NCE, així com a les entitats col·laboradores que intervenen en la utilització i protecció de la informació propietat de NCE i els sistemes que la suporten. Els incompliments de ciberseguretat, així com les possibles sancions, estan recollits en el conveni col·lectiu d'Iberdrola.

Aquest manual (o Política de seguretat de la informació) ha de ser accessible per a tots els membres de NCE i ha d'estar disponible per a les parts interessades.

L'abast de la certificació en l'ENS nivell mitjà i en l'ISO 27001 és: "*El sistema d'informació que dona suport al procés de contractació per canals digitals en negoci Clients Grup - Espanya i al procés de recàrrega pública segons declaració d'aplicabilitat vigent en data d'emissió del certificat*".

1.3. Definicions

Es proporcionen les definicions següents per permetre un enteniment comú dels conceptes de ciberseguretat rellevants inclosos en aquest document:

- **CoE:** Center of Excellence. Departament que té com a propòsit obtenir productes digitals que aportin valor al negoci i al client final.
- **NCE:** Negoci Clients Espanya. És un dels tres principals negocis d'Iberdrola.
- **BISO:** Business Information Security Officer. Ostenta un rol de CISO però de la primera línia de defensa, i es troba en el negoci del qual és BISO.
- **RGPD:** El Reglament general de protecció de dades (RGPD, o GDPR en anglès), és un reglament de la Unió Europea que regula el tractament de dades personals de les persones físiques dins de la UE.

- **SGSI:** El sistema de gestió de la seguretat de la informació és un marc estructurat usat per gestionar, controlar i millorar la seguretat de la seva informació de manera integral.

1.4. Documentació i contactes de referència

- Política de seguretat corporativa.
- Política de riscos de ciberseguretat.
- Política de protecció de dades personals.
- Política de resiliència operativa.
- Sèries CCN-STIC: S'han pres com a referència les normes, instruccions, guies i recomanacions aplicables desenvolupades pel Centre Criptològic Nacional (CCN) per al compliment dels estàndards de seguretat exigits per l'Esquema Nacional de Seguretat.
- ISO/IEC 27014.
- ISO/IEC 27001.
- Codi del bon govern de la ciberseguretat – CNMV.
- Marc de ciberseguretat del Grup Iberdrola.
- ciberseguridad_negocio_clientes_es@iberdrola.es

2. Seguretat de la informació

Les mesures implementades en NCE per salvaguardar la seguretat de la informació tenen com a pedra angular assegurar el següent:

- Confidencialitat: propietat de la informació, per la qual es garanteix que és accessible únicament a personal autoritzat a accedir a aquesta informació.
- Integritat: propietat de la informació, per la qual es garanteix l'exactitud de les dades transportades o emmagatzemades, assegurant que no se n'ha produït l'alteració, la pèrdua o la destrucció, sia de manera accidental o intencionada, per errors de programari o maquinari o per condicions mediambientals.
- Disponibilitat: propietat de la informació, per la qual es garanteix que és accessible i utilitzable pels usuaris o processos autoritzats quan aquests ho requereixin.
- Autenticitat: propietat de la informació, per la qual es garanteix que una entitat és qui diu ser o bé que garanteix la font de la qual procedeixen les dades.
- Traçabilitat: propietat de la informació, per la qual es garanteix que les actuacions d'una entitat es poden imputar exclusivament a aquesta entitat.

Així mateix, es tenen en compte els **principis bàsics** següents:

- Seguretat com a procés integral.

- Gestió de la seguretat basada en els riscos.
- Prevenció, detecció, resposta i recuperació.
- Existència de línies de defensa.
- Vigilància contínua.
- Reavaluació periòdica.
- Diferenciació de responsabilitats.

Finalment, l'actual Manual de seguretat (la Política de seguretat) es desenvolupa tenint en compte els requisits mínims següents (els quals són ampliats als diferents documents que componen el cos normatiu):

- Organització i implantació del procés de seguretat.
- Anàlisi i gestió dels riscos.
- Gestió de personal.
- Professionalitat.
- Autorització i control dels accessos.
- Protecció de les instal·lacions.
- Adquisició de productes de seguretat i contractació de serveis de seguretat.
- Mínim privilegi.
- Integritat i actualització del sistema.
- Protecció de la informació emmagatzemada i en trànsit.
- Prevenció davant altres sistemes d'informació interconnectats.
- Registre de l'activitat i detecció de codi nociu.
- Incidents de seguretat.
- Continuïtat de l'activitat.
- Millora contínua del procés de seguretat.

2.1. Missió, visió i context de l'organització

La missió del Grup es basa en la creació de valor de manera sostenible en el desenvolupament de totes les seves activitats, per als seus accionistes, treballadors, clients i altres grups d'interès i, en general, per als ciutadans i la societat en conjunt. La missió es complementa amb la visió, que reflecteix l'aspiració a ser el grup multinacional líder en el sector energètic que protagonitzi un futur millor creant valor de manera sostenible amb un servei de qualitat per a les persones, de manera eficient, segura, sostenible i respectuosa amb el medi ambient. La missió i la visió del Grup es fonamenten en el ferm compromís, amb uns valors, entre els quals destaquen l'impuls dinamitzador, la força integradora i l'energia sostenible. En aquest darrer valor, la seguretat es posiciona com un pilar essencial per a la seva consecució. Això es tradueix en la consolidació de la seguretat integral com un pilar

fonamental en la presa de decisions d'Iberdrola, promovent contínuament pràctiques de seguretat innovadores i sostenibles en totes les operacions, contribuint d'aquesta manera a la resiliència, la confiabilitat i l'èxit global del Grup en un entorn híbrid en constant transformació.

Negoci Clients Espanya ocupa un lloc destacat dins de l'estratègia empresarial d'Iberdrola, SA (d'ara endavant, "Iberdrola" o l'"Organització"), com una de les seves línies de negoci principals. Aquesta línia se centra en la comercialització i el subministrament d'energia, així com en la provisió de productes i serveis centrats en la descarbonització.

En l'àmbit de Negoci Clients Espanya, Iberdrola es dedica a satisfer les necessitats de l'usuari final, oferint solucions energètiques sostenibles. El seu objectiu és proporcionar energia neta i serveis innovadors que contribueixin a la transició cap a un model energètic més respectuós amb el medi ambient. A més, dins d'aquesta línia de negoci, Iberdrola també exerceix un paper clau en la compravenda d'energia en els mercats a l'engròs, i consolida així la seva posició en el mercat energètic.

Juntament amb Negoci Clients Espanya, Iberdrola desenvolupa altres línies de negoci igualment rellevants. Entre aquestes línies hi ha el Negoci de Xarxes Grup, que es dedica a la construcció, l'operació i el manteniment d'infraestructures elèctriques, com ara línies de transmissió, subestacions i centres de transformació. Aquestes infraestructures són fonamentals per garantir el subministrament eficient d'energia elèctrica des dels centres de producció fins a l'usuari final.

Així mateix, Iberdrola s'involucra activament en el Negoci Renovables Grup, en què s'especialitza en la generació d'energia elèctrica a partir de fonts renovables, com l'energia eòlica, solar tèrmica i fotovoltaica, entre d'altres. Aquesta línia de negoci reflecteix el compromís d'Iberdrola amb la generació d'energia neta i sostenible, i contribueix així a la mitigació del canvi climàtic i la preservació del medi ambient.

Per a més detalls sobre el propòsit corporatiu de la companyia, es poden consultar els recursos publicats Cap a un propòsit corporatiu global - Iberdrola

2.2. Objectius

Així mateix, s'identifiquen els sis objectius de seguretat de la informació, tenint en compte els principis bàsics d'actuació establerts a la Política de seguridad corporativa:

- Govern: Establir i mantenir un model de govern per gestionar i operar la seguretat de la informació a través d'una metodologia orientada a la gestió del risc.
- Identificació: Comprendre l'entorn i identificar els riscos per als seus sistemes, actius, dades i capacitats.
- Protecció: Dissenyar i implementar salvaguardes per minimitzar el nivell de risc en relació amb la materialització d'una possible ciberamenaça.
- Detecció: Monitorar els esdeveniments d'informació de l'Organització i identificar potencials comportaments anòmals que puguin derivar en la materialització d'una possible ciberamenaça.
- Resposta: Dur a terme totes les accions pertinents per gestionar, analitzar, respondre, escalar i mitigar els incidents identificats.

- Recuperació: Restaurar els actius i operacions afectats per un incident de ciberseguretat.

2.3. Organització de la ciberseguretat

Iberdrola s'organitza de manera que es controla i es garanteix la seguretat del sistema de gestió per mitjà de l'assignació, la comunicació i la coordinació dels diferents rols i responsabilitats en matèria de seguretat de la informació a fi de garantir que el sistema de gestió compleixi els requisits exigits en matèria de seguretat de la informació.

2.3.1. Triple línia de defensa Ciberseguretat Global Iberdrola

El sistema de control intern d'Iberdrola i les societats del grup es configuren prenent com a referència les millors pràctiques internacionals. Per això, aquest sistema de control està basat en un assegurament combinat entorn de tres línies de defensa, i proporciona una visió integrada de com les diferents parts de l'Organització interactuen d'una manera efectiva i coordinada, fent més eficaces els processos de gestió i control intern dels riscos rellevants de l'Organització.

A continuació, es proporcionen més detall sobre cadascuna de les línies de defensa:

- Primera línia de defensa: inclou totes les funcions propietàries dels riscos, en aquest sentit, les primeres línies designaran Business Information Security Officers (BISO) que lideraran la definició i supervisaran la implantació d'un pla de ciberseguretat específic per part de les seves organitzacions de negoci, alineat amb l'estratègia, les normes i els marcs generals de ciberseguretat, i s'assegurarà que disposen dels recursos (persones i pressupost) adequats en matèria de ciberseguretat. En aquesta línia es localitzen TAS (IT), els negocis i les àrees corporatives.
- Segona línia de defensa: inclou aquelles funcions que defineixen el marc general de govern i control de la ciberseguretat, estableixen normes, estàndards i criteris globals i suporten i supervisen la implantació dels plans de ciberseguretat de la primera línia, així com la identificació de riscos rellevants. En aquesta línia es localitzen riscos corporatius, seguretat i resiliència corporativa i ciberseguretat.
- Tercera línia de defensa: proporciona el més alt nivell d'independència i objectivitat en l'assegurament de l'eficàcia del govern corporatiu, la gestió de riscos i els controls interns, incloent-hi la forma en què la primera i la segona línia de defensa assoleixen els objectius de gestió i control de riscos. En aquesta línia es localitzen el Departament d'Auditoria Interna, les auditories externes i les auditories reguladores.

2.3.2. El Comitè de Seguretat de la Informació de NCE (1a línia de defensa)

El Comitè de Seguretat de la Informació de NCE és el màxim òrgan de govern de la ciberseguretat al qual assisteix l'Alta Direcció (i els responsables de Servei i Informació), i està liderat pel responsable de seguretat (BISO), que s'encarrega d'establir i supervisar l'estratègia de gestió dels riscos de ciberseguretat. Es reuneix almenys dues vegades a l'any.

Les funcions del Comitè del SG estan recollides al cos normatiu del sistema de gestió de l'organització, encara que destaquen, entre d'altres:

- **Revisar i aprovar l'estratègia** d'evolució de l'organització pel que fa a **seguretat de la informació**.
- **Atendre les inquietuds de la Direcció** de Negoci Clients i dels diferents departaments que siguin convidats al Comitè.
- Servir com a **fòrum per informar regularment de l'estat de la seguretat de la informació a l'Alta Direcció**.
- **Celebrar anualment la reunió de revisió per direcció** exigida per l'ISO 27001 i l'ENS.
- **Revisar i ratificar el model de govern de ciberseguretat**, així com els seus possibles canvis periòdics. Així mateix, **resoldre els conflictes de responsabilitat en matèria de ciberseguretat**.
- **Monitorar i aprovar els resultats de les anàlisis de riscos** periòdiques de ciberseguretat de l'organització.
- **Revisar i ratificar periòdicament la Política de seguretat de la informació** (aquest document) i els diferents documents que componen el cos normatiu.
- **Vetllar pel compliment de la normativa legal** i sectorial aplicable.
- **Promoure la realització de les auditories periòdiques.**
- **Promoure la comunicació, la coordinació d'esforços i la conscienciació** de ciberseguretat.
- **Vetllar** perquè la **seguretat** de la informació **es tingui en compte en els projectes** TIC.
- **Monitorar l'acompliment** dels **processos** de **gestió** d'**incidents** de seguretat.
- **Aprovar plans de millora de la seguretat de la informació de l'organització per aconseguir la millora contínua.**
- **Prioritzar** les **actuacions** en matèria de seguretat.
- **Promoure la millora contínua** del sistema de gestió de la seguretat de la informació.

2.3.3. Rols i responsabilitats de ciberseguretat de la 1a línea de defensa

Alta Direcció

- **Proveir i assegurar que els recursos necessaris** per a la planificació, la implantació, la revisió i la millora del SGSI (Sistema de Gestió de la Seguretat de la Informació) estiguin disponibles, aprovant els pressupostos de ciberseguretat.
- **Assegurar** que les **responsabilitats** per als rols pertinents a la seguretat de la informació **s'assignin i es comuniquin** dins de NCE.
- **Assegurar** que el SGSI **assoleix els objectius i els resultats** de seguretat de la informació i que es compleix la Política de seguretat.
- **Aplicar les mesures per a la gestió de riscos de ciberseguretat i supervisar-ne la implantació efectiva.** Per a això, han d'estar informats de tots els criteris d'acceptació de riscos i els seus corresponents nivells i complir amb tot el que defineixen els procediments interns de gestió de riscos i excepcions.
- **Assegurar** que **s'organitzen periòdicament formacions en matèria de ciberseguretat** per a tots els empleats.
- **Participar** i **promoure** la realització el Comitè de Revisió per part de Direcció (**Comitè de Ciberseguretat de Negoci Clients Espanya**).
- Responsable de vetllar pel compliment de la normativa legal i sectorial d'aplicació.
- **Garantir que es realitzen les auditories internes i externes** necessàries per a la correcta revisió periòdica del SGSI.
- Exercir totes les **funcions** que li **corresponguin** com a **participant** en el **Comitè de Ciberseguretat** de Negoci Clients Espanya.
- **Promoure la millora contínua** de ciberseguretat.

Responsable de la informació i el servei

- **Aprovar**, dins del seu àmbit d'actuació i competències, els **requisits de la informació i servei**.
- **Determinar els nivells de seguretat de la informació i servei**, valorant els impactes dels incidents que afectin la seguretat de la informació. Per a això, el responsable de la informació i el servei sol·licitarà informe del responsable de la seguretat. Els criteris seguits per fixar els nivells de seguretat es trobaran a la guia del CCN-CERT definida a aquest efecte i a la documentació interna d'Iberdrola.
- **Col·laborar** (amb la participació del responsable de la seguretat i el responsable del sistema) **en la participació en la realització de les preceptives anàlisis de riscos** dels actius dels quals és responsable i en la selecció de les salvaguardes que requereix.
- Responsable d'**acceptar els riscos residuals respecte de la informació i els serveis** (o actius) dels quals és responsable calculats a l'anàlisi de riscos.
- **Responsable de l'ús que es faci de la informació** i, per tant, de la seva protecció. Per a això disposarà del suport del responsable de seguretat, el responsable del sistema i el responsable de ciberseguretat del CoE.
- **Assegurar que s'implementen les mesures necessàries sobre els seus actius per tractar de minimitzar els possibles elements adversos que puguin comportar un incident de seguretat** sobre ells. Per a això disposarà del suport del responsable de seguretat, el de ciberseguretat del CoE i de l'equip de ciberseguretat.
- **Assegurar que s'inclouen les especificacions de seguretat en el cicle de vida del seu servei** (i sistemes que el componen), acompanyades dels corresponents procediments de control. Per a això disposarà del suport del responsable de seguretat, el de ciberseguretat del CoE i de l'equip de ciberseguretat.

- **Complir amb les tasques formatives de ciberseguretat** que se li assignin en el pla de formació i conscienciació.

Responsable de seguretat (BISO i responsable del SGSI de NCE):

Màxim responsable de ciberseguretat de NCE, el qual és responsable de determinar les decisions per satisfer els requisits de seguretat de la informació i els serveis. Lidera el report a l'Alta Direcció.

- Com a responsable del sistema de gestió de seguretat de la informació (SGSI), és **responsable de liderar la planificació, implantació, operació, manteniment, supervisió i millora contínua del sistema de gestió de seguretat de la informació.**
- **Mantenir la seguretat de la informació gestionada i dels serveis prestats pels sistemes d'informació en el seu àmbit de responsabilitat**, d'acord amb el que estableix la Política de seguretat de la informació de l'Organització.
- **Definir els objectius** de seguretat de la informació a escala de NCE i els recursos necessaris per poder complir-los i sotmetre'ls a aprovació. Així mateix, s'encarrega de supervisar el compliment d'aquests objectius.
- **Fomentar que la Direcció estigui implicada en la implantació, el manteniment i la millora contínua del SGSI.** Així mateix, liderar el report periòdic de l'estat i el nivell de compliment del SGSI a la Direcció.
- **Elaborar i sotmetre a l'aprovació de l'Alta Direcció l'estratègia** i les polítiques de seguretat, que hauran d'incloure les mesures de gestió de riscos de ciberseguretat, tècniques i organitzatives i proporcionades per gestionar els riscos que es plantegin per a la seguretat de les xarxes i els sistemes d'informació utilitzats i per prevenir i reduir al mínim els efectes dels ciberincidents que afectin l'Organització i els serveis.
- **Dissenyar i implementar el model de govern de ciberseguretat** de NCE.
- **Representar a NCE** (geografia concreta) **en els possibles grups de treball** de ciberseguretat (riscos, cultura, etc.) en l'àmbit d'Espanya i global dins d'Iberdrola.
- **Liderar el Departament de Ciberseguretat i tots els recursos** humans que hi conté.
- **Gestionar els recursos econòmics designats** per al Departament de **Ciberseguretat** de NCE, prioritzant els plans en funció dels recursos disponibles.
- **Supervisar l'estratègia de gestió de riscos**.
- **Report i comunicació de l'estat de la ciberseguretat en l'àrea de NCE a l'Alta Direcció**.
- **Supervisar i desenvolupar l'aplicació del cos normatiu.**Així mateix, dur a terme l'avaluació i la coordinació en la implementació de controls periòdics de seguretat en els sistemes i serveis que li siguin aplicables.
- **Aprovar els documents** que li corresponguin segons els fluxos d'aprovació marcats.
- **Supervisar el compliment de la normativa** aplicable en matèria de seguretat de les xarxes i sistemes d'informació, prenent totes les mesures necessàries per garantir-ne el compliment.
- **Liderar** els processos d'**auditoria** del SGSI.
- Actuar com a **capacitadora de bones pràctiques i estàndards en seguretat** de les xarxes i els sistemes d'informació.
- Elaborar i subscriure el **document d'aplicabilitat** de sistemes o actius.

- **Remetre a les autoritats de control**, a través dels CSIRT nacionals de referència, sense dilació indeguda, **les notificacions d'incidents** que tinguin efectes pertorbadors en la prestació dels serveis i de les vulnerabilitats detectades.
- **Recopilar, preparar i subministrar informació o documentació a l'autoritat de control i als CSIRT nacionals de referència**.
- **Rebre, interpretar i supervisar l'aplicació de les instruccions i guies emanades de l'autoritat de control**, tant per a l'operativa habitual com per a l'esmena de les deficiències observades.
- **Vetllar pel compliment d'empreses externes i proveïdors** dels criteris de seguretat de la informació establerts per l'entitat.
- Definir i aprovar el pla de resposta a incidents de NCE. Així mateix, s'encarrega de **gestionar i liderar els incidents** de ciberseguretat d'acord amb les responsabilitats fixades pels documents que governen la gestió d'incidents.

El responsable de seguretat **no depèn jeràrquicament del responsable de sistemes**.

Responsable de ciberseguretat CoE (Center of Excelence)

Encarregat de gestionar la ciberseguretat dels actius de CoE, **col·laborant** estretament amb el **responsable de seguretat de la informació (BISO)** de NCE en matèria de seguretat, i assegurant la millora contínua de la ciberseguretat del CoE. El detall de les seves funcions es troba recollit al cos normatiu del sistema de gestió de l'Organització.

Responsable de sistemes

Entre les principals responsabilitats destaquen:

- **Gestió** i/o **supervisió** del **desenvolupament, l'operació i el manteniment del sistema** d'informació durant tot el seu cicle de vida. L'operació és responsabilitat directa de Sistemes Corporatius per a aquells actius desplegats en la seva infraestructura.
- **Encarregat de desenvolupar la manera concreta de gestionar la implantació de la seguretat en el sistema definida pel responsable de seguretat** (i el responsable de ciberseguretat del CoE) i de **supervisar-ne l'operació diària**, **la qual poden executar administradors, operadors o sistemes corporatius** (incloent-hi les seves especificacions, la instal·lació i la verificació del seu correcte funcionament).
- **Definir la topologia i la gestió del sistema d'informació**, establint els criteris d'ús i els serveis que hi ha disponibles.
- **Supervisar i assegurar la identificació de vulnerabilitats i amenaces sobre els actius dels quals és responsable**. Per a això, rebrà el suport de l'equip de ciberseguretat.
- **Cerciorar-se** (amb el suport del Departament de Ciberseguretat) **que les mesures de seguretat s'integrin adequadament** en el marc general de seguretat.
- **Adoptar** les mesures correctores adequades d'acord amb les avaluacions i auditories de seguretat.
- **Proposar la suspensió de l'operació d'alguna informació, d'algun servei o del sistema íntegrament**, durant el temps que consideri prudent i **fins a la satisfacció de les modificacions prescrites en el cas d'apreciar deficiències greus de seguretat** que puguin afectar la satisfacció dels requisits establerts. Per a això, pot rebre el suport de l'equip de ciberseguretat. La decisió final, que la prendrà la direcció de l'entitat, s'ha d'acordar amb els responsables de la informació i els serveis afectats i el responsable de la seguretat.
- **Assistir a les tasques formatives de ciberseguretat** que se li assignin en el pla de formació i conscienciació.

Tècnic de ciberseguretat

Les principals responsabilitats del tècnic de ciberseguretat (que formarà part de l'equip de ciberseguretat) són **donar suport en totes les tasques de ciberseguretat que li assigni el responsable de seguretat** (BISO) i/o el r**esponsable de ciberseguretat del CoE**.

Propietari de l'actiu/risc associat

- **Conèixer** tota la **informació rellevant a l'actiu**.
- **Assegurar** que l'**actiu** estigui correctament **inventariat**, classificat i protegit degudament.

- **Definir i revisar periòdicament restriccions d'accés i classificació d'actius** important, tenint en compte les polítiques aplicables de control d'accés.
- Supervisar l'estat dels actius.
- **Conèixer els riscos de seguretat de la informació assignats.**
- **Aprovar el pla de tractament de riscos** de seguretat de la informació.
- **Acceptar els riscos residuals de seguretat** de la informació.
- **Supervisar** l'**estat** dels **riscos**.
- **Mantenir-se actualitzat sobre les amenaces i els riscos emergents**, amb la possibilitat de rebre el suport del responsable de seguretat de la informació (BISO) i de tot el Departament de Ciberseguretat.

Empleats de Negoci Clients Espanya

Les funcions i responsabilitats en matèria de ciberseguretat dels empleats estan recollides en el cos normatiu del sistema de gestió de l'Organització.

La resta dels elements que componen el model de govern de ciberseguretat (organigrama, matriu RASCI, fluxos de comunicació, designació i revocació de rols, etc.) de NCE es troben definits en el cos normatiu del SGSI.

2.4. Marc normatiu

- **Privacitat de dades**
  - Llei orgànica 3/2018, de 5 de desembre, de protecció de dades de caràcter personal.
  - REGLAMENT (UE) 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.

- **Altra legislació nacional**
  - Llei de coordinació i governança de la ciberseguretat, del 2025.
  - Directiva (UE) 2022/2555 del Parlament Europeu i del Consell, de 14 de desembre de 2022, relativa a les mesures destinades a garantir un elevat nivell comú de ciberseguretat en tota la Unió
  - Reial decret legislatiu 1/1996, de 12 d'abril, pel qual s'aprova el text refós de la Llei de propietat intel·lectual.
  - Llei 34/2002, d'11 de juliol, de serveis de la societat de la informació i comerç electrònic.
  - Llei 59/2003, de 19 de desembre, de signatura electrònica.
  - Reial decret d'aprovació de la Llei d'enjudiciament criminal.
  - Llei 10/2021, de 9 de juliol, de treball a distància.
  - Codi civil i penal.

- **Altra legislació o regulació internacional**
  - Normativa PCI – DSS, de juny de 2024.
  - Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities (CER).
  - IA Act.

- **Esquema Nacional de Seguretat**
  - Reial decret 311/2022, de 3 de maig, pel qual es regula l'Esquema Nacional de Seguretat.
  - Guies CCN-STIC.
  - Instruccions tècniques de seguretat de conformitat amb l'Esquema Nacional de Seguretat (Resolució, de 13 d'octubre de 2016, de la Secretaria d'Estat d'Administracions Públiques) i d'Auditoria de la Seguretat dels Sistemes d'Informació (Resolució, de 27 de març de 2018, de la Secretaria d'Estat de Funció Pública).

- **UNE-ISO/IEC 27001**
  - UNE-ISO/IEC 27001:2023 Especificacions per als sistemes de gestió de la seguretat de la informació.
  - UNE-ISO/#EC 27002:2023 Codi de bones pràctiques per a la gestió de la seguretat de la informació.

2.5. Conscienciació i formació

Tot el personal relacionat amb la informació, els serveis i els sistemes d'informació haurà de ser format i informat dels seus deures i obligacions en matèria de seguretat de la informació, per a la implantació i el seguiment d'aquesta política en matèria de seguretat de la informació.

Per garantir la seguretat de les tecnologies de la informació aplicables als sistemes i serveis de NCE, s'articularan els mecanismes necessaris per portar a la pràctica la conscienciació i la formació general i específica necessària i imprescindible en tots els nivells de l'organització de NCE.

2.6. Gestió de riscos

NCE identifica i, si escau, avalua i categoritza els riscos i les oportunitats inherents a les activitats, els processos i els serveis, planificant les accions necessàries per al seu tractament, prevenint els efectes no desitjats i potenciant-ne els efectes favorables.

Els processos d'apreciació de riscos de seguretat de la informació i el seu tractament es troben documentats en documents corporatius i propis de NCE.

En relació amb els riscos que es deriven del tractament de les dades personals, se seguiran tots els documents que regeixen el govern de la gestió de la protecció de dades.

2.7. Revisió i aprovació del document

Aquest manual de seguretat de la informació (que fa de Política de seguretat de la informació per a l'abast de l'ENS i l'ISO 27001) és aprovat formalment pel CEO de NCE i té caràcter imperatiu sobre l'organització de NCE. Estarà subjecte a un procés de revisió regular que l'adapti a noves circumstàncies, tècniques o organitzatives i que eviti que quedi obsolet. Es revisarà, com a mínim, de manera anual per assegurar-ne la contínua oportunitat, idoneïtat, completitud i precisió d'allò que estableixi la Política i que sigui sotmès a aprovació formal per l'Alta Direcció.

Així mateix, NCE disposa de documentació interna que defineix les línies mestres que regeixen el govern del cos normatiu.