DECRET

Aprovar la Política de Seguretat de la Informació de l'Organisme de Gestió Tributària de la Diputació de Barcelona, assignar funcions a efectes de l'Esquema Nacional de Seguretat i crear el Comitè de Seguretat de la Informació de la Corporació (exp. ORGT/ 2025/0045270)

Antecedents de fets

1. La missió de l'Organisme de Gestió Tributària de la Diputació de Barcelona (ORGT) és l'exercici de les funcions i potestats de gestió, inspecció i recaptació de tributs i altres ingressos de dret públic per delegació o encàrrec de gestió de les administracions públiques de Catalunya i dels Ens públics que en depenen.

2. L'ORGT necessita dels sistemes de tecnologies de la informació i les comunicacions (TIC) per aconseguir els seus objectius. Aquests sistemes han de ser administrats amb diligència, prenent les mesures adequades per protegir-los enfront de danys accidentals o deliberats que puguin afectar a la disponibilitat, integritat o confidencialitat de la informació tractada o els serveis prestats.

3. Entre els objectius de l'ORGT es troba el desenvolupament dels serveis que presta de conformitat amb l'evolució de la tecnologia, així com promoure i impulsar el seu ús entre la ciutadania i el sector privat. Aquesta evolució comporta també una major facilitat per al tractament d'una gran quantitat d'informació, la qual ha de ser degudament protegida.

4. La consagració del dret a comunicar-se amb l'Administració Pública a través de mitjans electrònics es va recollir a la Llei 11/2007, de 22 de juny, d'accés electrònic dels ciutadans als Serveis Públics. Aquesta Llei, a més, va imposar la necessitat d'una adequada protecció de la informació i dels serveis, que permetés utilitzar els mitjans electrònics amb confiança.

5. Per donar resposta a un marc comú de seguretat de la informació a les administracions públiques, en desenvolupament de la Llei 11/2007, de 22 de juny, es va aprovar el Reial decret 3/2010, de 8 de gener, pel qual es va regular l'Esquema Nacional de Seguretat (ENS) en l'àmbit de l'Administració Electrònica, i va establir els principis bàsics i requisits mínims que, d'acord amb l'interès general, la naturalesa i la complexitat de la matèria regulada, permetran, des de llavors, una protecció adequada de la informació i els serveis.

6. Amb l'aprovació de la Llei 39/2015, d'1 d'octubre, de procediment administratiu comú i la Llei 40/2015, d'1 d'octubre, de règim jurídic del sector públic, es dona un

Document signat electrònicament. Firmes vàlides. És còpia autèntica de l'original electrònic.

Codi Segur de Verificació (CSV): f4cd78e76e7738806b6c Adreça de validació: https://seuelectronica.diba.cat

impuls definitiu a la implantació dels processos electrònics en el sector públic, imposant-se la necessitat de respectar un marc comú de seguretat de la informació. L'entrada en vigor d'ambdues lleis consagra la necessitat de desenvolupar tots els mitjans electrònics necessaris perquè la ciutadania pugui relacionar-se electrònicament amb el sector públic, fent-se imprescindible garantir el compliment dels principis bàsics i requisits mínims, establint les mesures de seguretat necessàries que hauran de ser proporcionals a les dimensions de seguretat rellevants i a la categoria del sistema d'informació a protegir.

7. Mitjançant el Reial decret 311/2022, de 3 de maig, pel qual es regula l'ENS, es deroga el Reial decret 3/2010 (mencionat al punt tercer), actualitzant-se l'ENS per complir tres grans objectius: en primer lloc, alinear l'ENS amb el marc normatiu i el context estratègic existent per garantir la seguretat a l'administració digital; en segon lloc, introduir la capacitat d'ajustar els requisits de l'ENS per garantir la seva adaptació a la realitat de certs col·lectius o tipus de sistemes, atenent la semblança que presenten una multiplicitat d'entitats o serveis pel que fa als riscos als quals estan exposats els seus sistemes d'informació i serveis; i en tercer lloc, facilitar una millor resposta a les tendències en ciberseguretat, reduir vulnerabilitats i promoure la vigilància contínua mitjançant la revisió dels principis bàsics, dels requisits mínims i de les mesures de seguretat.

8. 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. En aquest sentit, l'article 156.2 de la Llei 40/2015, d'1 d'octubre, de règim jurídic del sector públic (LRJSP), disposa: *"L'Esquema Nacional de Seguretat té per objecte establir la política de seguretat en la utilització de mitjans electrònics en l'àmbit d'aquesta Llei, i està constituït pels principis bàsics i requisits mínims que permetin una protecció adequada de la informació."*

9. Per tant, en compliment de l'esmentada normativa, i per mitjà del present Decret, es fixa la Política de Seguretat de la Informació que vetlla per la gestió continuada de la seguretat i on s'estableixen els objectius, principis bàsics i estructura organitzativa necessaris per a la gestió de la seguretat de la informació a l'ORGT de la Diputació de Barcelona.

10. Com part necessària del desenvolupament de la Política de Seguretat la informació, aquest Decret també té per objecte la constitució d'un òrgan col·legiat en matèria de seguretat de la informació de l'ORGT, denominat Comitè de Seguretat de la Informació, incloent-hi la regulació de la seva composició i funcions.

11. Finalment, en el present Decret s'assignen també les funcions que en matèria de seguretat de la informació s'han d'atribuir al Responsable de Servei, Responsable de la Informació, Responsable de Seguretat i Responsable del Sistema, d'acord amb el que disposa l'article 13 ("Organització i implantació del procés de Seguretat") del Reial decret pel qual es regula l'ENS.

Document signat electrònicament. Firmes vàlides. És còpia autèntica de l'original electrònic.

Codi Segur de Verificació (CSV): f4cd78e76e7738806b6c Adreça de validació: https://seuelectronica.diba.cat

Amb aquest decret, la Corporació reafirma el seu compromís amb la necessitat de realitzar una gestió adequada de la seguretat de la informació i amb el compliment de l'ENS i la resta de normativa vigent en matèria de seguretat de la informació.

Fonaments de dret

1 . La Llei 39/2015, d'1 d'octubre, de procediment administratiu comú i la Llei 40/2015, d'1 d'octubre, de règim jurídic del sector públic, i especialment en el seu article 156, estableixen la necessitat d'aprovar una política de seguretat en la utilització de mitjans electrònics en l'àmbit d'actuació del sector públic.

2. El 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 la Llei orgànica 3/2018, de 5 de desembre, de Protecció de Dades i garantia dels drets digitals, estableixen la necessitat d'adoptar mesures de seguretat tècniques i organitzatives, i que en el cas del sector públic en general, són derivades per la Disposició Addicional Primera de la citada Llei orgànica a les mesures previstes a l'ENS.

3. En aplicació del Reial decret que regula l'ENS, és obligació de l'ORGT la protecció de la informació tractada i dels serveis prestats, per la qual cosa ha d'implantar una sèrie de mesures de seguretat que s'aplicaran tant en el marc organitzatiu com en l'operacional i de protecció, i haurà d'aprovar la Política de Seguretat de la Informació, la qual recollirà, entre altres aspectes, els requisits en matèria d'organització de la seguretat mitjançant la designació de rols de seguretat i la constitució del Comitè de Seguretat de la Informació.

4. D'acord amb el que disposa l'article 14, apartat n) dels Estatuts de l'Organisme de Gestió Tributària de la Diputació de Barcelona (publicats al BOPB de 22.02.2023), correspon a la Presidència de l'Organisme de Gestió Tributària de la Diputació de Barcelona exercir aquelles altres competències que, essent inherents a les comeses pròpies de l'Organisme, la normativa atribueixi a la Presidència de l'entitat local amb el caràcter de delegable i no hagi estat reservada a la Presidència de la Diputació o assignada a un altre òrgan.

Les competències atribuïdes a la Presidència de l'ORGT, s'han delegat mitjançant Decret de la Presidència de la Diputació de Barcelona, núm. 12955, de 3 d'octubre de 2024 (BOPB de 4.10.2024), que modifica parcialment els Decrets de la Presidència de la Diputació de Barcelona, números 9902 i 9903, de 26 de juliol de 2023 (BOPB de 28.07.2023), en la Presidenta delegada de l'Àrea de Serveis Generals i Transició Digital de la Diputació de Barcelona.

En virtut de tot això, es proposa l'adopció de la següent

Document signat electrònicament. Firmes vàlides. És còpia autèntica de l'original electrònic.

Codi Segur de Verificació (CSV): f4cd78e76e7738806b6c Adreça de validació: https://seuelectronica.diba.cat

RESOLUCIÓ

Primer. Aprovar la Política de Seguretat de la Informació de l'Organisme de Gestió Tributària de la Diputació de Barcelona en els termes que figuren en l'Annex al present Decret.

Segon. Crear el Comitè de Seguretat de la Informació de l'ORGT de la Diputació de Barcelona. Aquest comitè impulsarà el desenvolupament d'un sistema de gestió conforme als estàndards de seguretat de la informació i estarà integrat pels membres següents:

- El/la president/a del Comitè, càrrec que correspondrà al/la Coordinador/a de l'Àrea de Serveis Generals i Transició Digital de la Diputació de Barcelona, que podrà delegar l'exercici de les funcions de la presidència en la persona que designi
- El/la responsable de la informació
- Els/les responsables dels serveis
- El/la responsable de la seguretat
- El/la responsable del sistema

Tots els membres del Comitè actuaran amb veu i vot, i els seus acords requeriran, com mínim, el vot de la majoria simple dels seus membres.

En supòsit d'acumulació de les funcions de responsable de servei amb alguna altre funció com responsable de la Informació, responsable de la seguretat o responsable del sistema, el vot es computarà com un sol vot.

Els responsables dels serveis, en el cas s'hagin designat per sistemes específics, seran convocats en funció dels assumptes a tractar en cada sessió, sense que es tingui en compte a efectes de quòrum als responsables dels serveis no convocats.

El/la delegat/da de protecció de dades, formarà part del Comitè com assistent sense dret de vot.

Com secretària del Comitè actuarà el/la responsable de la seguretat de l'ORGT o persona designada per la Gerència de l'ORGT.

Es podrà convidar a assistir a determinades sessions a altres persones en funció de l'ordre del dia de la sessió, com assistents sense dret de vot.

El seu funcionament, règim de sessions, així com les funcions i comeses d'aquest comitè són les que es determinen a la Política de Seguretat de la Informació.

Document signat electrònicament. Firmes vàlides. És còpia autèntica de l'original electrònic.

Codi Segur de Verificació (CSV): f4cd78e76e7738806b6c Adreça de validació: https://seuelectronica.diba.cat

Tercer. Assignar les següents funcions a efectes de l'Esquema Nacional de Seguretat:

- El/la responsable de la Informació, a efectes de l'ENS, és la Gerència de l'ORGT o la persona en qui delegui.

- Els/les responsables dels serveis, a efectes de l'ENS, són les persones titulars d'una Direcció de Serveis, respecte als serveis inclosos en la seva direcció, així com la persona titular de la Sots-Direcció de Recursos Humans, respecte als sistemes d'informació de recursos humans.

Atès que l'ORGT disposa de Serveis i Unitats que no tenen una dependència orgànica de cap Direcció, en aquest casos la Gerència assumirà la funció de responsable del servei amb el suport i assistència de les persones que ocupin els respectius càrrecs de Cap de Servei o Cap d'Unitat.

- El/la responsable de la seguretat, a efectes de l'ENS, és la persona titular de la Direcció de Serveis d'Informàtica de l'ORGT o la persona o persones en qui delegui.

El/La responsable de la Seguretat no pot ser la mateixa persona que el/la responsable del Sistema.

La persona responsable de la Seguretat podrà designar un o varis administradors de seguretat dependents d'ella.

- El/la responsable del Sistema, a efectes de l'ENS, és el/la cap de Servei d'Explotació i Sistemes de l'ORGT o la persona en qui delegui.

La persona responsable del Sistema podrà designar un o varis administradors de sistema dependents d'ella.

La concreció de funcions i comeses de les persones designades són les que es determinen a la Política de seguretat d'informació.

Quart. Comunicar l'assignació de funcions a les persones titulars del càrrecs corresponents així com la designació -dels membres del Comitè de Seguretat de la Informació, pel seu coneixement.

Cinquè. Ordenar la publicació de la política aprovada al Portal de Transparència de l'ORGT i donar difusió d'aquesta a tot el personal al servei de l'ORGT per al seu coneixement i efectes.

Sisè. Donar compte a la Junta de Govern de l'Organisme de Gestió Tributària de la Diputació de Barcelona.

Document signat electrònicament. Firmes vàlides. És còpia autèntica de l'original electrònic.

Codi Segur de Verificació (CSV): f4cd78e76e7738806b6c Adreça de validació: https://seuelectronica.diba.cat

ANNEX al Decret pel qual s'acorda aprovar la Política de Seguretat de la Informació de l'Organisme de Gestió Tributària de la Diputació de Barcelona, assignar funcions a efectes de l'Esquema Nacional de Seguretat i crear el Comitè de Seguretat de la Informació de la Corporació (Exp. ORGT/ 2025/0045270)

POLÍTICA DE SEGURETAT DE LA INFORMACIÓ DE L'ORGANISME DE GESTIÓ TRIBUTÀRIA DE LA DIPUTACIÓ DE BARCELONA

Índex

Document signat electrònicament. Firmes vàlides. És còpia autèntica de l'original electrònic.

Codi Segur de Verificació (CSV): 9d5d8c40f51c3f59a53b Adreça de validació: https://seuelectronica.diba.cat

1. INTRODUCCIÓ

L'Organisme de Gestió Tributària de la Diputació de Barcelona (en endavant, "**ORGT**") depèn dels sistemes d'informació per assolir els seus objectius. Aquests sistemes han de ser administrats amb diligència, prenent les mesures adequades, en funció del risc, per protegir-los davant danys accidentals o deliberats que puguin afectar l'autenticitat, traçabilitat, integritat o confidencialitat de la informació tractada o la disponibilitat dels serveis prestats.

L'objectiu últim de la seguretat de la informació és garantir que l'entitat pugui complir amb els seus objectius, desenvolupar les seves funcions o competències i prestar els serveis per a la qual ha estat constituïda, actuant preventivament, supervisant l'activitat diària i reaccionant amb prestesa als incidents.

Els sistemes relatius a les tecnologies de les ciències de la informació i la comunicació (en endavant, "**TIC**") han d'estar protegits contra amenaces de ràpida evolució amb potencial per incidir en la confidencialitat, integritat, disponibilitat, ús previst i valor de la informació i els serveis. Per defensar-se d'aquestes amenaces, es requereix una estratègia que s'adapti als canvis en les condicions de l'entorn per garantir la prestació contínua dels serveis. Això implica que les administracions i òrgans competents han d'aplicar les mesures mínimes de seguretat exigides per l'Esquema Nacional de Seguretat (en endavant, "**ENS**"), així com fer un seguiment continu dels nivells de prestació de serveis, seguir i analitzar les vulnerabilitats reportades, i preparar una resposta efectiva als incidents per garantir la continuïtat dels serveis prestats.

L'ORGT s'ha de cerciorar que la seguretat TIC és una part integral de cada etapa del cicle de vida del sistema, des de la seva concepció fins a la seva 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 plecs de licitació per a projectes on es tractin dades personals, s'adquireixin serveis TIC o es prestin serveis que afectin els sistemes d'informació.

En aquest sentit la Política de Seguretat de la Informació és el conjunt de directrius que regeixen la forma en que una organització gestiona i protegeix la informació que tracta i els serveis que presta, i la seva aprovació és part fonamental del sistema de seguretat de cada Administració.

La present Política de Seguretat assegura un compromís manifest de l'ORGT, per a la seva difusió, consolidació i compliment.

Document signat electrònicament. Firmes vàlides. És còpia autèntica de l'original electrònic.

Codi Segur de Verificació (CSV): 9d5d8c40f51c3f59a53b Adreça de validació: https://seuelectronica.diba.cat

2. ABAST

Aquesta política s'aplica a tots els sistemes d'informació de l'ORGT, a les persones que conformen l'organització i els prestadors de serveis o proveïdors de solucions TIC de l'ORGT.

3. MISSIÓ

L'ORGT és un organisme autònom local de la Diputació de Barcelona, dotat de personalitat jurídica pròpia, que té com a principal finalitat l'exercici de les funcions i potestats de gestió, inspecció i recaptació de tributs i altres ingressos de dret públic per delegació o encàrrec de gestió de les administracions públiques de la província de Barcelona Catalunya i dels Ens públics que en depenen.

L'ORGT exerceix les seves competències, en els termes previstos a les lleis estatals i autonòmiques, en els diferents sectors d'acció pública tributària.

Per exercir les competències municipals, l'ORGT fa ús de sistemes d'informació que han de ser protegits d'una forma efectiva i eficient.

Els objectius en matèria de seguretat que l'ORGT pretén garantir amb la present Política seran:

- Garantir la confidencialitat, integritat, autenticitat de la informació i la continuïtat en la prestació dels serveis.

- Implementar mesures de seguretat en funció del risc.
- Formar i conscienciar els integrants de l'ORGT respecte a la seguretat de la informació. Implementar mesures de seguretat que permetin la traçabilitat dels accessos i respectar, entre d'altres, el principi de mínim privilegi, reforçant també el deure de confidencialitat de les persones usuàries en relació amb la informació que coneixen en l'acompliment de les seves funcions.
- Desplegar i controlar la seguretat física fent que els actius de informació es trobin en àrees segures, protegits per controls d'accés, atenent els riscos detectats.

- Establir la seguretat en la gestió de comunicacions mitjançant els procediments necessaris, aconseguint que la informació que sigui transmesa a través de xarxes de comunicacions sigui adequadament protegida.

- Controlar l'adquisició, desenvolupament i manteniment dels sistemes de informació en totes les fases del cicle de vida dels sistemes d'informació, garantint la seva seguretat per defecte.

Document signat electrònicament. Firmes vàlides. És còpia autèntica de l'original electrònic.

Codi Segur de Verificació (CSV): 9d5d8c40f51c3f59a53b Adreça de validació: https://seuelectronica.diba.cat

- Controlar el compliment de les mesures de seguretat en la prestació de serveis, mantenint el control en l'adquisició i incorporació de nous components del sistema.

- Gestionar els incidents de seguretat per a la correcta detecció, contenció, mitigació i resolució d'aquests, adoptant les mesures necessàries perquè aquests no tornin a reproduir-se.

- Protegir la informació personal, adoptant les mesures tècniques i organitzatives en atenció als riscos derivats del tractament conforme legislació en matèria de protecció de dades.

- Supervisar de forma continuada el sistema de gestió de la seguretat, millorant i corregint les ineficiències detectades.

4. PRINCIPIS RECTORS DE LA POLÍTICA

- Abast estratègic: la seguretat de la informació ha de comptar amb el compromís i suport de tots els nivells de l'entitat i s'haurà de coordinar i integrar-se amb la resta de les iniciatives estratègiques de forma coherent.

- Seguretat integral: la seguretat s'entendrà com un procés integral constituït per tots els elements tècnics, humans, materials i organitzatius, relacionats amb els sistemes de la informació, procurant evitar qualsevol actuació puntual o tractament conjuntural. La seguretat de informació s'ha de considerar com a part de l'operativa habitual, estant present i aplicant-se des del disseny inicial dels sistemes TIC.

- Gestió de la seguretat basada en el risc: la gestió de la seguretat basada en els riscos identificats permetrà el manteniment d'un entorn controlat, minimitzant els riscos fins a nivells acceptables. Les mesures de seguretat s'establiran en funció dels riscos a què estigui subjecta la informació i els seus sistemes, i seran proporcionals al risc que tracten, havent d'estar justificades. Es tindran també en compte els riscos identificats en el tractament de dades personals.

- Prevenció, detecció, resposta i conservació amb la implementació d'accions preventives d'incidents, minimitzant les vulnerabilitats detectades, evitant la materialització de les amenaces i, quan aquestes es produeixin, donant una resposta àgil per restaurar la informació o serveis prestats, garantint una conservació segura de la informació.

- Existència de línies de defensa: l'estratègia de seguretat de l'entitat es dissenya i implementa en capes de seguretat.

Document signat electrònicament. Firmes vàlides. És còpia autèntica de l'original electrònic.

Codi Segur de Verificació (CSV): 9d5d8c40f51c3f59a53b Adreça de validació: https://seuelectronica.diba.cat

- Vigilància contínua i reavaluació periòdica: l'entitat implementarà mitjans per a la detecció i resposta a activitats o comportaments anòmals, a més d'altres que permetin una avaluació continuada de l'estat de seguretat dels actius. Existirà, també, un procés de millora contínua per a la revisió i actualització de les mesures de seguretat, de manera periòdica, d'acord amb la seva eficàcia, l'evolució dels riscos i dels sistemes de protecció.

- Seguretat per defecte i des del disseny: els sistemes han d'estar dissenyats i configurats per garantir la seguretat per defecte. Els sistemes proporcionaran la funcionalitat mínima necessària per prestar el servei per al qual van ser dissenyats, en aplicació del principi de mínim privilegi.

- Diferenciació de responsabilitats: en aplicació d'aquest principi les funcions del Responsable de la Seguretat i del Responsable del Sistema estaran diferenciades.

5. MARC NORMATIU

L'ORGT es regeix pels seus Estatuts, per l'Ordenança general reguladora de gestió, inspecció i recaptació dels ingressos de dret públic la gestió dels quals ha estat delegada a la Diputació de Barcelona i per les normes de caràcter imperatiu intern i comunitari. Els estatuts vigents i resta de normativa interna d'aplicació poden ser consultats al portal de la transparència de l'ORGT.

El marc normatiu en que es desenvolupen les activitats de l'ORGT en l'àmbit de la prestació de serveis electrònics a la ciutadania, sense perjudici de la legislació específica, està integrat fonamentalment per les següents disposicions:

a) Reglament (UE) 2016/679, del Parlament Europeu i del Consell, de 27 d'abril de 2016, relatiu a la protecció de les persones físiques en el que respecta 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).

b) Llei Orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals.

c) Llei 39/2015, d'1 d'octubre, del procediment administratiu comú de les administracions públiques.

d) Llei 40/2015, d'1 d'octubre, de règim jurídic del sector públic.

e) 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.

Document signat electrònicament. Firmes vàlides. És còpia autèntica de l'original electrònic.

Codi Segur de Verificació (CSV): 9d5d8c40f51c3f59a53b Adreça de validació: https://seuelectronica.diba.cat

f) Reial decret llei 12/2018, de 7 de setembre, de seguretat de les xarxes i sistemes d'informació.

g) 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.

h) Llei 6/2020, d'11 de novembre, reguladora de determinats aspectes dels serveis electrònics de confiança.

i) Reial decret 203/2021, de 30 de març, pel qual s'aprova el reglament d'actuació i funcionament del sector públic per mitjans electrònics.

j) Reial decret 311/2022, de 3 de maig, pel qual es regula l'esquema nacional de seguretat en l'àmbit de l'administració electrònica .

k) Reial decret 4/2010, de 8 de gener, pel qual es regula l'esquema nacional d'interoperabilitat en l'àmbit de l'administració electrònica.

l) Llei 29/2010, del 3 d'agost, de l'ús dels mitjans electrònics al sector públic de Catalunya

m) Llei 26/2010, de 3 d'agost, de règim jurídic i de procediment de les administracions públiques de Catalunya

n) Llei 58/2003, de 17 de desembre, general tributària.

o) Reial decret legislatiu 2/2004, de 5 de març, pel que s'aprova el text refós de la Llei reguladora de les hisendes locals.

p) Reial decret 520/2005, de 13 de maig, que aprova el reglament general de desenvolupament de la Llei 58/2003, de 17 de desembre, general tributària, en matèria de revisió en via administrativa.

q) Reial decret 939/2005, de 29 de juliol, pel que s'aprova el reglament general de recaptació.

r) Reial decret 1065/2007, de 27 de juliol, que aprova el reglament general de les actuacions i els procediments de gestió i inspecció tributària i de desenvolupament de les normes comuns dels procediments d'aplicació dels tributs.

s) Reial decret 2063/2004, de 15 d'octubre, pel que s'aprova el reglament general del règim sancionador tributari.

Document signat electrònicament. Firmes vàlides. És còpia autèntica de l'original electrònic.

Codi Segur de Verificació (CSV): 9d5d8c40f51c3f59a53b Adreça de validació: https://seuelectronica.diba.cat

t) Reial decret legislatiu 1175/1990, de 28 de setembre, pel qual s'aproven les tarifes i la instrucció de l'impost sobre activitats econòmiques.

u) Reial decret 243/1995, de 17 de febrer, pel qual es dicten normes per a la gestió de l'impost sobre activitats econòmiques i es regula la delegació de competències en matèria de gestió censal d'aquest impost.

v) Reial decret legislatiu 6/2015, de 30 d'octubre, pel qual s'aprova el text refós de la llei sobre trànsit, circulació de vehicles a motor i seguretat viària.

w) Reial decret 320/1994, de 25 de febrer, pel qual s'aprova el reglament de procediment sancionador en matèria de trànsit, circulació de vehicles a motor i seguretat viària.

x) Reial decret 1428/2003, de 21 de novembre, pel qual s'aprova el reglament general de circulació.

6. ORGANITZACIÓ DE LA SEGURETAT

Tots i cadascun dels usuaris dels sistemes d'informació de l'ORGT, són responsables de la seguretat dels actius informàtics mitjançant un ús correcte dels mateixos, així com de la seguretat de la informació i de les dades de caràcter personal que utilitzen, sempre d'acord amb les seves atribucions professionals.

No obstant això, el manteniment i gestió de la seguretat dels sistemes d'informació i de la protecció de dades personals van íntimament lligats a l'establiment d'una organització. Aquesta organització s'estableix mitjançant la identificació i definició de les diferents activitats i responsabilitats en matèria de gestió de la seguretat dels sistemes d'informació i de la protecció de dades personals, i la implantació d'una estructura que les suporti.

Al respecte l'article 11 de l'ENS disposa que en els sistemes d'informació es diferenciarà el/la responsable de la informació, el/la responsable del servei, el/la responsable de la seguretat i el/la responsable del sistema.

A tal efecte, l'organització de la seguretat de la informació en l'ORGT s'estructura en tres nivells i un òrgan col·legiat amb capacitat decisòria en la seguretat de la informació de l'entitat, sense personalitat jurídica pròpia:

1) Nivells corresponents a les funcions assignades:

Document signat electrònicament. Firmes vàlides. És còpia autèntica de l'original electrònic.

Codi Segur de Verificació (CSV): 9d5d8c40f51c3f59a53b Adreça de validació: https://seuelectronica.diba.cat

a) Nivell de govern:
I. El/la responsable de la informació
II. Els responsables del serveis

b) Nivell de supervisió:
I. El responsable de seguretat

c) Nivell operatiu:
I. El responsable del sistema
II. Els administradors de seguretat de sistema i informació, que es designin pels responsables.

2. El Comitè de Seguretat de la Informació.

En base a les consideracions exposades i l'organització existent a l'ORGT, l'estructura i funcions definida per a l'ORGT és la presentada a continuació.

6.1. Rols i funcions de seguretat.

Per garantir el compliment i l'adaptació de les mesures exigides per la normativa, s'han creat rols o perfils de seguretat i s'han designat els càrrecs o òrgans que els ocuparan, de la manera següent:

- Responsable de la informació
- Responsables dels serveis
- Responsable de seguretat
- Responsable del sistema

El/la responsable de la informació, a efectes de l'ENS, és la Gerència de l'ORGT o la persona en qui delegui. Són funcions del/de la responsable de la informació:

- Establir els requisits de la informació en matèria de seguretat. En el marc de l'ENS, equival a la potestat de determinar els nivells de seguretat de la informació.
- Efectuar les valoracions a que es refereix l'article 40 de l'ENS respecte a la informació gestionada, així com, en el seu cas, la seva posterior modificació.
- Treballar en col·laboració amb els/les responsables de Seguretat i del Sistema en el manteniment dels sistemes catalogats segons l'annex I de l'ENS.
- Rep informació sobre els incidents i de les actuacions realitzades per la seva execució.

Document signat electrònicament. Firmes vàlides. És còpia autèntica de l'original electrònic.

Codi Segur de Verificació (CSV): 9d5d8c40f51c3f59a53b Adreça de validació: https://seuelectronica.diba.cat

- Determina els criteris per assignar i modificar a cada informació el nivell de seguretat requerit, i és responsable de la seva documentació i aprovació formal.
- Qualsevol altra funció que li atorgui l'ENS o la legislació vigent.

Els/les responsables dels serveis, a efectes de l'ENS, són les persones titulars d'una Direcció de Serveis, respecte als serveis inclosos en la seva direcció, així com la persona titular de la Sots-Direcció de Recursos Humans, respecte als serveis relatius a recursos humans. Són funcions dels/de les responsables del servei:

- Establir els requisits dels serveis en matèria de seguretat. En el marc de l'ENS, equival a la potestat de determinar els nivells de seguretat dels serveis .
- Determinar els requisits dels serveis prestats i adoptar les mesures de caràcter tècnic i organitzatiu necessàries que siguin possibles per garantir la seguretat en el cicle de vida dels serveis i sistemes.
- Efectuar les valoracions a que es refereix l'article 40 de l'ENS respecte als serveis gestionats, així com, en el seu cas, la seva posterior modificació.
- Treballar en col·laboració amb els/les responsables de seguretat i del sistema en el manteniment dels sistemes catalogats segons l'annex I de l'ENS.
- Rep informació sobre els incidents i de les actuacions realitzades per la seva execució.
- Vetllar per la inclusió de clàusules sobre seguretat en els contractes amb terceres parts i perquè es compleixin.
- Així mateix, podrà estar obligat a complir amb les obligacions i col·laborar amb els equips que, per raó del seu càrrec o funció, estableix internament el Pla de Continuïtat de Negoci, si escau, per a la gestió de les incidències i execució de les activitats de recuperació.
- Qualsevol altra funció que li atorgui l'ENS o la legislació vigent.

Atès que l'ORGT disposa de Serveis i Unitats que no tenen una dependència orgànica de cap Direcció, en aquest casos la Gerència assumirà la funció de responsable del servei amb el suport i assistència de les persones que ocupin els respectius càrrecs de Cap de Servei o Cap d'Unitat.

El/la responsable de la seguretat, a efectes de l'ENS, és la persona titular de la Direcció de Serveis d'Informàtica de l'ORGT o la persona o persones en qui delegui. El/La responsable de la seguretat no pot ser la mateixa persona que el/la responsable del sistema. Són funcions del/de la responsable de la seguretat:

Document signat electrònicament. Firmes vàlides. És còpia autèntica de l'original electrònic.

Codi Segur de Verificació (CSV): 9d5d8c40f51c3f59a53b Adreça de validació: https://seuelectronica.diba.cat

- Mantenir la seguretat de la informació que tracta i els serveis que presten les infraestructures TIC.
- La determinació de la categoria de seguretat del sistema, amb base en les valoracions dels responsables de la Informació i del Servei
- Realitzar o promoure les auditories periòdiques que permetin verificar el compliment de les obligacions de l'ORGT en matèria de seguretat.
- Promoure la formació i conscienciació del personal TIC dins del seu àmbit de responsabilitat.
- Verificar que les mesures de seguretat establertes són adequades per a la protecció de la informació que es tracta i els serveis que es presten.
- Analitzar, completar i aprovar tota la documentació relacionada amb la seguretat dels sistemes.
- Qualsevol altra funció que li atorgui l'ENS o la legislació vigent

El/la responsable del sistema, a efectes de l'ENS, és el/la cap de Servei d'Explotació i Sistemes de l'ORGT o la persona en qui delegui. Són funcions del/de la responsable del sistema:

- Monitoritzar l'estat de seguretat dels sistemes proporcionat per les eines de gestió d'esdeveniments de seguretat i els mecanismes d'auditoria implementats en els sistemes.
- Donar suport a la investigació dels incidents de seguretat, des que es notifiquen fins que es resolen, i supervisar-la.
- Elaborar els informes periòdics de seguretat, els quals han d'incloure els incidents més rellevants del període.
- Proposar els diferents procediments de seguretat.
- Proposar actualitzacions de les normatives de seguretat TIC de l'ORGT.
- Qualsevol altra funció que li atorgui l'ENS o la legislació vigent

Els/les responsables esmentats comptaran amb la col·laboració i assistència del/de la delegat/da de protecció de dades (en endavant, "**DPD**"). Són funcions del/de la DPD, entre d'altres:

- Informar i assessorar al/a la responsable o l'encarregat/da del tractament i als empleats/des que s'ocupin del tractament de les obligacions que els incumbeixen en matèria de protecció de dades.
- Supervisar el compliment del RGPD, i altres disposicions de protecció de dades, i de les polítiques del/de la responsable o de l'encarregat/da del tractament en matèria de protecció de dades personals, inclosa l'assignació de

Document signat electrònicament. Firmes vàlides. És còpia autèntica de l'original electrònic.

Codi Segur de Verificació (CSV): 9d5d8c40f51c3f59a53b Adreça de validació: https://seuelectronica.diba.cat

responsabilitats, la conscienciació i formació del personal que participa en les operacions de tractament, i les auditories corresponents.
- Cooperar i actuar com a punt de contacte amb les autoritats de control de protecció de dades.

La persona responsable de la seguretat podrà designar un o varis administradors que depenguin d'ella, amb les següents funcions:

a. Comprovar que els controls de seguretat establerts són degudament observats.
b. Comprovar que s'apliquen els procediments aprovats per gestionar el sistema d'informació.
c. La gestió de les autoritzacions i privilegis concedits als usuaris del sistema, incloent-hi la monitorització que l'activitat desenvolupada al sistema s'ajusta al que ha estat autoritzat.
d. Comprovar les instal·lacions de maquinari i programari, les seves modificacions i millores per assegurar que la seguretat no està compromesa i que en tot moment s'ajusten a les autoritzacions pertinents.
e. Monitoritzar l'estat de seguretat del sistema proporcionat per les eines de gestió d'esdeveniments de seguretat i mecanismes d'auditoria tècnica implementats al sistema.
f. Informar a la persona responsable de la seguretat de qualsevol anomalia, compromís o vulnerabilitat relacionada amb la seguretat.
g. Col·laborar en la investigació i resolució d'incidents de seguretat, des de la seva detecció fins a la seva resolució.

La persona responsable del sistema podrà designar un o varis administradors de sistema que realitzaran, entre altres, les següents funcions:

- La implantació, gestió i manteniment de les mesures de seguretat aplicables al sistema d'informació.
- La gestió, configuració i actualització, si escau, del maquinari i programari en què es basen els mecanismes i serveis de seguretat del sistema d'informació.
- L'aplicació dels Procediments Operatius de Seguretat (POS).
- Informar al/a la responsable del Sistema 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.

La designació de les persones corresponents, efectuada pels responsables serà comunicada al Comitè de Seguretat de la Informació.

Document signat electrònicament. Firmes vàlides. És còpia autèntica de l'original electrònic.

Codi Segur de Verificació (CSV): 9d5d8c40f51c3f59a53b Adreça de validació: https://seuelectronica.diba.cat

6.2. Comitè de Seguretat de la Informació.

L'ORGT ha creat el Comitè de Seguretat de la Informació, ha establert la seva composició, les seves funcions i els diversos rols associats.

El Comitè de Seguretat de l'ORGT es reunirà com a mínim amb una periodicitat anual i estarà format pels següents membres:

- El/la president/a del Comitè, càrrec que correspondrà al/la Coordinador/a de l'Àrea de Serveis Generals i Transició Digital de la Diputació de Barcelona, que podrà delegar l'exercici de les funcions de la presidència en la persona que designi
- El/la responsable de la informació
- Els/les responsables dels serveis
- El/la responsable de la seguretat
- El/la responsable del sistema

Tots els membres del Comitè actuaran amb veu i vot, i els seus acords requeriran, com mínim, el vot de la majoria simple dels seus membres.

En supòsit d'acumulació de les funcions de responsable de servei amb alguna altre funció com responsable de la Informació, responsable de la seguretat o responsable del sistema, el vot es computarà com un sol vot.

Els responsables dels serveis, en el cas s'hagin designat per sistemes específics, seran convocats en funció dels assumptes a tractar en cada sessió, sense que es tingui en compte a efectes de quòrum als responsables dels serveis no convocats.

El/la delegat/da de protecció de dades, formarà part del Comitè com assistent sense dret de vot.

Com secretària del Comitè actuarà el/la responsable de la seguretat de l'ORGT o persona designada per la Gerència de l'ORGT.

Es podrà convidar a assistir a determinades sessions a altres persones en funció de l'ordre del dia de la sessió, com assistents sense dret de vot, entre ells:

El/la cap del Gabinet de Prevenció i Seguretat de la Diputació de Barcelona o el/la cap del Servei de Coordinació i Contractació de l'ORGT seran convocats com assistents col·laboradors, en funció dels assumptes a tractar, sempre que es requereixi la seva participació per tractar-se qüestions de control d'accés

Document signat electrònicament. Firmes vàlides. És còpia autèntica de l'original electrònic.

Codi Segur de Verificació (CSV): 9d5d8c40f51c3f59a53b Adreça de validació: https://seuelectronica.diba.cat

físic, perímetres de seguretat, incidents de seguretat i temes relacionats amb el seu àmbit competencial.

Així mateix a nivell de gestió documental el Comitè comptarà amb la col·laboració del responsable de l'arxiu de l'ORGT.

Amb caràcter opcional, altres membres de l'ORGT podran incorporar-se als treballs del Comitè, que podrà crear grups de treball especialitzats, ja siguin de caràcter intern, extern o mixt.

Són funcions de qui ostenti la presidència:

- Convocar i presidir les reunions del Comitè
- Proposar les actuacions necessàries als òrgans de govern de l'ORGT.
- Donar compte a la següent sessió del Comitè d'aquelles actuacions realitzades directament amb els òrgans de govern de l'ORGT.

Són funcions de la Secretaria del Comitè:

- Preparar l'ordre del dia i la documentació necessària per a les reunions del Comitè.
- Aixecar acta dels acords.

6.3. Règim de funcionament i convocatòries del Comitè de Seguretat de la Informació.

Caràcter i periodicitat de les reunions:

- El Comitè celebrarà les seves sessions amb periodicitat mínima anual, prèvia convocatòria a aquest efecte realitzada per la seva Presidència.
- La fixació de les dates les determinarà també la Presidència del Comitè.

Convocatòria de les reunions:

- Les reunions del Comitè han de convocar-se, almenys, amb quatre dies hàbils d'antelació, llevat de les extraordinàries que ho hagin estat amb caràcter urgent.

Celebració de les reunions:

- En qualsevol cas no es podrà celebrar cap reunió sense l'assistència de les persones que ocupin la Presidència i la Secretaria o les persones que les substitueixin, d'acord amb la normativa administrativa vigent sobre òrgans col·legiats.
- El Comitè quedarà constituït amb la presència de la meitat de les persones integrants en segona convocatòria. En cas que no existeixi el quòrum suficient, la Presidència procedirà a convocar la sessió en el termini de 48 hores.
- El Comitè podrà celebrar les seves sessions tant de manera presencial com per videoconferència o altres sistemes telemàtics que permetin la comunicació en temps real entre tots els seus membres.

Document signat electrònicament. Firmes vàlides. És còpia autèntica de l'original electrònic.

Codi Segur de Verificació (CSV): 9d5d8c40f51c3f59a53b Adreça de validació: https://seuelectronica.diba.cat

Quan la sessió es dugui a terme per videoconferència, s'haurà de garantir en tot moment:

a) La identificació dels participants.

b) La possibilitat de seguir, intervenir i votar (si escau) en temps real.

c) La constància de les intervencions i dels acords adoptats, en els mateixos termes que en una sessió presencial.

La convocatòria haurà d'indicar expressament que la sessió es farà per mitjans telemàtics, especificant el sistema o plataforma que s'utilitzarà i les instruccions per a la connexió.

El secretari o la persona que exerceixi les funcions de secretaria comprovarà la identitat dels assistents i ho farà constar a l'acta.

Els acords adoptats en sessions celebrades per videoconferència tindran plena validesa i eficàcia.

6.4. Funcions del Comitè de Seguretat de la Informació.

El Comitè de Seguretat de la Informació tindrà les següents funcions:

a. Atendre les inquietuds que, en matèria de seguretat, es plantegin des de la Direcció de l'entitat i dels diferents departaments.

b. Informar a la Direcció i ser informat regularment de l'estat de la seguretat de la informació.

c. Promoure la millora contínua del sistema de gestió de la seguretat de la informació, amb l'aprovació de plans específics.

d. Elaborar l'estratègia d'evolució de l'organització en allò que respecta a seguretat de la informació.

e. Coordinar els esforços de les diferents àrees en matèria de seguretat de la informació, per assegurar que els esforços són consistents, que estan alineats amb l'estratègia decidida en la matèria, evitant duplicitats.

f. Controlar periòdicament el grau de compliment de les mesures proposades per reduir el risc residual (podent proposar accions de millora) i el correcte funcionament del procediment de gestió d'incidents, vetllant per la coordinació de les diferents àrees de seguretat en la gestió d'aquests incidents.

g. Elaborar (i revisar regularment) la Política de Seguretat de la Informació per a la seva aprovació per la Direcció (o per l'òrgan competent) i aprovar la Normativa de Seguretat de la informació.

Document signat electrònicament. Firmes vàlides. És còpia autèntica de l'original electrònic.

Codi Segur de Verificació (CSV): 9d5d8c40f51c3f59a53b Adreça de validació: https://seuelectronica.diba.cat

h. Promoure la realització de les auditories periòdiques que permetin verificar el compliment de les obligacions de l'ORGT en matèria de seguretat.

i. Prioritzar les actuacions en matèria de seguretat quan els recursos siguin limitats.

j. Vetllar perquè es respecti el principi de seguretat des del disseny, podent requerir l'assessorament el/la responsable de la Seguretat, en totes aquelles iniciatives de l'entitat que afectin la seguretat de la informació o dels sistemes. En particular, haurà de vetllar per la creació i utilització de serveis horitzontals que redueixin duplicitats i donin suport a un funcionament homogeni de tots els sistemes en l'àmbit d' aplicació de l' ENS.

k. Assistir a la Presidència del Comitè, en la resolució dels conflictes de responsabilitat que puguin aparèixer entre els/les diferents responsables i/o entre diferents àrees de l'organització.

l. En els supòsits de dependència jeràrquica entre diferents responsables revisar i validar les decisions de seguretat, així com reforçar el registre i traçabilitat de totes les actuacions per evitar conflictes d'interès.

6.5. Procediments de designació

La Presidència de l'ORGT designarà els integrants del Comitè de Seguretat de la Informació i els responsables . La designació es comunicarà a les parts afectades.

Els membres de Comitè de Seguretat de la Informació i els rols de seguretat s'han de revisar cada quatre anys o quan es produeixi una vacant.

6.6 Resolució de conflictes

La Presidència del Comitè, amb el suport del Comitè de Seguretat de la Informació, s'encarregarà de la resolució dels conflictes i diferències d'opinions que puguin sorgir entre els rols de seguretat.

7. TRACTAMENT DE DADES PERSONALS A L'ORGT

L'ORGT tracta dades de caràcter personal de conformitat amb la normativa de protecció de dades. L'ORGT haurà d'avaluar els riscos relacionats amb les dades personals tractades proposant un pla d'actuació per a la correcció d'aquells riscos que superin el llindar autoritzat.

Document signat electrònicament. Firmes vàlides. És còpia autèntica de l'original electrònic.

Codi Segur de Verificació (CSV): 9d5d8c40f51c3f59a53b Adreça de validació: https://seuelectronica.diba.cat

L'anàlisi de riscos serà reavaluat de forma periòdica, comptant amb l'assessorament i supervisió que realitzi el DPD, i, en tot cas, quan es detecti un tractament d'alt risc, havent de realitzar, en el seu cas, una avaluació d'impacte. La implementació del pla de tractament del risc es coordinarà amb el de l'ENS, així com la resta dels procediments o normes seguretat amb les derivades de les obligacions en matèria de protecció de dades, especialment en el control dels prestadors de serveis o la resposta a incidents i/o bretxes de dades personals.

8. GESTIÓ DE RISCOS

8.1 Anàlisi de riscos

Tots els sistemes subjectes a aquesta Política hauran de realitzar un anàlisi de riscos, avaluant les amenaces i riscos a que estan exposats. Aquest anàlisi es portarà a terme en els següents supòsits:

- regularment, almenys un cop l'any.
- quan canviï la informació tractada
- quan canviïn els serveis prestats.
- quan es produeixi un incident greu de seguretat.
- quan es reportin vulnerabilitats greus.

Per a l'harmonització de les anàlisis de riscos, el Comitè de Seguretat de la Informació establirà una valoració de referència per als diferents tipus d'informació gestionats i els diferents serveis prestats.

Els criteris d'avaluació de riscos detallats s'especificaran en la metodologia d'avaluació de riscos que elaborarà l'organització, basada en estàndards i bones pràctiques reconegudes.

S'hauran de tractar, com a mínim, tots els riscos que puguin impedir la prestació dels serveis o el compliment de la missió de l'organització de manera greu.

Es prioritzaran especialment els riscos que impliquin un cessament en la prestació de serveis a la ciutadania.

8.2. Acceptació del risc residual

Els riscos residuals seran avaluats pel/per la Responsable de Seguretat de la Informació.

Els nivells de risc residual esperats sobre cada informació, després de la implementació de les opcions de tractament previstes (inclosa la implantació de les mesures de seguretat previstes a l'Annex II de l'ENS), hauran de ser prèviament acceptats pel/per la responsable d'aquesta informació.

Document signat electrònicament. Firmes vàlides. És còpia autèntica de l'original electrònic.

Codi Segur de Verificació (CSV): 9d5d8c40f51c3f59a53b Adreça de validació: https://seuelectronica.diba.cat

Els nivells de risc residual esperats sobre cada servei, després de la implementació de les opcions de tractament previstes (inclosa la implantació de les mesures de seguretat previstes a l'Annex II de l'Esquema Nacional de Seguretat), hauran de ser prèviament acceptats pel Responsable d'aquest servei.

Els nivells de risc residual seran presentats pel/per la responsable de Seguretat de la Informació al Comitè de Seguretat de la Informació, perquè aquest procedeixi, si escau, a avaluar, aprovar o rectificar les opcions de tractament proposades.

8.3 Metodologia

Per a la realització de l'anàlisi de riscos es tindran en compte les recomanacions publicades per a l'àmbit de l'Administració Pública i, en especial, les guies elaborades pel Centre Criptològic Nacional i l'Agència Espanyola de Protecció de Dades.

9. GESTIO DEL PERSONAL I PROFESSIONALITAT

Tot el personal, propi o aliè, relacionat amb els sistemes d'informació de l'ORGT, dins de l'àmbit de l'ENS, serà format i informat sobre els seus deures, obligacions i responsabilitats en matèria de seguretat. La seva actuació serà supervisada per verificar que es compleixen els procediments establerts.

Abans de proporcionar les credencials als usuaris de l'ORGT, aquests hauran de conèixer i acceptar la política de seguretat de l'organisme en els aspectes que els hi afectin.

Tots els membres de l'ORGT atendran a una sessió de conscienciació en matèria de seguretat de la informació almenys una vegada a l'any. S'establirà un programa de conscienciació contínua per atendre tots els membres de l'ORGT, en particular als de nova incorporació.

La seguretat dels sistemes d'informació serà atesa, revisada i auditada per personal qualificat, dedicat i instruït en totes les fases del seu cicle de vida: planificació, disseny, adquisició, construcció, desplegament, explotació, manteniment, gestió d'incidències i desmantellament.

De manera objectiva i no discriminatòria, s'exigirà que les organitzacions que ens proporcionin serveis comptin amb professionals qualificats i amb uns nivells idonis de gestió i maduresa dels serveis prestats.

Document signat electrònicament. Firmes vàlides. És còpia autèntica de l'original electrònic.

Codi Segur de Verificació (CSV): 9d5d8c40f51c3f59a53b Adreça de validació: https://seuelectronica.diba.cat

10. CONTROL D'ACCESOS

Es limitarà l'accés als sistemes d'informació als usuaris, processos, dispositius i altres sistemes d'informació, degudament autoritzats i exclusivament a les funcions permeses.

Les credencials d'accés es basaran en sistemes d'autenticació multifactor , i es canviaran amb una periodicitat anual, excepte quan el responsable de seguretat estableixi un període diferent en funció del tipus de credencials i els factors de risc associats.

11. PROTECCIO DE LES INSTAL·LACIONS

L'ORGT disposarà de mecanismes de control d'accés físic, prevenint els accessos físics no autoritzats, així com els danys a la informació i als recursos, mitjançant perímetres de seguretat, controls físics i proteccions generals en àrees.

12. ADQUISICIÓ DE PRODUCTES DE SEGURETAT I CONTRACTACIÓ DE SERVEIS DE SEGURETAT

A l'hora d'adquirir productes, l'ORGT tindrà en compte que aquests productes tinguin certificada la funcionalitat de seguretat relacionada amb l'objecte de la seva adquisició, tret dels casos en què les exigències de proporcionalitat pel que fa als riscos assumits no ho justifiquin, segons el parer del responsable de Seguretat.

13. VIGILÀNCIA CONTÍNUA, REAVALUACIÓ PERIÒDICA I INTEGRITAT, ACTUALITZACIÓ DEL SISTEMA I MILLORA CONTÍNUA DEL PROCÉS DE SEGURETAT

La vigilància contínua per part de l'ORGT permetrà la detecció d'activitats o comportaments anòmals i la seva resposta oportuna.

L'avaluació permanent de l'estat de la seguretat dels actius permetrà mesurar-ne l'evolució, detectar vulnerabilitats i identificar deficiències de configuració.

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

Document signat electrònicament. Firmes vàlides. És còpia autèntica de l'original electrònic.

Codi Segur de Verificació (CSV): 9d5d8c40f51c3f59a53b Adreça de validació: https://seuelectronica.diba.cat

La inclusió de qualsevol element físic o lògic en el catàleg actualitzat d'actius del sistema, o la seva modificació, requerirà autorització formal prèvia.

L'avaluació i la monitorització permanents permetran adequar l'estat de seguretat dels sistemes tenint en compte les deficiències de configuració, les vulnerabilitats identificades i les actualitzacions que els afectin, així com la detecció primerenca de qualsevol incident que tingui lloc sobre aquests.

El procés integral de seguretat implantat haurà de ser actualitzat i millorat de manera contínua. Per a això, s'aplicaran els criteris i mètodes reconeguts en la pràctica nacional i internacional relatius a la gestió de la seguretat de les tecnologies de la informació.

14. PROTECCIÓ DE LA INFORMACIÓ EMMAGATZEMADA I EN TRÀNSIT I CONTINUÏTAT DE L'ACTIVITAT

L'ORGT disposarà de mecanismes per protegir la informació emmagatzemada o en trànsit, especialment quan es troba en entorns insegurs (portàtils, mòbils, tauletes, suports d'informació, xarxes obertes, etc.).

Els sistemes disposen de còpies de seguretat i hi ha establerts els mecanismes necessaris per garantir la continuïtat de les operacions, en cas de pèrdua dels mitjans habituals de treball. S'han desenvolupat procediments que asseguren la recuperació i conservació, a llarg termini, dels documents electrònics produïts per l'ORGT.

De la mateixa manera, s'han implementat mecanismes de seguretat d'acord amb la naturalesa del suport en què estiguin els documents, a fi de garantir que tota la informació relacionada en suport no electrònic estigui protegida amb el mateix grau de seguretat que l'electrònica.

15. EXISTÈNCIA DE LÍNIES DE DEFENSA I PREVENCIÓ DAVANT D'ALTRES SISTEMES D'INFORMACIÓ INTERCONNECTATS

L'ORGT ha implementat una estratègia de protecció del sistema d'informació constituïda per múltiples capes de seguretat, formades per mesures organitzatives, físiques i lògiques, de manera que, quan una capa hagi estat compromesa, permeti desenvolupar una reacció adequada davant dels incidents que no s'hagin pogut evitar, reduint la probabilitat que el sistema sigui compromès en el seu conjunt i minimitzant l'impacte final sobre aquest.

Es protegirà el perímetre del sistema d'informació, especialment quan el sistema de l'ORGT es connecti a xarxes públiques, tal com es defineix en la legislació vigent en matèria de telecomunicacions, reforçant-se les tasques de prevenció, detecció i resposta davant incidents de seguretat.

Document signat electrònicament. Firmes vàlides. És còpia autèntica de l'original electrònic.

Codi Segur de Verificació (CSV): 9d5d8c40f51c3f59a53b Adreça de validació: https://seuelectronica.diba.cat

En tot cas, s'analitzaran els riscos derivats de la interconnexió del sistema amb altres sistemes i es controlarà el seu punt d'unió.

16. REGISTRE D'ACTIVITATS

L'ORGT ha habilitat registres de l'activitat dels usuaris retenint la informació necessària per monitorar, analitzar, investigar i documentar activitats indegudes o no autoritzades, permetent identificar en cada moment la persona que actua. Tot això, amb la finalitat exclusiva d'aconseguir complir l'obligació d'implementar un registre d'activitat del Reial decret 311/2022, de 3 de maig, pel qual es regula l'ENS, amb plenes garanties del dret a l'honor, a la intimitat personal i familiar i la imatge dels afectats, i d'acord amb la normativa sobre protecció de dades personals o laboral i altres disposicions que siguin aplicables

Amb l'objectiu de preservar la seguretat dels sistemes d'informació, garantint l'estricte compliment dels principis d'actuació de les administracions públiques, i d'acord amb el que disposa el Reglament General de Protecció de Dades, així com amb respecte als principis de limitació de la finalitat, minimització de les dades i limitació del termini de conservació que hi són enunciats, l'ORGT podrà, en la mesura estrictament necessària i proporcionada, analitzar les comunicacions entrants o sortints, i únicament amb 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, així com altres danys a les esmentades xarxes i sistemes d'informació.

Per tal de corregir o, si escau, exigir responsabilitats, cada usuari que accedeixi al sistema d'informació haurà d'estar identificat de manera única, de manera que es pugui saber, en tot moment, qui rep drets d'accés, de quin tipus són aquests, i qui ha realitzat una activitat determinada.

17. GESTIÓ D'INCIDENTS DE SEGURETAT

L'ORGT disposarà d'un procediment per a la gestió àgil dels esdeveniments i incidents de seguretat que suposin una amenaça per a la informació i els serveis.

Aquest procediment s'integrarà amb altres relacionats amb els incidents de seguretat d'altres normes sectorials com la de protecció de dades personals o una altra que afecti l'organisme per coordinar la resposta des dels diferents enfocaments i comunicar als diferents organismes de control sense dilacions indegudes i, quan calgui, a les Forces i Cossos de Seguretat l'Estat o els jutjats.

Document signat electrònicament. Firmes vàlides. És còpia autèntica de l'original electrònic.

Codi Segur de Verificació (CSV): 9d5d8c40f51c3f59a53b Adreça de validació: https://seuelectronica.diba.cat

18. TERCERES PARTS /PRESTADORS DE SERVEIS / PROVEÏDORS DE SOLUCIONS

Quan l'ORGT presti serveis a altres entitats o gestioni i informació d'altres, se'ls farà partícips d'aquesta Política de Seguretat de la Informació, sens perjudici de respectar les obligacions de la normativa de protecció de dades si actua com a encarregat/da del tractament en la prestació dels serveis esmentats, i s'establiran canals per a report i coordinació dels respectius Comitès de Seguretat i procediments d'actuació per a la reacció davant incidents de seguretat. A més, el/la responsable de Seguretat (o persona en qui delegui) serà el Punt de Contacte (POC).

Quan l'ORGT utilitzi serveis de tercers o cedeixi informació a tercers, se'ls farà partícips d'aquesta Política de Seguretat i de la Normativa de Seguretat que ateny a aquests serveis o informació, sens perjudici del compliment d'altres obligacions en matèria de protecció de dades. En la contractació de prestadors de serveis o adquisició de productes es tindrà en compte l'obligació de l'adjudicatari de complir amb l'ENS.

L'organització prestatària de serveis a l'ORGT haurà de designar un POC (Punt o Persona de contacte) per 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 solució que proporcioni, com les comunicacions relatives a la seguretat de la informació i la gestió dels incidents per a l'àmbit de l'esmentat servei.

Aquesta tercera part queda subjecta a les obligacions establertes en aquesta normativa, podent desenvolupar els seus propis procediments operatius per a satisfer-la, de manera que l'ORGT pugui supervisar-los o demanar evidències del compliment d'aquests, fins i tot auditories de segona o tercera part. S'establiran procediments específics de report i resolució d'incidències que han de ser canalitzades pel POC dels tercers implicats i, a més, quan s'afecti dades personals pel delegat/da de Protecció de Dades. Els tercers garantiran que el seu personal està adequadament conscienciat en matèria de seguretat, almenys al mateix nivell que l'establert en aquesta Política o el que específicament es pugui exigir en el contracte.

Quan algun aspecte de la Política no pugui ser satisfet per un tercer segons es requereix en els paràgrafs anteriors, el/la Responsable de la Seguretat emetrà un informe que precisi els riscos en què s'incorre i la forma de tractar-los. Es requerirà l'aprovació d'aquest informe pels/per les responsables de la Informació i els Serveis afectats abans de l'inici de la contractació o, si s'escau, de l'adjudicació. L'informe es traslladarà al/a la representant de l'entitat que haurà d'autoritzar la continuació amb la tramitació de contractació del tercer, assumint els riscos detectats.

Document signat electrònicament. Firmes vàlides. És còpia autèntica de l'original electrònic.

Codi Segur de Verificació (CSV): 9d5d8c40f51c3f59a53b Adreça de validació: https://seuelectronica.diba.cat

Quan l'entitat adquireixi, desenvolupi o implanti un sistema d'Intel·ligència Artificial, a més de complir amb el que estableix la normativa vigent en la matèria, haurà de comptar amb l'informe del/de la Responsable de la Seguretat, que consultarà el/la Responsable de la Informació i del Servei i, quan sigui necessari, al/a la del Sistema, havent també el/la Delegat/da de Protecció de Dades d'emetre el seu parer.

19. DESENVOLUPAMENT DE LA POLÍTICA DE SEGURETAT DE LA INFORMACIÓ

Aquesta Política de Seguretat de la Informació complementa/s'integra juntament amb altres polítiques de l'ORGT en diferents matèries, entre elles la Política de signatura electrònica de la Diputació de Barcelona, i la Política de gestió documental, aplicables a l'ORGT en virtut del l'acord número 10 de la Junta de Govern de Diputació , aprovat en sessió de 28 de gener de 2021.

Aquesta Política es desenvoluparà per mitjà de normativa de seguretat que abordi punts específics. La normativa de seguretat estarà a disposició de tots els membres de l'ORGT que necessitin conèixer-la, en particular per a aquells que utilitzin, operin o administrin els sistemes d'informació i comunicacions.

El cos normatiu sobre seguretat de la informació es desenvoluparà en tres nivells per àmbit d'aplicació, nivell de detall tècnic i obligatorietat de compliment. D'aquesta manera cada norma d'un determinat nivell de desenvolupament es fonamentarà en les normes de nivell superior.

Aquests nivells són els següents:

1. Primer nivell normatiu: constituït per aquesta política de seguretat de la informació, la normativa interna de l'ús dels mitjans electrònics i les directrius generals de seguretat aplicables a l'ORGT.

2. Segon nivell normatiu: constituït per les normatives de seguretat derivades de les anteriors.

3. Tercer nivell normatiu: constituït per procediments, guies i instruccions tècniques. Són documents que compleixen el que s'ha exposat a la política de seguretat de la informació i a les normatives i determinen les accions o tasques a realitzar, en l'exercici d'un procés.

Document signat electrònicament. Firmes vàlides. És còpia autèntica de l'original electrònic.

Codi Segur de Verificació (CSV): 9d5d8c40f51c3f59a53b Adreça de validació: https://seuelectronica.diba.cat

20. ADEQUACIÓ DELS CANVIS NORMATIUS I ORGÀNICS

Les prescripcions establertes en aquesta disposició, que incorporen o reprodueixen aspectes de la legislació de l'Estat o l'autonòmica d'aplicació en la matèria aquí regulada, s'entendran automàticament modificades en el moment en què es produeixi la seva revisió.

Totes les referències a càrrecs, òrgans, llocs de treball o a àmbits orgànics, unipersonals o col·legiats, efectuades al llarg de tot el text d'aquesta Política de Seguretat de la Informació s'entendran referides als càrrecs, òrgans, llocs de treball o àmbits orgànics que en cada moment tinguin assignades les funcions nuclears per les què actualment se li han assignat les responsabilitats en l'àmbit de seguretat de la informació.

21. APROVACIÓ DE LA POLÍTICA I ENTRADA EN VIGOR/EFECTIVITAT

Aquesta Política de Seguretat de la Informació és vigent des de la data d'aprovació i fins a que sigui reemplaçada per una nova Política.

Les modificacions de la present Política que suposin canvis o adaptacions davant d'ineficiències les realitzarà el Comitè de Seguretat de la Informació, que haurà de revisar-la anualment.

En cas que els canvis suposin una modificació substancial o dels principis responsabilitats designades, el Comitè de Seguretat de la Informació proposarà els canvis que hauran de ser aprovats, si s'escau, per la persona o òrgan amb les degudes competències.

La substitució de la Política serà instada pel Comitè de Seguretat de la Informació i ratificada per la persona o òrgan amb les degudes competències, del que s'informarà adequadament els interessats pels mateixos canals usats per a la seva difusió.

Document signat electrònicament. Firmes vàlides. És còpia autèntica de l'original electrònic.

Codi Segur de Verificació (CSV): 9d5d8c40f51c3f59a53b Adreça de validació: https://seuelectronica.diba.cat