POLÍTICA DE SEGURETAT

POLÍTICA DE SEGURETAT DE LA INFORMACIÓ DEL CONSELL COMARCAL DEL GARRAF v.7.5

Contingut

INTRODUCCIÓ.

La seguretat de la informació és un dels principis rectors que aplica a tots els processos del procediment administratiu.

El consell Comarcal del Garraf té la ferma voluntat de continuar protegint les dades i la informació que tracta dins dels diferents àmbits de les seves competències aplicant aquelles mesures de seguretat tecnològica, procedimental i jurídica que l'estat de l'art aconselli i acomplint amb la normativa legal vigent.

Com a administració pública local el consell comarcal disposa de dades i d'informació en suport físic i també en suport digital, sent aquest últim el d'especial interès donat que el marc d'operació del procediment administratiu és digital.

L'article 11 de Reial decret 311/2022, de 3 de maig, pel qual es regula l'Esquema Nacional de Seguretat, obliga a les entitats públiques que disposin d'una Política de seguretat de la Informació que articuli un seguit de requisits mínims de seguretat.

La present Política és d'aplicació a les persones vinculades al consell comarcal del Garraf que tinguin accés als sistemes i serveis d'informació, al personal propi que presti els seus serveis als diferents municipis de la comarca, així com a les empreses proveïdores de serveis TIC.

El document recull i considera les dimensions principals de la seguretat d'un sistema d'informació que són: la disponibilitat, la confidencialitat, la integritat, l'autenticitat i la traçabilitat.

D'altra banda, és fonamental garantir que tots els membres de l'organització comprenen la importància de les seves accions en relació a la seguretat de la informació. Per això, és necessària una formació periòdica a tot el personal en matèria de les polítiques, normes i procediments relacionats amb la seguretat de la informació.

Al efectes d'aquesta política entenem que un Sistema d'Informació (SI) és un conjunt integrat de recursos tecnològics, humans, i procedimentals dissenyat per recollir, emmagatzemar, processar, analitzar i distribuir informació necessària per a la gestió i la presa de decisions al consell comarcal. Aquest sistema és fonamental per a la planificació, l'administració i la supervisió dels serveis i les activitats públiques i la seva adequació a la normativa vigent.

Així mateix, considerem que la Política de Seguretat de la Informació és un conjunt de directrius, normes, controls i procediments dissenyats per protegir la informació tractada pel consell comarcal, assegurant la seva confidencialitat, integritat i disponibilitat. Aquesta política estableix les responsabilitats del personal, els usuaris i les usuàries del sistema, de les empreses externes que puguin accedir al sistema i de l'accés a la informació interoperable així com les mesures necessàries per protegir els actius d'informació contra amenaces i riscos.

DESPLEGAMENT DE LA POLÍTICA DE LA SEGURETAT DE LA INFORMACIÓ

Al consell comarcal del Garraf, el desplegament de la Política de Seguretat de la Informació es realitza mitjançant el Pla de Seguretat de la Informació (PSI), que és el document que avalua i implanta les actuacions concretes, segons la base jurídica, tan siguin organitzatives com tecnològiques.

EL PLA DE SEGURETAT DE LA INFORMACIÓ (PSI)

El Pla de Seguretat de la Informació (PSI) del consell comarcal del Garraf considera certs aspectes bàsics per garantir la protecció adequada de la informació sensible i de la continuïtat dels serveis. Aquests són alguns dels aspectes clau que són tractats a la present política:

- Legislació i normatives vigent
- Identificació d'Actius d'Informació
- Avaluació de Riscos
- Polítiques i Procediments de Seguretat
- Control de les telecomunicacions
- Control d'accessos al Sistema d'Informació
- Actualitzacions dels sistemes del maquinari i del programari
- Política de còpies de seguretat i de rescabalament
- Gestió d'Incidents
- Auditories
- Col·laboracions amb altres entitats públiques
- Formació i sensibilització en seguretat TIC i en ciberseguretat
- Millora continuada de la seguretat TIC

CONSIDERACIONS JURÍDIQUES.

La redacció d'aquest document ha pres en consideració la següent normativa:

- Llei 39/2015, d'1 d'octubre, del procediment administratiu comú de les administracions públiques.
- Llei 40/2015, d'1 d'octubre, de règim jurídic del sector públic.
- Llei orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals.
- Llei 59/2003, de 19 de desembre, de signatura electrònica.
- Reial decret 311/2022, de 3 de maig, pel qual es regula l'Esquema Nacional de Seguretat
- Reial decret 4/2010, de 8 de gener, pel qual es regula l'Esquema Nacional d'Interoperabilitat en l'àmbit de l'Administració electrònica.
- Reial Decret 817/2023, de 8 de novembre, que estableix un entorn controlat de proves per a l'assaig del compliment de la proposta de Reglament del Parlament Europeu i del

Consell pel qual s'estableixen normes harmonitzades en matèria d'intel·ligència artificial.

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

ELS SISTEMES D'INTEL·LIGÈNCIA ARTIFICIAL.

La intel·ligència artificial (IA) és una tecnologia disruptiva amb una alta capacitat d'impacte en l'economia i la societat i juntament amb altres tecnologies digitals, presenta un alt potencial per a l'augment de la productivitat, el desenvolupament de nous productes o serveis, la millora en la facilitat de realització de tasques quotidianes, l' automatització de certes tasques rutinàries i el desenvolupament de la innovació.

D'altra banda, els sistemes d'intel·ligència artificial també poden suposar riscos sobre el respecte dels drets fonamentals de la ciutadania, com per exemple els relatius a la discriminació i a la protecció de dades personals.

Donades aquestes circumstàncies actuals, la Comissió Europea ha presentat una proposta de Reglament del Parlament Europeu i del Consell pel qual s'estableixen normes harmonitzades en matèria d'intel·ligència artificial amb l'objectiu d'assegurar el respecte dels drets fonamentals de la ciutadania i generar confiança en el desenvolupament i la utilització de la intel·ligència artificial en l'economia i la societat. L'esmentat Reglament busca proveir la Unió Europea d'un marc normatiu per tal de promoure una intel·ligència artificial fiable, ètica i robusta.

El consell comarcal considerarà i aplicarà l'evolució normativa de la intel·ligència artificial en aquells productes o serveis que incorpori en un futur tant als processos com als procediments del govern local, a l'entorn de direcció i administratiu i en la prestació del serveis. Especialment es farà ús, quan hi siguin disponibles, de les guies oficials que facilitin a les entitats i els organismes públics l'alineament amb la proposta del Reglament Europeu d'Intel·ligència Artificial.

El compromís és, en el moment que s'incorporin tecnologies d'IA al consell comarcal, el de portar un Registre d'aquests sistemes d'IA, el proveïdor de la solució tecnològica, les dades que tracti, la ubicació de les mateixes, els procediments afectats, i donar publicitat al registre pels mitjans adients.

L'ESQUEMA NACIONAL DE SEGURETAT.

El Reial decret 311/2022, de 3 de maig, pel qual es regula l'Esquema Nacional de Seguretat substitueix el Reial decret 3/2010, de 8 de gener, pel qual es regula l'Esquema Nacional de Seguretat en l'àmbit de l'Administració Electrònica.

El Reial decret 311/2022 actualitza l'Esquema Nacional de Seguretat (ENS) per a:

Primer, alinear l' ENS amb el marc normatiu i el context estratègic existents per garantir la seguretat en l' Administració Digital.

Segon, 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 dels riscos als quals estan exposats els seus sistemes d'informació.

Tercer, reforçar la protecció davant les tendències en ciberseguretat mitjançant la revisió dels principis bàsics, els requisits mínims i les mesures de seguretat que s' han d' adoptar per les entitats subjectes a l' ENS.

Els sistemes afectats s'han d'adequar al que disposa el Reial decret en un termini de vint-i-quatre mesos comptats a partir de la seva entrada en vigor.

OBJECTIUS

L'Esquema Nacional de Seguretat (ENS) persegueix els següents grans objectius:

- Crear les condicions necessàries de seguretat en l' ús dels medi electrònics, a través de mesures per garantir la seguretat dels sistemes, les dades, les comunicacions, i els serveis electrònics, que permeti l' exercici de drets i el compliment de deures a través d' aquests mitjans.
- Promoure la gestió continuada de la seguretat.
- Promoure la prevenció, detecció i correcció, per a una millor resiliència en l'escenari de ciberamenaces i ciberatacs.
- Promoure un tractament homogeni de la seguretat que faciliti la cooperació en la prestació de serveis públics digitals quan hi participen diverses entitats.

ELEMENTS DE L'ESQUEMA NACIONAL DE SEGURETAT.

Els elements principals de l' ENS són els següents:

- Els principis bàsics a considerar en les decisions en matèria de seguretat (arts. 5-11).
- Els requisits mínims que permetin una protecció adequada de la informació (arts. 12-27).
- El mecanisme per aconseguir el compliment dels principis bàsics i dels requisits mínims mitjançant l'adopció de mesures de seguretat proporcionades a la naturalesa de la informació i els serveis a protegir (arts. 28, 40, 41, Annex I i Annex II).
- L'ús d'infraestructures i serveis comuns (art. 29).
- Els perfils de compliment específics (art. 30).
- L'informe d'estat de la seguretat (art. 32)
- L'auditoria de la seguretat (art. 31 i Annex III).
- La resposta davant incidents de seguretat (arts. 33 i 34).
- L'ús de productes certificats (art. 19 i Annex II).
- La conformitat (art. 38).
- La formació i la conscienciació (disposició addicional primera).
- Les guies de seguretat (disposició addicional segona).
- Les instruccions tècniques de seguretat (disposició addicional segona).

El mandat principal de l'ENS és l'establert a l'article 12 'Política de seguretat i requisits mínims de seguretat', segons el qual "cada administració pública comptarà amb una política de seguretat formalment aprovada per l'òrgan competent", la qual "és el conjunt de directrius que regeixen la forma en què una organització gestiona i protegeix la informació que tracta i els serveis que presta" i s'establirà d'acord amb els principis bàsics i es desenvoluparà aplicant els requisits mínims, en proporció als riscos identificats en cada sistema.

Les instruccions tècniques de seguretat , d'obligat compliment, són essencials per aconseguir una adequada, homogènia i coherent implantació dels requisits i mesures recollits en l'Esquema i, particularment, per indicar la manera comuna d'actuar en aspectes concrets.

Les guies de seguretat CCN-STIC , publicades pel Centre Criptològic Nacional, en particular, la col·lecció de guies de la sèrie 800 ajuden al millor compliment del que estableix l'Esquema Nacional de Seguretat.

ÀMBIT D'APLICACIÓ.

L'àmbit d'aplicació de l'Esquema Nacional de Seguretat comprèn tot el Sector Públic, en els termes previstos a l'article 2 de la Llei 40/2015; als sistemes que tracten informació classificada, sense perjudici de l'aplicació de la Llei 9/1968, de 5 d'abril, de Secrets Oficials; i als sistemes d' informació de les entitats del sector privat quan prestin serveis o proveeixin solucions a les entitats del sector públic per a l' exercici de les seves competències i potestats administratives.

ADEQÜACIÓ A L'ESQUEMA NACIONAL DE SEGURETAT.

Una adequació ordenada a l' Esquema Nacional de Seguretat requereix genèricament el tractament de les següents qüestions principals:

- Preparar i aprovar la política de seguretat, incloent-hi els objectius o missió de l' organització, el marc regulatori de les activitats, la definició de rols de seguretat, l' estructura i composició del comitè per a la gestió i coordinació de la seguretat, les directrius d' estructuració de la documentació de la seguretat, i els riscos derivats del tractament de dades personals.
- Categoritzar els sistemes atenent la valoració de la informació manejada i dels serveis prestats.
- Realitzar l' anàlisi de riscos, incloent-hi la valoració de les mesures de seguretat existents.
- Preparar i aprovar la Declaració d' aplicabilitat de les mesures de l' Annex II de l' ENS.
- Elaborar un pla d' adequació per a la millora de la seguretat, sobre la base de les insuficiències detectades, incloent terminis estimats d' execució.
- Implantar, operar i monitoritzar les mesures de seguretat a través de la gestió continuada de la seguretat corresponent.
- Auditar la seguretat per verificar el compliment dels requisits de l' ENS.
- Obtenir i donar publicitat a la conformitat amb l' ENS.
- Informar sobre l' estat de la seguretat.

- Adequació a l' ENS

CONFORMITAT AMB L'ENS.

L'article 38 sobre 'Procediments de determinació de la conformitat amb l'Esquema Nacional de Seguretat' assenyala que tots els subjectes responsables dels sistemes d'informació afectats per l'ENS donaran publicitat de les declaracions i certificacions conforme a l'ENS en els seus portals d'internet o seus electròniques. Aquesta obligació afecta tot el Sector Públic, els sistemes d' informació classificada i les entitats del sector privat que els prestin solucions i serveis per a l' exercici de competències i potestats administratives.

La Instrucció Tècnica de Seguretat de conformitat amb l' Esquema Nacional de Seguretat estableix els criteris i procediments per a la determinació de la conformitat, així com per a la publicitat de l' esmentada conformitat. Precisa els mecanismes d' obtenció i publicitat de les declaracions de conformitat i dels distintius de seguretat obtinguts respecte al compliment de l'ENS.

DADES DE CARÀCTER PERSONAL.

L'ús correcte dels recursos disponibles, la gestió adequada dels serveis en línia i la necessitat d'intercanvis de dades en entorns digitals comporten tots ells el tractament de dades de caràcter personal, un àmbit de creixent importància i subjecte a un escrutini normatiu rigorós. Donada la gran sensibilitat d'aquest tipus d'informació, s'estableixen una sèrie de directives específiques que l'organització i terceres parts associades han de seguir en el seu tractament, sota el marc del que estipula l'Esquema Nacional de Seguretat.

El Consell comarcal del Garraf vetllarà per garantir els drets relacionats amb la protecció de dades de caràcter personal com són el dret d'accés, el dret de rectificació, el dret de supressió, el dret d'oposició al tractament, el dret de limitació del tractament i el dret a la portabilitat de les dades de caràcter personal.

COMPLIMENT DE LA LEGALITAT.

Compliment legal: Es garantirà el compliment estricte de totes les normes aplicables en matèria de protecció de dades personals incloses, entre d'altres, la Llei Orgànica de Protecció de Dades i Garantia de Drets Digitals i el Reglament General de Protecció de Dades de la Unió Europea.

PRINCIPIS RECTORS.

Principis rectors: El tractament de dades personals haurà de tenir sempre com a principis rectors la licitud, la lleialtat i la transparència, garantint-se sempre que l'obtenció de les dades s'hagi fet de manera legal i justa.

MINIMITZACIÓ DE LES DADES.

Minimització de dades: Només es recolliran les dades estrictament necessàries per a l'execució de la funció o servei requerit, assegurant-se que les dades no s'utilitzin més enllà de la finalitat per la qual es van recollir.

SEGURETAT DE LES DADES.

Seguretat de les dades: Es garantirà la seguretat de les dades personals emmagatzemades o processades, mitjançant l'ús de mesures de seguretat tècniques i organitzatives apropiades que protegeixin les dades contra pèrdua, alteració o accés no autoritzat.

DRET D'INFORMACIÓ I CONSENTIMENT.

Dret d'informació i consentiment: Es garantirà la informació clara, transparent i comprensible a la persona afectada sobre quines dades personals es recullen, com seran tractades i amb quin propòsit, així com la recollida del seu consentiment explícit quan escaigui.

ACTUALITZACIÓ I RECTIFICACIÓ.

Actualització i rectificació: Es garantirà que totes les dades personals processades estiguin actualitzades i siguin correctes. En aquest sentit, es proporcionaran mitjans perquè les persones afectades puguin sol·licitar la rectificació o supressió de les seves dades.

CONSERVACIÓ I SUPRESSIÓ.

Conservació i supressió: Les dades personals només es conservaran durant el temps necessari per a la finalitat per la qual van ser recollides. Una vegada transcorregut aquest període, o si aquestes han de ser esborrades a petició de la persona afectada, es garantirà la seva supressió segura.

TRANSFERÈNCIA DE DADES.

Transferència de dades: Tot tipus de transferència de dades personals a terceres parts complirà amb el marc legal vigent i els criteris establerts per la política de seguretat de la informació.

Aquesta política de tractament escrupolós de les dades de caràcter personal contribueix a garantir el respecte dels drets i llibertats individuals i a augmentar la confiança de les persones usuàries cap a l'organització.

LA INTEROPERABILITAT.

El marc legal de la interoperabilitat està basat en el Reial decret 4/2010, de 8 de gener, pel qual es regula l'Esquema Nacional d'Interoperabilitat en l'àmbit de l'Administració electrònica.

El Consell comarcal del Garraf accedeix als serveis interoperables mitjançant la plataforma Extranet de les Administracions Catalanes (EACAT), concretament fent ús del Servei de via Oberta.

Els processos administratius, i els tràmits associats, han estat adaptats amb totes les garanties jurídiques a la consulta digital de dades dels administrats en poder d'altres administracions públiques.

El sistema requereix de les auditories internes anuals per verificar el bon funcionament del sistema i, així mateix, per identificar possibilitats de millora.

OBLIGACIONS DE TERCERS.

En un entorn cada cop més interconnectat, l'organització comparteix i intercanvia informació amb altres organitzacions públiques i també amb empreses externes que son proveïdores de serveis, i amb la ciutadania. Aquests tercers també tenen un paper clau en el manteniment de la seguretat de la informació del consell comarcal. Sota l'Esquema Nacional de Seguretat, és pertinent establir un conjunt d'obligacions per a aquests tercers per garantir el tractament de la informació segons la legislació vigent i la normativa pròpia del consell comarcal.

IDENTIFICACIÓ DE RISCOS DE TERCERS.

El consell comarcal és conscient dels riscos que genera l'accés per tercers al Sistema d'Informació i, en conseqüència, ha definit un conjunt de mesures de seguretat aplicables i exigibles a aquest col·lectiu.

El consell comarcal es reserva el dret de verificar, mitjançant auditories periòdiques, el compliment de tota mesura de seguretat addicional no recollida a la present normativa i inclosa a les clàusules particulars dels contractes subscrits amb tercers.

Addicionalment, els anàlisis de riscos periòdics realitzats pel consell comarcal recolliran les amenaces detectades de serveis prestats per tercers.

COMPLIMENT DE LES POLÍTIQUES DE SEGURETAT.

Els tercers han de complir amb les polítiques i procediments de seguretat de la informació establerts per l'organització, incloent-hi, entre d'altres, els relacionats amb l'accés, ús, emmagatzematge i transmissió de dades.

És d'especial importància que les empreses proveïdores del consell comarcal de serveis i productes TIC coneguin, respectin i apliquin aquesta política de seguretat de la informació, així com altres instruccions tècniques i normatives internes relacionades amb la seguretat de la informació.

RESPONSABILITATS DEL PERSONAL DE TERCERS QUE PRESTIN SERVEIS TIC AL CONSELL COMARCAL.

Com a responsables de la informació que es processa, els tercers han de respondre per qualsevol incident de seguretat que pogués afectar a aquesta informació, incloent la seva obligació de comunicar immediatament al consell comarcal del Garraf qualsevol problema o incident de seguretat.

És responsabilitat de les persones que depenen d'organitzacions o tercers que prestin serveis TIC al consell comarcal el compliment de les directrius establertes en aquesta Política de Seguretat de la Informació, fent un ús segur i responsable dels canals de comunicació del consell comarcal, dels recursos TIC i de la informació intercanviada.

CONFIDENCIALITAT I PROTECCIÓ DE LA INFORMACIÓ.

Els tercers han de respectar i assegurar la confidencialitat de tota la informació a la qual tinguin accés, així com implementar les mesures de seguretat adequades per garantir la protecció de la mateixa.

FORMACIÓ.

Els tercers han de garantir que el personal que té accés a la informació de l'organització hagi rebut la formació adequada en termes de la seguretat de la informació.

REVISIÓ I AUDITORIA.

El consell comarcal es reserva sol·licitar revisions de seguretat o auditories a tercers que accedeixen al sistema d'informació a efectes d'avaluar el compliment de les polítiques i procediments de seguretat.

CONSIDERACIONS ORGANITZATIVES.

EL COMITÉ DE SEGURETAT DE LA INFORMACIÓ.

L'aplicació de la Política de Seguretat de la Informació del consell comarcal requereix del treball conjunt del Comitè de Seguretat de la Informació (CSI) que està integrat per personal de l'administració amb les funcions de Gerència, Secretaria, Delegat de Protecció de dades, Cap de Serveis Generals, i Coordinador TIC com a Responsable de Seguretat i l'Administrador del sistema.

El CSI es reunirà amb un periodicitat mínima semestral i aixecarà acta dels assumptes tractats i dels acords adoptats.

El CSI aprovarà els procediments interns de seguretat i supervisarà altres assumptes com les inversions en seguretat, les auditories periòdiques i altres competències que li siguin assignades.

FUNCIONS DELS MEMBRES DEL COMITÉ DE SEGURETAT DE LA INFORMACIÓ.

Les principals funcions dels diferents membres del Comité de Seguretat de la Informació es detallen tot seguit.

RESPONSABLE DE SEGURETAT DE LA INFORMACIÓ.

El Responsable de seguretat de la informació té com a funcions principals les següents:

- Coordinació i Control: Coordinar i controlar les mesures de seguretat definides i garantir-ne el compliment.
- Informe al Comitè: Reportar regularment al Comitè de Seguretat de la Informació sobre l'estat de la seguretat.
- Secretari del Comitè: Actuar com a secretari del Comitè de Seguretat de la Informació, convocar les reunions i preparar els temes a tractar.
- Formació i Conscienciació: Promoure la formació i la conscienciació en matèria de seguretat de la informació dins del seu àmbit de responsabilitat.
- Anàlisi de Riscos: Realitzar l'anàlisi de riscos i elaborar una declaració d'aplicabilitat a partir de les mesures de seguretat requerides.
- Documentació de Seguretat: Coordinar l'elaboració de la documentació de seguretat del sistema.
- Política de Seguretat: Participar en l'elaboració i l'aprovació de la política de seguretat de la informació.
- Procediments Operatius: Elaborar i aprovar els procediments operatius de seguretat de la informació.
- Resum d'Actuacions: Facilitar periòdicament un resum d'actuacions en matèria de seguretat, incidents i estat de la seguretat del sistema.

- Plans de Millora: Elaborar plans de millora de la seguretat conjuntament amb els responsables de sistemes.
- Validació de Plans de Continuïtat: Validar els plans de continuïtat dels sistemes i assegurar-ne les proves periòdiques.

RESPONSABLE DE SISTEMES.

El Responsable de sistemes, bé sigui personal del consell comarcal o es contractin aquestes funcions a una empresa externa qualificada a nivell alt de compliment amb l'ENS, i sent aquest perfil incompatible amb el de Responsable de seguretat, ha d'exercir les següent funcions principals:

- Desenvolupament i Operació: Desenvolupar, operar i mantenir els sistemes d'informació, definint la seva topologia i sistema de gestió.
- Integració de Seguretat: Garantir que les mesures de seguretat s'integrin adequadament dins del marc general de seguretat.
- Suspensió de Serveis: Acordar la suspensió de l'operació amb certa informació o la prestació d'un servei si es detecten deficiències greus de seguretat, en coordinació amb els responsables corresponents.
- Monitorització de Seguretat: Monitoritzar l'estat de la seguretat del sistema d'informació i reportar periòdicament al Responsable de Seguretat de la Informació.
- Plans de Continuïtat: Elaborar plans de continuïtat del sistema, validar-los i realitzar proves periòdiques per mantenir-los actualitzats.
- Directrius de Seguretat: Elaborar directrius per considerar la seguretat de la informació durant tot el cicle de vida dels actius i processos, i facilitar-les al Responsable de Seguretat de la Informació per a la seva aprovació.

DELEGAT DE PROTECCIÓ DE DADES (DPD)

Les funcions principals del Delegat de Protecció de Dades (DPD) pel que fa a questa política de seguretat són les que es recullen a continuació:

- Informació i Assessorament: Informar i assessorar el responsable, l'encarregat i els empleats sobre les seves obligacions en matèria de protecció de dades.
- Supervisió del Compliment: Supervisar el compliment de la normativa, incloent-hi l'assignació de responsabilitats, la conscienciació i la formació del personal.
- Avaluació d'Impacte: Assessorar sobre les avaluacions d'impacte relatives a la protecció de dades i supervisar-ne la realització.
- Cooperació amb Autoritats: Cooperar amb les autoritats de control i actuar com a punt de contacte en qüestions relatives al tractament de dades.
- Gestió de Violacions de Seguretat: Establir procediments per a la gestió de violacions de seguretat de les dades, incloent-hi l'avaluació del risc i la notificació a les autoritats de supervisió i els afectats.
- Registre d'Activitats: Mantenir els registres d'activitats de tractament de dades i assegurar-ne la correcta gestió.

- Formació i Sensibilització: Desenvolupar programes de formació i sensibilització en matèria de protecció de dades per al personal.

OBLIGACIONS DEL PERSONAL.

En l'àmbit de la seguretat de la informació, un dels elements més importants és el factor humà. L'Esquema Nacional de Seguretat (ENS) estableix la necessitat de fixar un conjunt clar d'obligacions per al personal de l'organització. Aquestes obligacions garanteixen el compliment de la normativa esdevenint recursos claus per a la creació d'una cultura organitzativa centrada en la seguretat. A continuació es detallen aquestes obligacions.

COMPLIMENT DE LES POLÍTIQUES DE SEGURETAT.

Tots els membres de l'organització estan subjectes al compliment de les polítiques i procediments relatius a la seguretat de la informació. L'incompliment d'aquests pot comportar sancions d'acord amb el que disposi la normativa interna.

RESPONSABILITAT INDIVIDUAL.

Cada membre del personal és directament responsable de la seguretat de la informació que gestiona en l'exercici de les seves funcions. Tot el personal té l'obligació de fer conèixer al Responsable de seguretat qualsevol incident de seguretat de la informació.

CONFIDENCIALITAT.

El personal està obligat a respectar i preservar la confidencialitat de la informació a la qual tingui accés per raó del seu treball. La divulgació d'aquesta informació a terceres parts sense l'autorització corresponent estarà estrictament prohibida.

ÚS ADEQUAT DELS RECURSOS.

Les eines tecnològiques posades a disposició del personal per l'organització han de ser utilitzades de manera conscient i responsable. Qualsevol ús inapropiat d'aquests recursos, o la realització d'activitats contràries a les polítiques de seguretat, comportarà l'adopció de les mesures disciplinàries corresponents.

PREVENCIÓ D'ACTUACIONS DE RISC.

El personal ha de prendre totes les mesures necessàries per prevenir qualsevol comportament que pugui posar en perill la seguretat de la informació de l'organització.

PLA DE CONTINUÏTAT.

El Pla de Continuïtat estableix la continuïtat d'una organització des de múltiples perspectives: infraestructura TIC, recursos humans, sistemes de comunicació, infraestructures físiques, etc.

Cadascun d' aquests àmbits disposa un pla de continuïtat més específic. Per exemple, un Pla de Continuïtat TIC (PCTIC), centrat en l'àmbit de les tecnologies de la informació o un Pla de Recuperació davant Desastres (PRD), centrat un àmbit més general de l'organització.

Aquests plans es realitzen prenent en consideració l'Anàlisi de l'impacte per protegir els actius i els processos crítics. Una vegada identificats es realitza un Anàlisis de riscos que poden afectar a sistema d'informació, la seva probabilitat i l'impacte que tindrien. Per últim es redacta un Pla de tractament dels riscos per eliminar-los, mitigar-los, o transferir el risc a un tercer.

La estratègia de continuïtat ha de considerar l'absència de personal, la no disponibilitat de la ubicació habitual de treball, les fallides i els atacs a les tecnologies utilitzades al consell comarcal, la no disponibilitat de la informació i la no disponibilitat dels proveïdors.

Segons la Guia CCN-TEC 010 publicada pel Centre Criptològic Nacional que tracta de la disponibilitat dels sistemes TIC, les fases a considerar són les següents:

- Fase 0. Determinació de l'abast
- Fase 1. Anàlisi de l'organització
- Fase 2. Determinació de l'estratègia de continuïtat
- Fase 3. Resposta a la contingència
- Fase 4. Prova, manteniment i revisió
- Fase 5. Conscienciació

GESTIÓ DE RISCOS.

Un dels aspectes indispensables per a una gestió eficient de la seguretat de la informació és la identificació i tractament dels riscos de seguretat que poden afectar els actius del consell comarcal. Això requereix d'un procés continu que permeti la identificació, l'anàlisi i el tractament del risc, així com la presa de decisions per mitigar o acceptar els riscos identificats. Les directrius bàsiques a seguir segons l'ENS són les que a continuació es descriuen.

IDENTIFICACIÓ DE RISCOS.

S'han d'identificar de potencials amenaces i vulnerabilitats que poden afectar la confidencialitat, integritat i disponibilitat dels actius d'informació. Aquesta identificació ha de ser exhaustiva i ha de tindre en compte tots els possibles vectors d'atac.

AVALUACIÓ DE RISCOS.

Una vegada identificats els riscos, aquests han de ser analitzats i avaluats per a determinar la seva probabilitat i impacte potencial. Aquesta avaluació ha de prendre en consideració no només els aspectes tècnics, sinó també els aspectes legals, operatius i de reputació.

TRACTAMENT DE RISCOS.

Segons els resultats de l'anàlisi i avaluació, s'ha d'establir un pla de tractament de riscos que pot recomanar el tancament d'una activitat de risc, la implementació de mesures de control per reduir el risc, la transferència del risc o simplement l'acceptació del risc.

CONTROL I REVISIÓ.

El procés de gestió de riscos ha de ser revisat i controlat de manera regular per considerar nous riscos emergents i valorar l'eficàcia de les mesures de control implementades.

COMUNICACIÓ I FORMACIÓ.

Els riscos, així com les mesures de control establertes, han de ser comunicats adequadament al personal pertinent, i aquest haurà de rebre la formació necessària per comprendre i gestionar aquests riscos.

DOCUMENTACIÓ.

Totes les activitats relacionades amb la gestió de riscos s'han de documentar adequadament, incloent la identificació de riscos, l'anàlisi i avaluació, les decisions de tractament de riscos, així com les revisions i canvis.

GESTIÓ DE LA INTEROPERABILITAT.

El consell comarcal del Garraf disposa d'un Responsable d'interoperabilitat que, entre d'altres funcions, vetlla per l'ús proporcional dels sistema de consultes digitals de dades dels administrats en poder d'altres administracions públiques.

CATEGORITZACIÓ DELS SISTEMES D'INFORMACIÓ.

És obligatori establir una sèrie de mesures i salvaguardes per al compliment dels requisits mínims de disponibilitat. Per tal de determinar l' impacte que tindria sobre l'organització un incident que afectés la seguretat de la informació tractada o dels serveis prestats, s'ha establert la categoria de seguretat de les dimensions: Disponibilitat, Confidencialitat, Integritat, Autenticitat i Traçabilitat (segons l'ENS).

Aquesta categorització servirà per conèixer els actius i serveis de més importància, permetent així seleccionar aquelles salvaguardes necessàries per a la protecció dels sistemes i prioritzar aquestes mateixes segons la seva importància.

Les categories definides dins del marc de l'Esquema Nacional de Seguretat (ENS), són les següents:

- Nivell BAIX. Una interrupció en l'accés o ús de la informació suposa un perjudici limitat sobre les funcions del consell comarcal, els seus actius o sobre el personal o els tercers que puguin resultar afectats. S'entén per perjudici limitat:
    - La reducció de forma apreciable de la capacitat del consell comarcal per a desenvolupar eficaçment les seves funcions i competències, encara que aquestes segueixin desenvolupant-se.
    - Causar un dany menor en els actius de l'organització.
    - L'incompliment formal d' alguna llei o regulació, que tingui caràcter esmenable.
    - Altres anàlegs.
- Nivell MITJÀ. Una interrupció en l'accés o ús de la informació suposa un perjudici greu sobre les funcions del consell comarcal, els seus actius o sobre els individus afectats. S'entén per perjudici greu:
    - La reducció significativa de la capacitat del consell comarcal per desenvolupar eficaçment les seves funcions i competències, encara que aquestes segueixin desenvolupant-se.
    - Causar un dany significatiu en els actius de l' organització.
    - L' incompliment material d' alguna llei o regulació, o l' incompliment formal que no es pugui esmenar.
    - Causar un perjudici significatiu a algun individu, de difícil reparació.
    - Altres anàlegs.

• Nivell ALT. Una interrupció en l' accés o ús de la informació suposa un perjudici molt greu sobre les funcions del consell comarcal, els seus actius o sobre els individus afectats. S' entendrà per perjudici molt greu:

- L'anul·lació efectiva de la capacitat del consell comarcal per desenvolupar eficaçment les seves funcions i competències.
- Causar un dany molt greu, i fins i tot irreparable, als actius del consell comarcal.
- L' incompliment greu d' alguna llei o regulació.
- Causar un perjudici greu a algun individu, de difícil o impossible reparació.
- Altres anàlegs.

LA SEGURETAT FÍSICA.

Els actius d'informació físics es protegeixen en espais adequats i segurs dins de les mesures disposades per l'Àrea de Serveis Generals i Organització sent les principals les de disposar de control d'accés mitjançant el servei de Consergeria, registre d'entrades i sortides del personal d'empreses externes, sistemes d'alarma de seguretat connectats amb la policia local, sistema de gravació d'imatges, accessos amb clau als espais amb sistemes d'informació i de sistema antiincendis.

SEGURETAT FÍSICA I AMBIENTAL DELS SISTEMES TIC.

Els Centres de Processament de Dades (CPDs) són sales o instal·lacions degudament condicionades que contenen servidors i xarxes de comunicació necessàries per a l'operació de l'organització. Mantenen una gran quantitat de dispositius informàtics i electrònics.

Aquests centres ajuden a aconseguir un alt grau de protecció física gràcies a la implementació de les següents mesures com són el monitoratge de la ubicació mitjançant videovigilància, el control d'accés estricte i el control ambiental (humitat i temperatura) i prevenció contra incendis i inundacions.

PLA DE FORMACIÓ EN CIBERSEGURETAT

El consell comarcal elaborarà, promourà i executarà un Pla de conscienciació anual en ciberseguretat destinat al seu personal considerant especialment les noves incorporacions de persones.

Així mateix, s'informarà clarament al personal de les seves responsabilitats individuals relacionades amb la ciberseguretat.

RESPOSTA A INCIDENTS I CIBERINCIDENTS DE SEGURETAT DEL SISTEMA D'INFORMACIÓ

El Pla de continuïtat del negoci considera l'aspecte de la resposta a incidents i ciberincidents de seguretat al Sistema d'Informació.

En cas de produir-se un ciberincident el consell comarcal ha d'activar l'Equip de Resposta a Ciberincidents (ERC) per aplicar un primer conjunt de mesures de seguretat que permetran la detecció, l'anàlisi i la identificació de l'amenaça.

Posteriorment s'activaran les fases de contenció, mitigació i recuperació del ciberincident.

Per últim, es realitzarà una activitat posterior al ciberincident corresponent a l'emissió d'un Informe del Ciberincident que detallarà la causa original i el cost implicat en termes de compromís de la informació del Sistema d'Informació i d'impacte als serveis que s'haurien d'haver prestat.

La perillositat del ciberincidents serà classificada i tractada segons la Guia de Seguretat de les TIC (CCN-STIC 817) Esquema Nacional de Seguretat. Gestió de ciberincidents. Aquesta correspondrà al nivell 1 per baixa perillositat, nivell 2 o mig, nivell 3 o alt, nivell 4 molt alt o nivell 5 o crític.

Finalment, des de l'inici del ciberincident fins a la seva finalització, i en coordinació amb el departament de Comunicació, es faran aquells comunicats públics que es considerin necessaris. També es considera notificar a altres administracions públiques i tercers aquella informació que sigui legalment pertinent.

CONSIDERACIONS TECNOLÒGIQUES.

Fem esment a que la seguretat total, en qualsevol àmbit, no existeix, i aquest principi de la teoria dels sistemes aplica també a la seguretat de la informació.

A la nostra societat global és conegut que la rapidesa de les comunicacions i la possibilitat d'establir una connexió amb qualsevol equip, que estigui connectat a Internet, facilita en gran mesura una estreta relació de persones i tecnologia on el factor de la distància física passa a ser irrellevant.

La societat digital està a un clic de les administracions públiques i el Consell comarcal del Garraf ha desplegat un seguit de mesures que es recullen en aquest document d'alt nivell, on les consideracions més tècniques es recullen en altres instruments interns com instruccions tècniques i documents específics.

LA CIBERSEGURETAT

L'anàlisi de l'estat de la ciberseguretat de la xarxa TIC del consell comarcal forma part de la cultura de la seguretat i de la protecció de la informació perquè permet conèixer el nivell de risc i el compliment de les mesures de seguretat de la informació, així com les amenaces reals a què està exposat el sistema d'informació.

Aquest anàlisi forma part del Pla Estratègic de Seguretat de la Informació que s'estructura en Plans Anuals de Seguretat de la Informació.

TELECOMUNICACIONS CORPORATIVES

Les telecomunicacions de l'organització han de ser segures per garantir que els intercanvis de dades amb origen o destí el consell comarcal acompleixin els estàndards de seguretat de la informació.

Pel que fa a la comunicació de dades es prendran les mesures necessàries per protegir la xarxa privada del consell comarcal i les xarxes privades virtuals (VPN) mitjançant un sistema de control d'accessos a la xarxa (NAC), sistemes de detecció i prevenció d'intrusions (IDPS), l'ús d'equips tallafocs, el xifratge i la monitorització de les comunicacions i la seguretat de les aplicacions.

En referència a la telefonia mòbil es protegirà l'accés al dispositiu amb el nivell de seguretat adient a l'ús professional que se'n faci.

La redundància dels canals de comunicació s'aconsegueix mitjançant la duplicació dels canals de comunicació. És a dir, una xarxa externa alternativa, contractada amb un Operador diferent al que subministri xarxa principal. De tal manera que, en cas de problema amb

l'operador principal, es disposi d' una contingència immediata. Aquest model és l'actual del consell comarcal a la data de redacció d'aquest document.

LA XARXA INFORMÀTICA.

El consell comarcal del Garraf disposa de dues tipologies de xarxa. La cablejada i la sense fils. Aquestes tipologies s'utilitzen a les dues seus actuals de l'organisme.

Les principals tecnologies associades a la seguretat d'aquestes xarxes són:

- la prevenció de la pèrdua de dades (DLP),
- les solucions de seguretat dels punts finals entesos com a ordinadors, servidors, dispositius mòbils i altres
- Solucions de seguretat web
- La segmentació de xarxes
- Solucions de seguretat al núvol
- L'anàlisi del comportament d'usuaris i entitats (UEBA)

XARXA CABLEJADA.

En relació a aquest document, entenem com a xarxa cablejada aquelles xarxes informàtiques i de comunicacions que utilitzen la interconnexió cablejada entre els diferents dispositius a efectes de permetre la recepció, el tractament i l'enviament d'informació digital.

Les actuacions de seguretat s'adrecen a protegir la disponibilitat dels serveis, i els accessos segurs a la informació, segons una tipologia principal d'elements que, breument, indiquem a continuació:

- Serveis de telecomunicacions
    - Dades
    - Electrònica de telecomunicacions
- Centres de processament de dades (CPD).
- Parc de servidors físics i servidors virtuals en ubicacions locals o remotes.
- Electrònica de xarxa
- Elements de seguretat físics i en programari com tallafocs i altres.
- Parc de components destinats a usuaris de les xarxes
    - Ordinadors de sobretaula
    - Ordinadors portàtils

XARXA SENSE FILS.

Per oposició al cas anterior, la xarxa sense fils serà aquella que connecta els diferents dispositius per mitjà d'ones electromagnètiques per assolir les mateixes finalitats.

En el cas del consell comarcal aquestes són del tipus WLAN (*Wireless Local Area Network*) o també anomenades xarxes wifi que permeten connectar-se a les Intranets i també a Internet.

Una relació, no exhaustiva, dels principals elements que la formen és la següent:

- Serveis de telecomunicacions
    - Dades mòbils
    - Telefonia mòbil
- Parc de servidors virtuals en ubicacions locals o remotes.
- Electrònica de xarxa
- Elements de seguretat físics i en programari com Punts d'Accés (AP), tallafocs i altres.
- Parc de components destinats a usuaris de les xarxes
    - Ordinadors portàtils
    - Tauletes
    - Telèfons mòbils tipus smartphone

A totes dues seus de l'organisme es disposen xarxes wifi privades i xarxes wifi per convidats sense possibilitat d'accés a les Intranets.

Aquests tipus de xarxes són susceptibles a patir atacs dels següents tipus:

- Denegació de Servei (DoS)
- Man in the middle
- Atac per força bruta
- Eavesdropping
- Mac Spoofing

En la mesura del possible, el consell comarcal compta amb dispositius i configuracions de seguretat per eliminar o minimitzar els riscos associats a aquests potencials atacs.

EL PARC DE TELEFONIA MÒBIL

El consell comarcal de Garraf disposa d'un notable Parc de telefonia mòbil degut a la pròpia activitat de l'organisme i al fet de prestar serveis ubicats a diferents municipis de la comarca.

Aquests dispositius es troben protegits per evitar un accés indegut, a més, es disposa d'una gestió àgil que permet bloquejar el dispositiu i la SIM del terminal en cas de pèrdua o robatori.

La gestió de la seguretat d'aquests dispositius necessita d'una permanent revisió i actualització a les últimes tecnologies de seguretat.

LA DISPONIBILITAT DELS SISTEMES TIC

En l' àmbit de tecnologies de la informació i les comunicacions, el concepte de disponibilitat es pot definir com la capacitat d' un servei, conjunt de dades o sistema de ser

operable i accessible en el període de temps determinat en què són requerits. Aquesta operació ha d' estar garantida i per a això, són necessàries mesures i mecanismes que permetin a un sistema o servei mantenir el seu estat d' operativitat i accessibilitat en cas que un esdeveniment amenacés amb inhabilitar-lo.

La disponibilitat és una de les tres dimensions principals de la seguretat d'un sistema d'informació, juntament amb la confidencialitat, que garanteix que la informació només estigui a disposició de sistemes o usuaris autoritzats i la integritat, que garanteix que el seu estat original no ha estat manipulat durant un procés o comunicació.

Es considera com a alta disponibilitat a la capacitat d' un servei, sistema o conjunt de dades de trobar-se operatius per als usuaris en tot moment i sense interrupcions. L'objectiu de l'alta disponibilitat és mantenir els sistemes funcionant 24 hores al dia els 7 dies de la setmana. Generalment aquest tipus de disponibilitat s' estableix per a sistemes de caràcter crític com és el cas dels registres d'entrada i sortida del Consell comarcal.

Segons la guia *CCN-STIC Valoració de sistemes en l'ENS*, és necessari assolir un temps de recuperació (RTO) màxim de quatre hores pels sistemes crítics d'alta disponibilitat, un dia per a sistemes de disponibilitat mitjana i cinc dies per a sistemes de baixa disponibilitat.

MÈTRIQUES

Les principals mètriques per garantir la disponibilitat són les següents:

- El MTTF *(Mean Time to Failure)* que és la mesura que estima el temps entre fallides en els sistemes durant la seva operació normal.
- El MTTR *(Mean Time Reecovery)* que mesura el temps mig en que un sistema es restableix a una situació de normalitat després d'una fallida.
- El RTO *(Recovery Time Objetive)* és el temps de recuperació on el sistema no podrà operar fins a la seva restauració.
- El MTD *(Maximum Tolerable Downtimwe)* és el temps que un procés o sistema pot estar caigut abans que es produeixin conseqüències crítiques.
- El ROL *(Revised Point Objetive)* és el nivell mínim d'operació que ha de tenir una activitat per considerar-la recuperada.
- El RPO *(Recovery Point Objetive)* que es correspon amb l'impacte que té sobre l'activitat la pèrdua de dades.

Aquests valors es prendran en consideració en el disseny dels sistemes d'informació, la seva gestió i manteniment, així com en els procediments de contractació TIC.

Els diferents nivells de disponibilitat, en el període d'un any, adequats als serveis que són competència del consell comarcal són els següents:

- 99,99 %, equivalent a 53 minuts o 0,88 hores de sistema inactiu
- 99,9% que corresponen a 526 minuts o 8.77 hores
- 99,5% o 2.628 minuts; 43,8 hores
- 99% o 5.256 minuts; 87,6 hores

AMENACES CONTRA LA DISPONIBILITAT

Les principals amenaces contra la disponibilitat poden ser les interrupcions previstes i imprevistes, fallides del maquinari, fallida del programari, amenaces físiques i amenaces lògiques.

Contra totes aquestes amenaces s'ha de preveure actuacions per garantir la disponibilitat pel disseny dels sistemes, garantint una protecció física i lògica, i un manteniment i actualització permanent del maquinari i del programari.

VIRTUALITZACIÓ

La virtualització de màquines i sistemes pot ajudar a aconseguir un alt grau de disponibilitat perquè, en cas de fallida, es poden recuperar en un curt període de temps, permetent tornar a un estat previ del servidor.

Aquests servidor disposen d'una major escalabilitat, estalviant el procés de renovació de maquinari físic i faciliten una més fàcil redundància de sistemes.

Actualment el consell comarcal disposa d'un Parc de servidors virtuals amb les suficients garanties de seguretat dels serveis i de la informació que allotgen.

SISTEMES D' EMMAGATZEMATGE

El sistema d'Informació del consell comarcal disposen de diversos sistemes d'emmagatzemament de dades. Els principals són sistemes RAID 5 *(Redundant Array of Independent Disks)* i NAS *(Network Attached storage)*. També s'utilitzen serveis de còpies de seguretat al núvol *(Cloud)*.

SISTEMES CLOUD

L'ús de sistemes en entorns cloud ajuda a millorar la disponibilitat dels serveis i de les dades. És important l'acord d'un SLA *(Service Level Agreement)* adequat al sistema d'informació, així com garantir la confidencialitat de les dades i exigir el xifratge en cas de dades de confidencials, sensibles o de caràcter personal.

SEGURETAT FÍSICA I AMBIENTAL DELS SISTEMES TIC

El consell comarcal disposa de sistemes de protecció de la informació front a desastres naturals, inundacions o altres problemes previsibles que es puguin donar a les seus de la institució.

CENTRE DE PROCESSAMENT DE DADES (CPD)

El consell comarcal disposa de dos Centres de processament de dades (CPD) que són sales condicionades que allotgen els servidors i les xarxes de comunicacions necessàries per l'operació de l'organització incloent els sistemes SAI (Sistemes d'Alimentació Ininterrompuda). Han de disposar de monitorització per videovigilància, control d'accés estricte, control ambiental i prevenció contra incendis i inundacions.

PROTECCIÓ DE L'ENTORN FÍSIC

Les mesures més importants de protecció de l'entorn físic són el control de l'accés físic, els sistemes d'alimentació ininterrompuda (SAI) i les fonts d'alimentació redundants. En aquest cas el consell comarcal disposa de les dues primeres, fet que permet garantir un temps suficient per a la terminació ordenada dels processos i la desconnexió dels servidors en cas d'esgotar-se el temps de subministrament d'energia de les fonts addicionals a la prinicpal.

SEGURETAT LÒGICA

AUDITORIA DE SEGURETAT DELS SISTEMES

Les auditories de seguretat i de ciberseguretat dels sistemes abasten l' anàlisi i la gestió dels sistemes per identificar i corregir possibles vulnerabilitats. Els objectius de l' auditoria de seguretat són verificar la seguretat d'entorns i sistemes, l'acompliment amb legislacions i normatives i la realització d'un informe que orienti en el procés de millor continua.

El consell comarcal disposa d'auditories de ciberseguretat, tant externes com internes, que es programen de forma periòdica.

PROTECCIÓ CONTRA ATACS

En l' actualitat s'han incrementat notablement el nombre d'atacs i ciberatacs als equips, sistemes i xarxes que poden generar una degradació dels serveis.

Per protegir l'organització contra aquests atacs el consell comarcal disposa de diferents eines i salvaguardes com són els dispositius de protecció de perímetre (tallafocs i servidors proxy); els sistemes de detecció d'intrusions (IDS) i sistemes de prevenció d'intrusions (IPS); també es protegeixen les comunicacions mitjançant xarxes privades virtuals (VPN); es disposa també de software antimalware *(Endpoint Protection Platform (EPP) i Endpoint Detecció i Resposta (EDR))*; s'aplica un estricta polítiques de contrasenyes així com un control d'accés als equips i comptes d'usuari.

CÒPIES DE SEGURETAT I PROVES DE RESTAURACIÓ.

Les còpies de seguretat són una eina cabdal per garantir la disponibilitat dels serveis i de les dades del consell comarcal sota qualsevol circumstància previsible. Aquestes abasten tota la informació necessària per recuperar el servei en cas de pèrdua d'informació com són les dades, els programes, els fitxers de configuració i la imatge del sistema operatiu.

Per definir i estructurar la forma de realitzar aquestes còpies de seguretat es disposa d'una Política de Còpies de Seguretat en l' organització. Aquesta inclou, per a tots els sistemes crítics, la informació següent:

- Periodicitat de les còpies de suport.
- Períodes de retenció de les còpies.
- Ubicació dels suports de les còpies, tant en la ubicació pròpia i en ubicacions remotes.
- Controls per a l'accés autoritzat a les còpies de suport.
- Procediments de recuperació de la informació.
- Procediments de restauració i verificació de la integritat de la informació recolzada.
- Procediments d'inventari i gestió de suports.

S'hauran de realitzar proves periòdiques de restauració per verificar el correcte funcionament dels procediments de recuperació de còpies de seguretat. Tant les proves com els resultats es documentaran, permetent així l' esmena de qualsevol incidència que pogués succeir.

En els casos en els quals els fitxers continguin dades de caràcter personal, el responsable del fitxer haurà de verificar semestralment la correcta definició, funcionament i l' aplicació dels procediments de realització de còpies de suport i recuperació.

SISTEMES D'ALTA DISPONIBILITAT

Considerem l'alta disponibilitat a la capacitat d'un servei, sistema o conjunt de dades de ser operatius per als usuaris en tot moment i sense interrupcions. L'objectiu de l'alta disponibilitat és mantenir funcionant el sistemes les 24 h del dia els 7 dies de la setmana.

Són sistemes crítics al consell comarcal:

- El Registre d'entrades
- El Registre de sortides
- El gestor d'expedients
- Les comunicacions dels servidors crítics

Segons la guia CNN-STIC-803 Valoració de sistemes en l'ENS, el temps de recuperació (RTO) per aquests sistemes ha de ser inferior a quatre hores.

Altres sistemes que també es consideren crítics però que no es recullen a l'anterior guia són les comunicacions dels sistemes d'alarmes de pànic, d'intrusió i antiincendis.

ELS REGISTRES D'ENTRADA I DE SORTIDA

El Registre d'entrada i el Registre de sortida del consell comarcal està integrat al Sistema de Gestor d'Expedients (SGE).

Els assentaments realitzats als registres de forma presencial requereixen únicament de la disponibilitat dels serveis interns del SGE i del servei d'escaneig certificat. Així mateix és necessari el funcionament del servei extern de validació de certificats digitals PSIS del Consorci AOC.

Els assentaments telemàtics requereixen dels serveis interns del SGE i del servei d'escaneig certificat. Si per alguna incidència tecnològica al consell comarcal el sistema de registres del SGE no estigués disponible, el registre de l'EACAT actuarà com a registre auxiliar. Aquests assentament del registre auxiliar s'incorporaran posteriorment al sistema de registres del SGE quan aquest torni a ser operatiu.

Així mateix, els assentaments telemàtics poden requerir de la disponibilitat d'altres serveis externs del Consorci AOC com són: MUX, Vàlid, PSIS, eNotum, eFact, eTRAM, eTauler, Seu-e, Via Oberta, RPC, PSCP i Representa.

EL GESTOR D'EXPEDIENTS

Prenent en consideració el procediment administratiu, el Sistema de Gestió d'Expedients (SGE) permet donar compliment a la normativa vigent.

Els mòduls del SGE de criticitat superior són els de Registre d'entrades i el de Registre de sortides. Ara bé, sent aquest dos sistemes els que permeten l'inici dels expedients a instància de part o la terminació convencional per notificació de la resolució, també és necessari i crític que el personal tramitador dels expedients pugui continuar amb la seva normal activitat d'ordenació i instrucció dels expedients per garantir els terminis legals dels diferents procediments administratius. Així doncs, el SGE també es considera crític.

EQUIPS INFORMÀTICS

El consell comarcal del Garraf disposa d'un parc de 125 equips destinats als usuaris i a les usuàries del Sistema d'Informació. Aquests equips estan protegits per soluciones de seguretat destinades a equips finals *("end points"*) i es disposa d'un sistema centralitzat de supervisió del conjunt dels equips (EDR), del seu estat, de les actualitzacions de firmware i dels programaris autoritzats.

Existeix i es fa una actualització de la relació de dispositius autoritzats a operar dins dels Sistema d'Informació. En espais i sales destinades a reunions amb personal extern es permet la connexió d'altres equips a xarxes wifi de convidats.

EL PROGRAMARI

El programari a instal·lar als equips ha de ser prèvia autoritzat i dona't d'alta al sistema de control de programari. Els usuaris i les usuàries dels equips informàtics no disposen del rol administrador per a instal·lar nou programari. Aquesta instal·lació es fa per personal amb rol d'administrador d'equips informàtics.

ELS SERVEIS I EL PROGRAMARI AL NÚVOL TECNOLÒGIC

L'entorn del núvol (Cloud) ajuda a millorar la disponibilitat, tant dels serveis com les dades.

L'emmagatzematge de dades i còpies de seguretat al núvol proporciona un grau addicional de disponibilitat, però ha d'anar acompanyat d'Acords a Nivell de Servei (SLA) adequats i s'haurà de prestar especial atenció a la confidencialitat de les dades. Es podria requerir, per tant, que les dades s' emmagatzemen xifrades, en cas que siguin confidencials, sensibles o de caràcter personal.

L'ús de serveis Cloud també permet més disponibilitat a causa de la facilitat de desplegament, ampliació de recursos i tolerància a fallades dels entorns. D' igual manera, s'ha de prestar especial atenció durant la definició dels SLA, per determinar de forma clara i precisa els nivells de disponibilitat i seguretat necessaris.

Actualment es disposa de còpies de seguretat al núvol del sistema de gestor d'expedients.

També es fa ús del núvol amb els serveis de Google i de Microsoft Office, així com de varis allotjaments web.

SEGURETAT DE LA INFORMACIÓ DE SERVEIS TECNOLÒGICS DELEGATS

El consell comarcal del Garraf opera serveis tecnològics digitals delegats segons diferents convenis amb el Consorci AOC. Aquests serveis disposen d'un Responsable que vetlla pel bon funcionament del sistema i per la seva seguretat segons els requisits propis del consell comarcal com els del Consorci AOC.

Els serveis són els d'Entitat de Registre TCAT i el d'Entitat de Registre IDCAT i ambdós estan vinculats a l'Oficina Comarcal de Suport a l'Administració Electrònica (OCSAE).

Així mateix, es disposa de l'Ens Subscriptor TCAT pel consum de certificats digitals amb destinació al propi consell comarcal.

ENTITAT DE REGISTRE TCAT

L'Entitat de Registre TCAT (ERTCAT) correspon al servei d'emissió de certificats digitals destinats al personal, als aplicatius i als sistemes dels organismes públics de la comarca del Garraf.

Per l'ERTCAT se segueixen els protocols del Consorci AOC anomenats: Procediment de seguretat de les Entitats de Registre i Procediment d'arxiu de les Entitats de Registre. Aquests protocols són d'obligat compliment i s'avaluen en auditories externes periòdiques.

ENTITAT DE REGISTRE IDCAT

L'Entitat de Registre idCAT (ERidCAT) correspon al servei d'emissió de certificats digitals destinats a la ciutadania de la comarca del Garraf, encara que és possible emetre certificats digitals idCAT per persones empadronades a municipis d'altres comarques catalanes.

Per l'ERTCAT se segueixen els protocols del Consorci AOC anomenats: Procediment de seguretat de les Entitats de Registre i Procediment d'arxiu de les Entitats de Registre. Aquests protocols són d'obligat compliment i s'avaluen en auditories externes periòdiques.

ENS SUBSCRIPTOR TCAT

Com a administració pública local, el consell comarcal també sol·licita certificats digitals pel personal, els aplicatius i pels sistemes propis.

Per l'Ens subscriptor s'adopten els processos descrits al Procediment de seguretat dels Ens Subscriptors i al Procediment d'arxiu dels Ens Subscriptors del Consorci AOC. Aquests protocols són d'obligat compliment i s'avaluen en auditories externes periòdiques.

INTEROPERABILITAT TECNOLÒGICA

CONSUM DE SERVEIS TECNOLÒGICS DE LES ADMINISTRACIONS PÚBLIQUES

La seguretat de la informació de les plataformes tecnològiques d'altres administracions públiques interconnectades amb el consell comarcal depèn de l'organisme que ofereix el servei tecnològic.

Les dades i informació obtingudes d'aquests serveis externs han de ser custodiades administrativament per la unitat orgànica, o àrea organitzativa del consell comarcal, i aquesta ha d'informar al Servei TIC del nivell d'accés i seguretat que han d'aplicar a les dades i documents interoperables.

Les consultes interoperables de dades de tercers en poder d'altres administracions públiques han de ser guardades en el corresponent expedient que va originar la consulta.

AUDITORIES.

El Sistema d'Informació (SI) del consell comarcal del Garraf se sotmet a diverses auditories de seguretat tant en relació a la ciberseguretat, com als serveis delegats pel Consorci AOC, com pels serveis d'interoperabilitat.

AUDITORIES EN CIBERSEGURETAT

Anualment es realitza una auditoria interna per supervisar el grau de compliment amb l'Esquema Nacional de Seguretat (ENS). Per la seva realització es considera la possible modificació de normativa des d'última auditoria interna, les recomanacions fetes per les auditories externes, i els informes de ciberseguretat produïts pels Serveis TIC.

Periòdicament el Sistema d'Informació s'audita mitjançant una empresa externa amb la suficient acreditació per realitzar-la.

Les actuacions a realitzar segons les conclusions i les recomanacions de totes dues auditories s'incorporen al corresponent Pla anual TIC.

AUDITORIES EXTERNES DE SERVEIS TIC DELEGATS I DE SERVEIS INTEROPERABLES

El Sistema d'Informació del consell comarcal és auditat pel Consorci AOC pel servei d'Entitat de Registre TCAT, el servei d'Entitat de Registre idCAT, l'Ens subscriptor TCAT i pel servei d'Interoperabilitat Via Oberta.

Les conclusions i recomanacions de les auditories s'apliquen al Sistema d'Informació en un procés de millora continuada.

FONTS D'INFORMACIÓ

- CCN-TEC 010, La disponibilidad de los sistemas TIC
- Guía de Seguridad de las TIC (CCN-STIC-803). Valoración de sistemas en el ENS
- Guía de Seguridad de las TIC (CCN-STIC-804). ENS. Guía implantación.
- Guía de Seguridad de las TIC (CCN-STIC-805). Esquema Nacional de Seguridad. Política de Seguridad de la Información.
- Guía de Seguridad de las TIC (CCN-STIC 817). Esquema Nacional de Seguridad. Gestión de ciberincidentes
- Guía de Seguridad de la TIC (CCN-STIC-402). Organización y gestión de la Seguridad de los sistemas TIC.