

	Política de Seguretat de la Informació	09-09-2026 Pàg. 1 de 24
Classificació: Pública	SGSI 01	Versió 1.2

Control de versions

Versió	Motiu	Realitzat per	Data
0.9	Versió preliminar.	Consultor extern	29-10-2025
1.0	Versió Inicial	Responsable de Seguretat	13-11-2025
1.1	Ajustos i correccions	Responsable de Seguretat	04-05-2026
1.2	Reindexació taula índex	Responsable de Seguretat	09-09-2026

Aprovat per: Direcció el 17-07-2026

	Política de Seguretat de la Informació	09-09-2026 Pàg. 2 de 24
Classificació: Pública	SGSI 01	Versió 1.2

Contingut

Introducció	3
Definicions	3
Propòsit	4
Abast.....	4
Objectius o Missió de l'Organització	5
Fonaments d'aquesta Política	5
Requisits de Seguretat	7
Organització i implantació del procés de seguretat	7
Anàlisi i gestió dels riscos. Inclusió dels riscos amb Dades Personals.....	7
Requisits Legals i marc normatiu	13
Rols, Responsabilitats i Deures.....	14
Usuaris	14
Responsable de la Informació (Esquema Nacional de Seguretat)	15
Responsable del Servei (Esquema Nacional de Seguretat)	15
Direcció.....	15
Responsable de Seguretat	16
Delegat de Protecció de Dades	18
Responsable del Sistema	19
Persona Administradora de la Seguretat del Sistema	19
Comitè de Seguretat de la Informació	20
Procediment de designació i resolució de conflictes	21
Dades de Caràcter Personal	22
Terceres parts	22
Terceres parts com a serveis externalitzats de Seguretat.....	23
Desenvolupament de l'SGSI, Revisió i Auditories	23

	Política de Seguretat de la Informació	09-09-2026 Pàg. 3 de 24
Classificació: Pública	SGSI 01	Versió 1.2

Introducció

Aquest document exposa la Política de Seguretat de la Informació de Layers of Reality com el conjunt de principis bàsics i línies d'actuació amb què l'organització es compromet, en el marc de l'Esquema Nacional de Seguretat (ENS).

La informació és un actiu crític, essencial i de gran valor per al desenvolupament de l'activitat de Layers Of Reality. Aquest actiu ha d'estar protegit adequadament, mitjançant les mesures de seguretat necessàries, davant de les amenaces que el puguin afectar, independentment dels formats, suports, mitjans de transmissió, sistemes o persones que intervinguin en el seu coneixement, processament o tractament.

La Seguretat de la Informació és la protecció d'aquest actiu, amb la finalitat d'assegurar la qualitat de la informació i la continuïtat del negoci, minimitzar el risc i permetre maximitzar el retorn de les inversions i les oportunitats de negoci.

La seguretat de la informació és un procés que requereix mitjans tècnics i humans i una gestió i definició adequades dels procediments, i en el qual és fonamental la màxima col·laboració i implicació de tot el personal de Layers Of Reality.

La direcció de Layers Of Reality, conscient del valor de la informació, està profundament compromesa amb la política descrita en aquest document.

Definicions

- **Sistema d'Informació:** conjunt organitzat de recursos perquè la informació es pugui recollir, emmagatzemar, processar o tractar, mantenir, utilitzar, compartir, distribuir, posar a disposició, presentar o transmetre.
- **Risc:** estimació del grau d'exposició al fet que una amenaça es materialitzi sobre un o més actius i causi danys o perjudicis a l'organització.
- **Gestió de riscos:** activitats coordinades per dirigir i controlar una organització pel que fa als riscos.
- **Sistema de Gestió de Seguretat de la Informació (SGSI):** sistema de gestió que, basat en l'estudi dels riscos, s'estableix per crear, implementar, fer funcionar, supervisar, revisar, mantenir i millorar la seguretat de la informació. El sistema de gestió inclou l'estructura organitzativa, les polítiques, les activitats de planificació, les responsabilitats, les pràctiques, els procediments, els processos i els recursos.

	Política de Seguretat de la Informació	09-09-2026 Pàg. 4 de 24
Classificació: Pública	SGSI 01	Versió 1.2

- **Disponibilitat:** propietat o característica dels actius consistent en el fet que les entitats o els processos autoritzats hi tenen accés quan ho requereixen. Cal garantir que els recursos del sistema estaran disponibles quan es necessitin, especialment la informació crítica.
- **Integritat:** propietat o característica consistent en el fet que l'actiu d'informació no ha estat alterat de manera no autoritzada. La informació del sistema ha d'estar disponible tal com la va emmagatzemar un agent autoritzat.
- **Confidencialitat:** propietat o característica consistent en el fet que la informació ni es posa a disposició ni es revela a individus, entitats o processos no autoritzats. La informació només ha d'estar disponible per a agents autoritzats, especialment el seu propietari.
- **Autenticitat:** propietat o característica consistent en el fet que una entitat és qui diu ser o bé que garanteix la font de la qual procedeixen les dades. S'ha d'assegurar la identitat o l'origen de la informació.
- **Traçabilitat:** propietat o característica consistent en el fet que les actuacions d'una entitat (persona o procés) es poden traçar de manera indiscutible fins a aquesta entitat. S'ha d'assegurar, per a determinades dades, qui va fer què i en quin moment.

Propòsit

El propòsit d'aquesta Política de Seguretat de la Informació és protegir els actius d'informació de Layers Of Reality, assegurant per a això la disponibilitat, la integritat, la confidencialitat, l'autenticitat i la traçabilitat de la informació i de les instal·lacions, sistemes i recursos que la processen, gestionen, transmeten i emmagatzemen, sempre d'acord amb els requeriments del negoci i la legislació vigent.

Abast

Aquesta Política de Seguretat de la Informació és aplicable a totes les persones, sistemes i mitjans que accedeixin, tractin, emmagatzemin, transmetin o utilitzin la informació coneguda, gestionada o propietat de Layers Of Reality per als serveis de: a) conceptualització i disseny d'experiències immersives; b) instal·lació de sistemes audiovisuals, interactius i immersius i integració de programari; i c) control integral de l'experiència, posada en marxa i seguiment de la producció i explotació.

El personal subjecte a aquesta política inclou totes les persones amb accés a la informació descrita, independentment del suport, automatitzat o no, en què es trobi i de si la persona usuària és empleada o no de Layers Of Reality.

	Política de Seguretat de la Informació	09-09-2026 Pàg. 5 de 24
Classificació: Pública	SGSI 01	Versió 1.2

Per tant, també s'aplica a qualsevol altra tercera part que tingui accés a la informació o als sistemes de Layers Of Reality.

Per garantir que el procés de seguretat implantat s'actualitzarà i millorarà de manera contínua, s'implanta i es documenta un Sistema de Gestió de la Seguretat de la Informació. D'aquesta manera, el contingut d'aquesta Política de Seguretat de la Informació es desenvolupa en normes i procediments complementaris de seguretat.

Objectius o Missió de l'Organització

Layers of Reality és un estudi de creació de continguts per a realitat augmentada que genera experiències memorables, significatives i transformadores per al nombre més gran possible de persones, independentment dels seus coneixements tecnològics, l'edat o l'origen social. La nostra missió és crear experiències immersives, memorables i transformadores mitjançant tecnologia de realitat augmentada i tecnologies interactives d'avantguarda. Creiem a trencar barreres i fer que el món digital sigui accessible per a tothom, independentment de l'edat, l'origen o el nivell de coneixement tecnològic. El nostre objectiu és desenvolupar continguts atractius i significatius que connectin les persones amb experiències úniques i multisensorials que enriqueixin la seva comprensió i apreciació del món que les envolta.

Ja sigui a través de l'art, la cultura o la innovació, estem compromesos a explorar noves dimensions de la narrativa, expandir els límits de la realitat i oferir a cada individu l'oportunitat de connectar amb el futur d'una manera inclusiva i impactant.

Fonaments d'aquesta Política

L'objectiu últim de la seguretat de la informació és garantir que una organització pugui complir els seus objectius, desenvolupar les seves funcions i exercir les seves competències utilitzant sistemes d'informació. Per això, en matèria de seguretat de la informació s'han de tenir en compte els principis bàsics següents:

Seguretat com a procés integral.

La seguretat s'ha d'entendre com un procés integrat per tots els elements tècnics, humans, materials i organitzatius relacionats amb el sistema.

Es promourà la conscienciació de les persones que intervenen en el procés i dels seus responsables jeràrquics, perquè ni la ignorància, ni la manca d'organització i coordinació, ni les instruccions inadequades siguin font de risc per a la seguretat.

Gestió de la seguretat basada en els riscos.

	Política de Seguretat de la Informació	09-09-2026 Pàg. 6 de 24
Classificació: Pública	SGSI 01	Versió 1.2

L'anàlisi dels riscos és part essencial i contínua del procés de seguretat. La gestió d'aquests riscos permetrà mantenir un entorn controlat, amb aquests riscos a nivells acceptables, i es durà a terme mitjançant l'aplicació de mesures de seguretat de manera proporcionada a la naturalesa de la informació tractada i dels serveis que s'han de prestar.

Prevenició, detecció, resposta i conservació.

La seguretat del sistema preveu mesures que implementin els aspectes de prevenició, detecció i resposta davant d'incidents de seguretat, i de conservació de la informació i els serveis en cas que es produeixi l'incident.

Existència de línies de defensa.

Layers Of Reality implementa una estratègia de protecció basada en múltiples capes, constituïdes per mesures organitzatives, físiques i lògiques, de manera que, quan una de les capes falli, el sistema implementat permeti:

- Guanyar temps per a una reacció adequada davant dels incidents que no s'han pogut evitar.
- Reduir la probabilitat que el sistema quedi compromès en el seu conjunt.
- Minimitzar-ne l'impacte final.

Les línies de defensa han d'estar constituïdes per mesures de naturalesa organitzativa, física i lògica.

Vigilància contínua i reavaluació periòdica.

La vigilància contínua permetrà detectar activitats o comportaments anòmals i donar-hi una resposta oportuna.

Layers Of Reality implementa controls i avaluacions regulars de la seguretat (incloent-hi avaluacions dels canvis de configuració de manera rutinària) per conèixer en tot moment l'estat de la seguretat dels sistemes en relació amb les especificacions dels fabricants i amb les vulnerabilitats i les actualitzacions que els afectin, i reacciona amb diligència per gestionar el risc a la vista del seu estat de seguretat. Abans de l'entrada de nous elements, ja siguin físics o lògics, caldrà una autorització formal.

Així mateix, sol·licitarà la revisió periòdica per part de tercers amb la finalitat d'obtenir una avaluació independent.

Les mesures de seguretat s'avaluaran i s'actualitzaran periòdicament, adequant-ne l'eficàcia a l'evolució dels riscos i dels sistemes de protecció, i es podrà arribar a un replantejament de la seguretat, si calgués.

Diferenciació de responsabilitats.

Layers Of Reality ha organitzat la seva seguretat compromentent tots els

	Política de Seguretat de la Informació	09-09-2026 Pàg. 7 de 24
Classificació: Pública	SGSI 01	Versió 1.2

membres de la corporació mitjançant la designació de diferents rols de seguretat amb responsabilitats clarament diferenciades, tal com es recull més endavant en aquest document.

En els sistemes d'informació es diferenciarà:

- La persona o les persones responsables de la informació, que determinen els requisits de seguretat de la informació tractada;
- La persona o les persones responsables del servei, que determinen els requisits de seguretat dels serveis prestats;
- La persona responsable del sistema, que té la responsabilitat sobre la prestació dels serveis; i
- La persona responsable de seguretat, que determina les decisions per satisfer els requisits de seguretat.

En els supòsits de tractament de dades personals, a més, s'identificarà, segons escaigui, la persona o les persones DPD (delegada de protecció de dades), la persona o les persones responsables del tractament i la persona o les persones encarregades del tractament.

Requisits de Seguretat

Aquesta política de seguretat es desenvoluparà aplicant els requisits següents:

Organització i implantació del procés de seguretat

La seguretat de la informació compromet tots els membres de l'organització. Layers Of Reality identifica els responsables i n'estableix les responsabilitats a aquest efecte en els apartats "Rols, responsabilitats i deures" i "Terceres parts" d'aquest document. Aquesta Política de seguretat i la normativa seran conegudes per totes les persones compreses en l'àmbit d'aplicació d'aquest document.

Anàlisi i gestió dels riscos. Inclusió dels riscos amb Dades Personals

Conèixer els riscos i elaborar una estratègia per gestionar-los adequadament és primordial per a Layers Of Reality, ja que únicament si es coneix l'estat de seguretat es podran prendre les decisions adequades per mitigar els riscos a què s'enfronta.

Quan un sistema d'informació tracti dades personals, li serà aplicable el que disposen l'RGPD i la LOPDGDD o, si escau, la Llei orgànica 7/2021, de 26 de maig, de protecció de dades personals tractades per a fins de prevenció, detecció, investigació i enjudiciament d'infraccions penals i d'execució de

	Política de Seguretat de la Informació	09-09-2026 Pàg. 8 de 24
Classificació: Pública	SGSI 01	Versió 1.2

sancions penals. El responsable o l'encarregat del tractament, assessorat pel delegat de protecció de dades, durà a terme una anàlisi de riscos d'acord amb l'article 24 del Reglament general de protecció de dades i, en els supòsits del seu article 35, una avaluació d'impacte en la protecció de dades. Del resultat d'aquesta anàlisi se'n poden derivar mesures addicionals que calgui implantar.

Layers Of Reality utilitza la metodologia **Magerit** per analitzar els riscos, i fa una anàlisi detallada dels riscos que afectin els actius recollits en un inventari d'actius, que queda documentada en un document d'Anàlisi de Riscos.

L'entitat determina els nivells de risc a partir dels quals pren accions de tractament sobre aquests riscos. Un Risc es considera acceptable quan s'estima que implementar més controls de seguretat consumiria més recursos que el possible impacte associat.

La persona Responsable de Seguretat serà l'encarregada que es dugui a terme l'anàlisi de riscos, així com d'identificar mancances i febleses i posar-les en coneixement del Comitè de Seguretat de la Informació.

Aquesta anàlisi es repetirà:

- Regularment, com a mínim un cop l'any.
- Quan canviïn de manera significativa la informació gestionada i/o els serveis prestats.
- Quan es produeixi un incident greu de seguretat o es detectin vulnerabilitats greus.

Un cop dut a terme el procés d'avaluació de riscos, la direcció de Layers Of Reality és la responsable d'aprovar els riscos residuals i els plans de tractament del risc.

En el cas de les mesures implantades en l'ENS, si l'anàlisi de riscos estableix mesures més importants, aquestes s'afegiran a les descrites en l'ENS.

Gestió de Personal.

Tot el personal de Layers Of Reality relacionat amb la informació i els sistemes és format i informat dels seus deures i obligacions en matèria de seguretat, essencialment mitjançant la normativa d'ús dels actius. Les seves actuacions són supervisades segons els rols establerts per verificar que se segueixen els procediments definits.

Els accessos dels usuaris i usuàries són únics i se'n verifiquen periòdicament els drets i les activitats que tenen a veure amb la Seguretat de la informació per corregir o exigir responsabilitats, si escau.

	Política de Seguretat de la Informació	09-09-2026 Pàg. 9 de 24
Classificació: Pública	SGSI 01	Versió 1.2

Professionalitat, Conscienciació i Formació.

La seguretat dels sistemes és gestionada i revisada per personal qualificat de Layers Of Reality i per personal extern especialitzat, que rep i actualitza la formació necessària per garantir la seguretat de la informació en tot el cicle de vida dels sistemes d'informació: planificació, disseny, adquisició, construcció, desplegament, explotació, manteniment, gestió d'incidències i desmantellament. Els requisits de qualificació (formació i experiència) els establirà sempre Layers Of Reality.

Aquesta Política de Seguretat de la Informació ha de ser coneguda per totes les persones usuàries internes i externes i per les empreses que accedeixin, gestionin o tractin dades de Layers Of Reality.

El conjunt de Polítiques, normes i procediments complementaris a aquesta Política de Seguretat de la Informació també s'han de comunicar adequadament i posar en coneixement de les persones, empreses i institucions afectades o implicades en cada cas.

Es definiran periòdicament programes de comunicació, conscienciació i formació i es posarà a disposició de les persones usuàries la normativa d'ús dels actius d'informació.

Layers Of Reality promourà la Formació tècnica en Seguretat de la Informació necessària, especialment per a les persones Responsables de Seguretat i de Sistemes.

Autorització i control dels accessos.

L'accés als sistemes d'informació és controlat, monitorat i limitat a les persones usuàries, processos, dispositius i sistemes d'informació amb les funcionalitats mínimes permeses i/o autoritzades.

S'establiran i es gestionaran les autoritzacions necessàries per a les tasques crítiques.

Protecció de les instal·lacions.

Els sistemes de Layers Of Reality i la seva infraestructura de comunicacions estan situats en àrees degudament protegides, dotades de mesures de seguretat físiques, de redundància, continuïtat i ambientals, i amb un procediment de control d'accés físic.

Adquisició de productes de seguretat i contractació de serveis de seguretat

Per a l'adquisició de productes, Layers Of Reality tindrà en compte que aquests productes tinguin certificada la funcionalitat de seguretat relacionada amb l'objecte de la seva adquisició, excepte en els casos en què les exigències

	Política de Seguretat de la Informació	09-09-2026 Pàg. 10 de 24
Classificació: Pública	SGSI 01	Versió 1.2

de proporcionalitat quant als riscos assumits no ho justifiquin, a criteri de la persona Responsable de Seguretat.

Per a la contractació de serveis de seguretat, cal atènyer-se al que s'assenyala en els apartats anteriors i al que disposa l'apartat "Terceres parts" més endavant en aquest document.

Mínim Privilegi i Seguretat des del Disseny.

A Layers Of Reality els sistemes es dissenyen i es configuren sempre pensant en la Seguretat per Defecte. El sistema proporciona la funcionalitat mínima requerida perquè les funcions d'operació, administració i registre d'activitat són les mínimes necessàries, i Layers Of Reality s'assegura que només hi poden accedir les persones autoritzades i des d'emplaçaments o equips autoritzats.

S'eliminaran o desactivaran, mitjançant el control de la configuració, les funcions que siguin innecessàries o inadequades per a la finalitat que es persegueix. L'ús ordinari del sistema ha de ser senzill i segur, de manera que una utilització insegura requereixi un acte conscient per part de la persona usuària. Per a això, s'aplicaran guies de configuració de seguretat per a les diferents tecnologies, adaptades a la categorització del sistema, a l'efecte d'eliminar o desactivar les funcions que siguin innecessàries o inadequades.

Tots els projectes relacionats amb els sistemes d'informació o que els afectin hauran d'incloure, en el seu procés d'anàlisi, una avaluació dels requisits de seguretat i definir un model de seguretat consensuat amb el responsable de seguretat de la informació.

En el disseny, desenvolupament, instal·lació i gestió dels sistemes d'informació i en els projectes es tindran en compte i s'aplicaran els conceptes de seguretat des del disseny, codificació segura i els controls i mesures de seguretat que escaiguin segons el document d'aplicabilitat aprovat per Layers Of Reality.

Integritat i actualització del sistema.

A Layers Of Reality els sistemes s'avaluen periòdicament per conèixer en tot moment el seu estat de seguretat, tenint en consideració les especificacions dels fabricants, les vulnerabilitats, les deficiències de configuració, les actualitzacions que escaiguin i la detecció primerenca d'incidents, i gestionant d'aquesta manera la seva integritat.

Tots els elements dels sistemes requereixen autorització prèvia a la seva instal·lació.

	Política de Seguretat de la Informació	09-09-2026 Pàg. 11 de 24
Classificació: Pública	SGSI 01	Versió 1.2

Protecció de la informació emmagatzemada i en trànsit.

La informació es classifica d'acord amb la sensibilitat requerida en el seu tractament i segons els nivells de seguretat i protecció exigibles.

Layers Of Reality presta una atenció especial a la informació emmagatzemada o en trànsit a través d'entorns insegurs. Això inclou la informació emmagatzemada o tractada en equips portàtils, tauletes, telèfons intel·ligents, dispositius perifèrics i suports d'informació, així com les comunicacions sobre xarxes obertes o amb xifratge feble, on s'apliquen les mesures de seguretat que garanteixin que la informació es tracta d'acord amb la seva classificació.

S'aplicaran procediments que garanteixin la recuperació i la conservació a llarg termini dels documents electrònics produïts pels sistemes d'informació.

Tota informació en suport no electrònic que hagi estat causa o conseqüència directa de la informació electrònica haurà d'estar protegida amb el mateix grau de seguretat que aquesta. Per a això, s'aplicaran les mesures que corresponguin a la naturalesa del suport, de conformitat amb les normes que siguin aplicables.

Prevenició davant d'altres sistemes d'informació interconnectats.

Layers Of Reality protegeix el perímetre d'accés al seu sistema, en particular en les connexions a través d'Internet, analitzant sempre els riscos derivats de la interconnexió amb altres sistemes i establint les mesures que garanteixin el nivell de seguretat necessari.

Registre d'activitat i detecció de codi nociu

Layers Of Reality ha habilitat registres de l'activitat de les persones usuàries que retenen la informació necessària per monitorar, analitzar, investigar i documentar activitats indegudes o no autoritzades, i que permeten identificar en cada moment la persona que actua. Tot això amb plenes garanties del dret a l'honor, a la intimitat personal i familiar i a la pròpia imatge de les persones afectades, i d'acord amb la normativa sobre protecció de dades personals i la resta de disposicions que siguin aplicables.

Layers Of Reality implementa un procés integral de detecció, reacció i recuperació davant de codi nociu mitjançant el desenvolupament de procediments que cobreixen els mecanismes de detecció, els criteris de classificació, els procediments d'anàlisi i resolució, així com els canals de comunicació a les parts interessades i el registre de les actuacions.

Amb l'objectiu de preservar la seguretat dels sistemes d'informació, garantint la rigorosa observança dels principis d'actuació de les administracions públiques, i de conformitat amb el que disposa el Reglament general de protecció de dades i el respecte als principis de limitació de la finalitat,

	Política de Seguretat de la Informació	09-09-2026 Pàg. 12 de 24
Classificació: Pública	SGSI 01	Versió 1.2

minimització de les dades i limitació del termini de conservació que s'hi enuncien, es podran analitzar, en la mesura estrictament necessària i proporcionada, les comunicacions entrants o sortints, i únicament per a finalitats de seguretat de la informació, de manera que sigui possible impedir l'accés no autoritzat a les xarxes i sistemes d'informació, aturar els atacs de denegació de servei, evitar la distribució malintencionada de codi nociu i altres danys a les xarxes i sistemes d'informació esmentats.

Per corregir o, si escau, exigir responsabilitats, cada persona usuària que accedeixi al sistema d'informació haurà d'estar identificada de manera única, de manera que se sàpiga, en tot moment, qui rep drets d'accés, de quin tipus són i qui ha dut a terme una activitat determinada.

Incidents de seguretat.

Perquè la informació i/o els serveis no es vegin perjudicats per incidents de seguretat, Layers Of Reality implementa les mesures de seguretat establertes, així com qualsevol altre control addicional que hagi identificat com a necessari, a través d'una avaluació d'amenaques i riscos. Aquests controls, així com els rols i les responsabilitats de seguretat de tot el personal, estan clarament definits i documentats.

Quan es produeix una desviació significativa dels paràmetres que s'hagin preestablert com a normals, s'establiran els mecanismes de detecció, anàlisi i comunicació necessaris perquè arribin regularment a les persones responsables.

Layers Of Reality establirà les mesures de reacció següents davant d'incidents de seguretat:

- Mecanismes per respondre eficaçment als incidents de seguretat.
- Designar un punt de contacte per a les comunicacions relatives a incidents detectats en altres departaments o en altres organismes.
- Establir protocols per a l'intercanvi d'informació relacionada amb l'incident. Això inclou comunicacions, en tots dos sentits, amb els Equips de Resposta a Emergències.
- Per garantir la disponibilitat dels serveis, Layers Of Reality disposa dels mitjans i les tècniques necessaris que permeten garantir la recuperació dels serveis més crítics.

Les persones usuàries disposen de canals establerts per informar immediatament de qualsevol incident o anomalia detectada.

	Política de Seguretat de la Informació	09-09-2026 Pàg. 13 de 24
Classificació: Pública	SGSI 01	Versió 1.2

Continuïtat de l'activitat.

Layers Of Reality fa les còpies de seguretat que garanteixen la recuperació de la informació i estableix els mecanismes adequats per garantir la continuïtat de les operacions en cas de pèrdua dels mitjans habituals.

En aquest sentit, s'han desenvolupat procediments que assegurin la recuperació i la conservació a llarg termini dels documents i les dades electròniques produïts en l'àmbit de les seves competències.

Millora contínua del procés de seguretat.

El sistema de gestió de seguretat implantat s'actualitza i es millora de manera contínua, segons estableixen les certificacions, tal com es descriu més endavant en aquest document.

Requisits Legals i marc normatiu

- 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 (RGPD).
- Llei orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals (LOPDGDD).
- Reial decret legislatiu 1/1996, de 12 d'abril, Llei de propietat intel·lectual.
- Llei 2/2019, d'1 de març, per la qual es modifica el text refós de la Llei de propietat intel·lectual, aprovat pel Reial decret legislatiu 1/1996, de 12 d'abril, i per la qual s'incorporen a l'ordenament jurídic espanyol la Directiva 2014/26/UE del Parlament Europeu i del Consell, de 26 de febrer de 2014, i la Directiva (UE) 2017/1564 del Parlament Europeu i del Consell, de 13 de setembre de 2017.
- Llei 34/2002, d'11 de juliol, de serveis de la societat de la informació i de comerç electrònic.
- Reial decret llei 12/2018, de 7 de setembre, de seguretat de les xarxes i sistemes d'informació.
- Reial decret 43/2021, de 26 de gener, pel qual es desplega el Reial decret llei 12/2018, de 7 de setembre, de seguretat de les xarxes i sistemes d'informació.
- Reial decret 311/2022, de 3 de maig, pel qual es regula l'Esquema Nacional de 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.

	Política de Seguretat de la Informació	09-09-2026 Pàg. 14 de 24
Classificació: Pública	SGSI 01	Versió 1.2

- 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 d'informe de l'estat de la 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 d'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.
- UNE-ISO/IEC 27001:2023 Seguretat de la informació, ciberseguretat i protecció de la privadesa. SGSI. Requisits.
- UNE-ISO/IEC 27002:2023 Seguretat de la informació, ciberseguretat i protecció de la privadesa. Controls de seguretat de la informació.

Així mateix, la persona Responsable de Seguretat serà responsable d'identificar les guies de seguretat del Centre Criptològic Nacional (CCN) que s'aplicaran per millorar el compliment del que estableix l'Esquema Nacional de Seguretat.

Rols, Responsabilitats i Deures

Usuaris

Tota persona o sistema que accedeixi a la informació tractada, gestionada o propietat de Layers Of Reality es considerarà una persona usuària. Les persones usuàries són responsables de la seva conducta quan accedeixen a la informació o utilitzen els sistemes informàtics de Layers Of Reality. Les persones usuàries són responsables de totes les accions dutes a terme utilitzant els seus identificadors o credencials personals.

Les persones usuàries tenen l'obligació de:

- Complir la Política de Seguretat de la Informació i les normes, procediments i instruccions complementàries.
- Protegir i custodiar la informació de Layers Of Reality, evitant-ne la revelació, l'emissió a l'exterior, la modificació, l'esborrament o la destrucció accidentals o no autoritzats o el mal ús, independentment del suport o els mitjans pels quals s'hi hagi accedit o s'hagi conegut.
- Conèixer i aplicar la Política de Seguretat de la Informació, les Normes d'Ús dels Sistemes d'Informació i la resta de polítiques, normes, procediments i mesures de seguretat aplicables.

	Política de Seguretat de la Informació	09-09-2026 Pàg. 15 de 24
Classificació: Pública	SGSI 01	Versió 1.2

Les persones usuàries que incompleixin la Política de Seguretat de la Informació o les normes i els procediments complementaris podran ser sancionades d'acord amb el que estableixen els contractes que emparin la seva relació amb Layers Of Reality i amb la legislació vigent i aplicable.

Responsable de la Informació (Esquema Nacional de Seguretat)

La persona Responsable de la Informació és qui determina els requisits de la informació tractada, i té les responsabilitats següents:

- Vetllar pel bon ús de la informació i, per tant, per la seva protecció.
- Establir els requisits de la informació en matèria de seguretat.
- Determinar els nivells de seguretat de la informació tractada, valorant les conseqüències d'un impacte negatiu.

Responsable del Servei (Esquema Nacional de Seguretat)

La persona responsable del servei tindrà les responsabilitats generals següents:

- Establir els requisits del servei en matèria de seguretat, incloent-hi els requisits d'interoperabilitat, accessibilitat i disponibilitat.
- Determinar els nivells de seguretat del servei, d'acord amb el Responsable de Seguretat i el Responsable del Sistema.
- Mantenir la seguretat de la informació gestionada i dels serveis prestats pels sistemes d'informació en el seu àmbit de responsabilitat.

Direcció

La direcció de Layers Of Reality està profundament compromesa amb la política descrita en aquest document i és conscient del valor de la informació i del greu impacte econòmic i d'imatge que pot produir un incident de seguretat.

En el context de l'Esquema Nacional de Seguretat, la Direcció assumeix les responsabilitats descrites per a les persones Responsables de la Informació i del Servei.

La Direcció és, per tant, propietària dels actius d'informació propis de Layers Of Reality, i també és responsable dels riscos.

La direcció assumeix a més les responsabilitats següents:

- Demostrar lideratge i compromís pel que fa al sistema de gestió de seguretat de la informació
- Assegurar que s'estableixen la política i els objectius de seguretat de la informació i que aquests són compatibles amb la direcció estratègica de l'organització.

	Política de Seguretat de la Informació	09-09-2026 Pàg. 16 de 24
Classificació: Pública	SGSI 01	Versió 1.2

- Aprovar i comunicar la Política de Seguretat de la Informació, les Normes d'Ús dels Sistemes d'Informació i la importància del seu compliment a tots els usuaris, interns o externs, als clients i als proveïdors.
- Reunir-se i acordar amb el Comitè de Seguretat Corporatiu i amb les persones Responsables de Seguretat i de Sistemes, per ser informada sobre l'SGSI i actualitzar l'estratègia en matèria de Seguretat de la Informació.
- Fomentar una cultura corporativa de seguretat de la informació.
- Donar suport a la millora contínua dels processos de seguretat de la informació.
- Assegurar que estiguin disponibles els recursos necessaris per al compliment de la política de seguretat de la informació i de les normes d'ús dels sistemes, i per al funcionament del sistema de gestió de seguretat de la informació.
- Definir l'enfocament per a l'anàlisi i la gestió dels riscos de seguretat de la informació i els criteris per assumir els riscos, i assegurar-ne l'avaluació com a mínim amb una periodicitat anual.
- Assegurar que es duen a terme auditories internes de seguretat de la informació i que se'n revisen els resultats per identificar oportunitats de millora.
- Definir i controlar el pressupost per a seguretat de la informació.
- Aprovar els plans de formació i les millores i els projectes relacionats amb la Seguretat de la Informació.
- Aprovar la documentació fins al segon nivell de normes i procediments.
- Determinar les mesures, siguin disciplinàries o de qualsevol altre tipus, que es poguessin aplicar a les persones responsables de violacions de seguretat.

Responsable de Seguretat

La persona Responsable de la Seguretat determina les decisions per satisfer els requisits de seguretat de la informació i dels serveis i supervisa la implantació de les mesures necessàries per garantir que se satisfan els requisits, i n'informarà

La persona amb el càrrec de Responsable de Seguretat de la Informació assumirà les funcions següents:

- Promoure la seguretat de la informació gestionada i dels serveis electrònics prestats pels sistemes d'informació, amb la responsabilitat i l'autoritat per assegurar-se que el Sistema de Gestió de la Seguretat de la Informació compleix els requisits de l'Esquema Nacional de Seguretat.

	Política de Seguretat de la Informació	09-09-2026 Pàg. 17 de 24
Classificació: Pública	SGSI 01	Versió 1.2

- Supervisar el compliment d'aquesta Política, de les seves normes, dels procediments derivats i de la configuració de seguretat dels sistemes.
- Establir les mesures de seguretat adequades i eficaces per complir els requisits de seguretat establerts per les persones Responsables del Servei i de la Informació, seguint en tot moment el que exigeix l'Annex II de l'ENS, i declarar l'aplicabilitat d'aquestes mesures.
- Promoure les activitats de conscienciació i formació en matèria de seguretat en el seu àmbit de responsabilitat.
- Coordinar i fer el seguiment de la implantació dels projectes d'adequació a les normes especificades en col·laboració amb la persona Responsable de Sistemes.
- Dur a terme, amb la col·laboració de la persona Responsable del Sistema, les preceptives anàlisis de riscos, seleccionant les salvaguardes que cal implantar i revisant el procés de gestió del risc. Així mateix, juntament amb la Direcció, acceptar els riscos residuals calculats en aquesta anàlisi.
- Promoure auditories periòdiques per verificar el compliment de les obligacions en matèria de seguretat de la informació i analitzar els informes d'auditoria, elaborant les conclusions que s'han de presentar a la persona Responsable del Sistema perquè adopti les mesures correctores adequades.
- Coordinar el procés de Gestió de la Seguretat, en col·laboració amb la persona Responsable de Sistemes.
- Signar la Declaració d'Aplicabilitat, que comprèn la relació de mesures de seguretat seleccionades per a un sistema.
- Elaborar informes periòdics de seguretat que incloguin els incidents més rellevants de cada període, en coordinació amb la persona Responsable de Sistemes.
- Determinar la categoria del sistema segons el procediment descrit a l'Annex I de l'ENS i les mesures de seguretat que s'han d'aplicar d'acord amb el que preveu l'Annex II de l'ENS.
- Verificar que les mesures de seguretat són adequades per a la protecció de la informació i els serveis.
- Preparar els temes que s'han de tractar en les reunions del Comitè de Seguretat, en coordinació amb la persona Responsable del Sistema, aportant informació puntual per a la presa de decisions.
- Responsable de l'execució directa o delegada de les decisions de la Direcció, es reunirà amb aquesta i amb la persona Responsable del Sistema per assegurar l'estratègia.

	Política de Seguretat de la Informació	09-09-2026 Pàg. 18 de 24
Classificació: Pública	SGSI 01	Versió 1.2

Pel que fa a la documentació, i amb el suport de la persona Responsable del Sistema, són funcions de la persona Responsable de Seguretat:

- Proposar a la Direcció, al Comitè de Seguretat i a la persona Responsable de Sistemes, per a la seva aprovació, la documentació de seguretat de segon nivell (Normes de Seguretat TIC –STIC– i Procediments Generals del Sistema de Gestió de la Seguretat de la Informació –SGSI–) i signar aquesta documentació.
- Aprovar la documentació de seguretat de tercer nivell (Procediments Operatius STIC i Instruccions Tècniques STIC).
- Mantenir la documentació organitzada i actualitzada, gestionant-ne els mecanismes d'accés.

Per al desenvolupament de qualsevol de les seves funcions, la persona Responsable de Seguretat podrà demanar la col·laboració de la persona Responsable del Sistema.

Delegat de Protecció de Dades

D'acord amb el que indiquen l'RGPD i la LOPDGDD, la persona Delegada de Protecció de Dades tindrà com a mínim les funcions següents:

- Informar i assessorar les persones responsables del tractament i, en general, el personal de l'organització, de les obligacions que els incumbeixen en relació amb l'RGPD i altres disposicions de protecció de dades.
- Supervisar el compliment del que disposa aquest Reglament, d'altres disposicions de protecció de dades de la Unió Europea o dels estats membres i de les polítiques del responsable o de l'encarregat del tractament en matèria de protecció de dades personals, inclosa l'assignació de responsabilitats, la conscienciació i formació del personal que participa en les operacions de tractament, i les auditories corresponents;
- Oferir l'assessorament que se li sol·liciti sobre l'avaluació d'impacte relativa a la protecció de dades i supervisar-ne l'aplicació de conformitat amb l'article 35 de l'RGPD;
- Cooperar amb l'autoritat de control;
- Actuar com a punt de contacte de l'autoritat de control per a qüestions relatives al tractament, inclosa la consulta prèvia a què fa referència l'article 36 de l'RGPD, i fer consultes, si escau, sobre qualsevol altre assumpte.

	Política de Seguretat de la Informació	09-09-2026 Pàg. 19 de 24
Classificació: Pública	SGSI 01	Versió 1.2

Responsable del Sistema

La persona Responsable del Sistema, per si mateixa o a través de recursos propis o contractats, s'encarrega de desenvolupar la manera concreta d'implementar la seguretat en el sistema i de supervisar-ne l'operació diària, i pot delegar en persones administradores o operadors sota la seva responsabilitat.

Són funcions de la persona Responsable del Sistema les següents:

- Desenvolupar, operar i mantenir el sistema d'Informació durant tot el seu cicle de vida, les seves especificacions, la instal·lació i la verificació del seu funcionament correcte.
- Definir la topologia i el sistema de gestió del Sistema d'Informació, i establir-ne els criteris d'ús i els serveis disponibles.
- Assegurar-se que les mesures específiques de seguretat s'integren adequadament dins del marc general de seguretat.
- Dur a terme exercicis i proves sobre els procediments operatius de seguretat i els plans de continuïtat existents.
- Seguiment del cicle de vida dels sistemes: especificació, arquitectura, desenvolupament, operació, canvis.
- Implantar les mesures necessàries per garantir la seguretat del sistema durant tot el seu cicle de vida, d'acord amb la persona Responsable de Seguretat.
- Aprovar tota modificació substancial de la configuració de qualsevol element del sistema.
- Dur a terme, amb la col·laboració de la persona Responsable de Seguretat, les preceptives anàlisis de riscos, seleccionar les salvaguardes que cal implantar i revisar el procés de gestió del risc.
- Elaborar, en col·laboració amb la persona Responsable de Seguretat, la documentació de seguretat de tercer nivell (Procediments Operatius STIC i Instruccions Tècniques STIC).

Persona Administradora de la Seguretat del Sistema

Les funcions que exercirà són les següents:

- La implementació, gestió i manteniment de les mesures de seguretat aplicables al sistema d'informació.

	Política de Seguretat de la Informació	09-09-2026 Pàg. 20 de 24
Classificació: Pública	SGSI 01	Versió 1.2

- La gestió, configuració i actualització, si escau, del maquinari i el programari en què es basen els mecanismes i serveis de seguretat dels sistemes d'informació.
- La gestió de les autoritzacions concedides a les persones usuàries del sistema, en particular els privilegis concedits, incloent-hi la monitorització que l'activitat desenvolupada en el sistema s'ajusta al que s'ha autoritzat.
- L'aplicació dels procediments operatius de seguretat.
- Aplicar els canvis de configuració del sistema d'informació.
- Assegurar que els controls de seguretat establerts es compleixen estrictament, així com assegurar que s'apliquen els procediments aprovats per gestionar el sistema d'informació.
- Supervisar les instal·lacions de maquinari i programari, les seves modificacions i millores per assegurar que la seguretat no queda compromesa i que en tot moment s'ajusten a les autoritzacions pertinents.
- Monitorar l'estat de seguretat del sistema proporcionat per les eines de gestió d'esdeveniments de seguretat i els mecanismes d'auditoria tècnica implementats en el sistema.
- Informar les persones responsables de qualsevol anomalia, compromís o vulnerabilitat relacionada amb la seguretat.
- Col·laborar en la investigació i resolució d'incidents de seguretat, des de la seva detecció fins a la seva resolució.

Comitè de Seguretat de la Informació

Compost pel Director General Corporatiu, el Director General de Mitjans, el Director del Departament Legal, el Director de Tecnologies de la Informació i el Responsable de la Seguretat de la Informació, es reuneix periòdicament per coordinar la seguretat de la informació a escala de l'organització.

Les seves funcions són les següents:

- Atendre les sol·licituds, en matèria de Seguretat de la Informació, de l'Administració i dels diferents rols de seguretat i/o àrees, informant regularment de l'estat de la Seguretat de la Informació.
- Assessorar en matèria de Seguretat de la Informació.
- Resoldre els conflictes de responsabilitat que puguin sorgir entre les diferents unitats administratives.
- Promoure la millora contínua del sistema de gestió de la Seguretat de la Informació. Per a això s'encarregarà de:

	Política de Seguretat de la Informació	09-09-2026 Pàg. 21 de 24
Classificació: Pública	SGSI 01	Versió 1.2

- Coordinar els esforços de les diferents àrees en matèria de Seguretat de la Informació, per assegurar que siguin coherents i estiguin alineats amb l'estratègia decidida en la matèria, i evitar duplicitats.
- Proposar plans de millora de la Seguretat de la Informació, amb la dotació pressupostària corresponent, prioritzant les actuacions en matèria de seguretat quan els recursos siguin limitats.
- Vetllar perquè la Seguretat de la Informació es tingui en compte en tots els projectes des de la seva especificació inicial fins a la posada en funcionament. En particular, haurà de vetllar per la creació i la utilització de serveis horitzontals que redueixin duplicitats i donin suport a un funcionament homogeni de tots els sistemes TIC.
- Fer un seguiment dels principals riscos residuals assumits i recomanar possibles actuacions respecte d'aquests.
- Fer un seguiment de la gestió dels incidents de seguretat i recomanar possibles actuacions respecte d'aquests.
- Revisar regularment aquesta Política de Seguretat de la Informació perquè l'òrgan competent l'aprovi.
- Elaborar la normativa de Seguretat de la Informació per a la seva aprovació en coordinació amb la Direcció General.
- Verificar els procediments de seguretat de la informació i la resta de documentació per a la seva aprovació.
- Elaborar programes de formació destinats a formar i sensibilitzar el personal en matèria de Seguretat de la Informació i protecció de dades de caràcter personal.
- Elaborar i aprovar els requisits de formació i qualificació de les persones administradores, operadores i usuàries des del punt de vista de la Seguretat de la Informació.
- Promoure la realització de les auditories periòdiques de l'ENS i de protecció de dades que permetin verificar el compliment de les obligacions de l'organització en matèria de seguretat de la Informació.

Procediment de designació i resolució de conflictes

El Comitè de Seguretat de la Informació de Layers Of Reality **assigna, renova i comunica** les responsabilitats, autoritats i rols pel que fa a la seguretat de la informació, i determina en cada cas els motius i el termini de vigència. També s'assegurarà que les persones usuàries coneixen,

	Política de Seguretat de la Informació	09-09-2026 Pàg. 22 de 24
Classificació: Pública	SGSI 01	Versió 1.2

assumeixen i exerceixen les responsabilitats, autoritats i rols assignats, **i resoldrà els conflictes** que es generin en relació amb cada responsabilitat en Seguretat de la Informació.

La persona Responsable de la Seguretat serà diferent de la persona Responsable del Sistema, i no hi ha d'haver dependència jeràrquica entre totes dues.

Dades de Caràcter Personal

L'organització només recollirà dades de caràcter personal quan siguin adequades, pertinents i no excessives i estiguin relacionades amb l'àmbit i les finalitats per a les quals s'hagin obtingut. De la mateixa manera, adoptarà les mesures d'índole tècnica i organitzativa necessàries per complir la normativa de Protecció de Dades vigent en cada cas.

D'aquesta manera, amb la LOPDGDD s'han adoptat les mesures oportunes, com ara l'anàlisi de la legitimitat jurídica de cadascun dels tractaments de dades que es duuguin a terme, l'anàlisi de riscos, l'avaluació d'impacte si el risc és alt, el registre d'activitats i el nomenament de qui hagi d'exercir les funcions de persona Delegada de Protecció de Dades.

Terceres parts

Quan l'organització presti serveis a altres organismes, o gestioni informació d'altres organismes, se'ls farà partícips d'aquesta Política de Seguretat de la Informació. Layers Of Reality definirà i aprovarà els canals per a la coordinació de la informació i els procediments d'actuació per a la reacció davant d'incidents de seguretat, així com la resta d'actuacions que Layers Of Reality dugui a terme en matèria de Seguretat en relació amb altres organismes.

Quan Layers Of Reality utilitzi serveis de tercers o cedeixi informació a tercers, se'ls farà partícips d'aquesta Política de Seguretat i de la Normativa de Seguretat existent que afecta aquests serveis o aquesta informació. Aquesta tercera part quedarà subjecta a les obligacions establertes en la normativa esmentada, i podrà desenvolupar els seus propis procediments operatius per complir-la. S'establiran procediments específics de comunicació i resolució d'incidències. Es garantirà que el personal de tercers estigui adequadament conscienciat en matèria de seguretat, com a mínim al mateix nivell que l'establert en aquesta Política de Seguretat.

Quan algun aspecte d'aquesta Política de Seguretat no pugui ser satisfet per una tercera part segons es requereix en els paràgrafs anteriors, caldrà un informe de la persona Responsable de Seguretat que precisi els riscos en què s'incorre i la manera de tractar-los. Caldrà que les persones responsables de

	Política de Seguretat de la Informació	09-09-2026 Pàg. 23 de 24
Classificació: Pública	SGSI 01	Versió 1.2

la informació i dels serveis afectats aprovin aquest informe abans de seguir endavant.

Terceres parts com a serveis externalitzats de Seguretat

En el cas de serveis externalitzats, excepte per causa justificada i documentada, l'organització prestadora d'aquests serveis haurà de designar un POC (Punt o Persona de Contacte) per a la seguretat de la informació tractada i el servei prestat, que compti amb el suport dels òrgans de direcció i que canalitzi i supervisi tant el compliment dels requisits de seguretat del servei que presta o de la solució que proveeixi com les comunicacions relatives a la seguretat de la informació i la gestió dels incidents per a l'àmbit d'aquest servei.

Aquest POC de seguretat serà la persona Responsable de Seguretat de l'organització contractada, formarà part de la seva àrea o hi tindrà comunicació directa.

Desenvolupament de l'SGSI, Revisió i Auditories

El Comitè de Seguretat de la Informació ha aprovat el desenvolupament d'un sistema de gestió de seguretat de la informació (SGSI) que s'estableix, implementa, manté i millora d'acord amb els estàndards de seguretat. Aquest sistema s'adequarà i servirà de gestió dels controls de l'Esquema Nacional de Seguretat. El sistema estarà documentat i permetrà generar evidències dels controls i del compliment dels objectius fixats. Hi ha un procediment de gestió documental que estableix les directrius per a l'estructuració de la documentació de seguretat del sistema, la seva gestió i l'accés.

La Política i les Normes de Seguretat de la Informació s'adaptaran a l'evolució dels sistemes i de la tecnologia i als canvis organitzatius, i s'alinearán amb la legislació vigent i amb els estàndards i les millors pràctiques de l'Esquema Nacional de Seguretat, i es prestarà una atenció especial a les guies publicades pel Centre Criptològic Nacional com a desplegament de les mesures i els controls de seguretat.

Les mesures de seguretat i els controls físics, administratius i tècnics aplicables es detallaran en el Document d'Aplicabilitat, i seran proporcionals a la criticitat de la informació que cal protegir i a la seva classificació.

El Comitè de Seguretat de la Informació revisarà aquesta política anualment o quan hi hagi canvis significatius que ho aconsellin, i la tornarà a sotmetre a l'aprovació de la direcció. Les revisions comprovaran l'efectivitat de la política i valoraran els efectes dels canvis tecnològics i de negoci.

	Política de Seguretat de la Informació	09-09-2026 Pàg. 24 de 24
Classificació: Pública	SGSI 01	Versió 1.2

La direcció serà responsable d'aprovar les modificacions necessàries en el text quan es produeixi un canvi que afecti les situacions de risc establertes en aquest document.

El sistema de gestió de seguretat s'auditarà anualment, segons un pla d'auditories desenvolupat pel responsable de seguretat.