Expedient: 4316520002-2021-0000066
Òrgan competent: Alcalde

DECRET

Aprovació del Pla d'adequació a l'Esquema Nacional de Seguretat

Fets

L'Ajuntament de Vilabella utilitza els mitjans que en cada moment posen a la seva disposició les Tecnologies de la Informació i de les Comunicacions (TIC) per assolir els seus objectius.

Els sistemes TIC han d'estar protegits contra amenaces accidentals o deliberades amb potencial per incidir en la confidencialitat, integritat, disponibilitat, autenticitat o traçabilitat 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 els òrgans superiors i directius responsables de la informació, els sistemes i els serveis electrònics han d'aplicar les mesures mínimes de seguretat exigides pel Reial Decret 3/2010, de 8 de gener, que regula l'Esquema Nacional de Seguretat (en endavant , ENS) en l'àmbit de l'Administració Electrònica, modificat mitjançant Reial Decret 951/2015, de 23 d'octubre, així com realitzar 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. Els diferents òrgans superiors i directius responsables han de garantir la seguretat TIC com una part integral de cada etapa del cicle de vida del sistema, des de la seva concepció fins a la retirada de servei, passant per les decisions de desenvolupament o adquisició i les activitats d'explotació.

Els requisits de seguretat i el seu finançament han de ser identificats i inclosos en la planificació, en la sol·licitud d'ofertes, i en plecs de licitació per a projectes de TIC.

Segons l'article 7 de Reial Decret regulador de l'ENS, la seguretat de la informació ha de contemplar els aspectes de prevenció, detecció, reacció,

correcció i recuperació per aconseguir que les amenaces sobre la mateixa no es materialitzin i no afectin els serveis que es presten.

L'Ajuntament de Vilabella, considera necessari realitzar **el Pla d'Adequació** per dur a terme el procés d'implantació de l'ENS, motiu pel qual s'ha elaborat el següent document (ANNEX), que s'estructura en els apartats que s'indiquen a continuació:
- Política de seguretat (ANNEX 1)
- Categorització del sistema de l'Ajuntament de Vilabella (ANNEX 2).
- Anàlisi de riscos (ANNEX 3).
- Declaració d'Aplicabilitat (ANNEX 4).
- Informe d'insuficiències ENS (ANNEX 5).
- Pla de millora de seguretat (ANNEX 6).

Fonaments de dret

La "*Disposició transitòria. Adequació de sistemes* "de 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, establia:
1. Els sistemes existents a l'entrada en vigor d'aquest Reial decret s'han d'adequar a l'Esquema Nacional de Seguretat de manera que permetin el compliment del que estableix la disposició final tercera de la Llei 11/2007, de 22 de juny. Els nous sistemes d'aplicar el que estableix el present Reial decret des de la seva concepció.
2. Si als dotze mesos de l'entrada en vigor de l'Esquema Nacional de Seguretat hagués circumstàncies que impedeixin la plena aplicació del que exigeix __el mateix, **es disposarà d'un pla d'adequació que marqui els terminis d'execució** dels quals, en cap cas , seran superiors a 48 mesos des de l'entrada en vigor.
El pla indicat en el paràgraf anterior s'ha d'elaborar amb l'antelació suficient i aprovat pels òrgans superiors competents.
3. Mentre no s'hagi aprovat una política de seguretat per l'òrgan superior competent s'aplicaran les polítiques de seguretat que puguin existir a nivell d'òrgan directiu.
Termini que va vèncer al gener de 2014
Posteriorment, el Reial Decret 951/2015, de 23 d'octubre, de modificació de 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, va establir un nou termini per a la implantació de les noves mesures, recollit també en el seu "Disposició transitòria única. Adequació de sistemes ".

Les entitats incloses dins en l'àmbit d'aplicació d'aquest Reial decret disposen d'un termini de vint mesos comptats a partir de la data de l'entrada en vigor d'aquest Reial decret, per l'adequació dels seus sistemes al que disposa el mateix.
Termini que va vèncer al novembre de 2017.

En conseqüència, RESOLC:

PRIMER.- Aprovar el Pla d'adequació a l'Esquema Nacional de Seguretat.

SEGON.- Els criteris i instruccions contingudes en el document que s'aprova mitjançant la present resolució constitueixen directrius vinculants per a tots els òrgans superiors i directius de l' Ajuntament de Vilabella. Tanmateix ho serà per a terceres parts a les quals l'Ajuntament presti serveis, cedeixi informació o de les que n'utilitzi serveis o manipuli informació. L'Ajuntament mantindrà a la seu electrònica la versió actualitzada del document de Política de seguretat de la informació.

Règim de recursos:

Si es vol impugnar la present resolució, que posa fi a la via administrativa, procedeix interposar recurs contenciós administratiu davant el Jutjat Contenciós Administratiu de Tarragona, en el termini de dos mesos a comptar de l'endemà de la seva notificació.

Alternativament i de forma potestativa, es pot interposar recurs de reposició davant el mateix òrgan que l'ha dictat, en el termini d'un mes a comptar de l'endemà de la seva notificació.

L'Alcalde.
Joan Maria Sanahuja Segú

SEGURdades

Consultors en protecció de dades personals

Pla d'Adequació a l'ENS
Ajuntament de Vilabella

Ajuntament de Vilabella

PLA D'ADEQUACIÓ A L'ENS

ÍNDEX

CONTROL DEL DOCUMENT

Nom del document**: Pla Adequació - Vilabella** Nombre de Pàgines: **4**	
Autor: SEGURdades – Jordi Vidal	Revisat per:
Data:	Data:
Aprovat per: Decret d'alcaldia de dada 18 de febrer de 2021	
Classificació de la Informació: **CONFIDENCIAL**	
Llista de Distribució: COMITÈ STIC	

1 APROVACIÓ I ENTRADA EN VIGOR

Text aprovat el dia 18 de febrer de 2021 per resolució de l'Alcaldia de l'Ajuntament de Vilabella.

2 INTRODUCCIÓ

FUNDAMENTS JURÍDICS

La "*Disposició transitòria. Adequació de sistemes* "de 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, establia:

1. Els sistemes existents a l'entrada en vigor d'aquest Reial decret s'han d'adequar a l'Esquema Nacional de Seguretat de manera que permetin el compliment del que estableix la disposició final tercera de la Llei 11/2007, de 22 de juny. Els nous sistemes d'aplicar el que estableix el present Reial decret des de la seva concepció.

2. Si als dotze mesos de l'entrada en vigor de l'Esquema Nacional de Seguretat hagués circumstàncies que impedeixin la plena aplicació del que exigeix el mateix, **es disposarà d'un pla d'adequació que marqui els terminis d'execució** dels quals, en cap cas , seran superiors a 48 mesos des de l'entrada en vigor.

El pla indicat en el paràgraf anterior s'ha d'elaborar amb l'antelació suficient i aprovat pels òrgans superiors competents.

3. Mentre no s'hagi aprovat una política de seguretat per l'òrgan superior competent s'aplicaran les polítiques de seguretat que puguin existir a nivell d'òrgan directiu.

Termini que va vèncer al gener de 2014

Posteriorment, el Reial Decret 951/2015, de 23 d'octubre, de modificació de 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, va establir un nou termini per a la implantació de les noves mesures, recollit també en el seu "Disposició transitòria única. Adequació de sistemes ".

Les entitats incloses dins en l'àmbit d'aplicació d'aquest Reial decret disposen d'un termini de vint mesos comptats a partir de la data de l'entrada en vigor d'aquest Reial decret, per l'adequació dels seus sistemes al que disposa el mateix.

Termini que va vèncer al novembre de 2017.

CONCLUSIONS

L'Ajuntament de Vilabella, considera que la necessitat de realitzar **el Pla d'Adequació segueix mantenint-se vigent i que, a més, ho considera necessari per dur a terme el procés d'implantació de l'ENS**, motiu pel qual s'ha elaborat el següent document, que es s'estructura en els apartats que s'indiquen a continuació.

3 POLÍTICA DE SEGURETAT

L'Ajuntament de Vilabella, disposa d'una Política de Seguretat aprovada l'1de desembre de 2020. Aquesta Política de Seguretat ha estat desenvolupada tenint en compte els principis bàsics i en base als requisits mínims de seguretat establerts per la normativa de l'ENS i d'acord amb el que exigeix l'Annex II de Reial Decret ENS, contemplant els requisits exigits en la secció [org. 1].

A l'**Annex I**, de el present document, s'adjunta la **Política de Seguretat** juntament amb el document de designació de rols de seguretat i de constitució del Comitè de Seguretat.

Al Pla de Millora de la Seguretat (**Annex VI**) es detalla com es planeja adaptar la política a les exigències de l'Annex II de Reial Decret ENS.

4 CATEGORIZACIÓ DEL SISTEMA

En l'Annex II, de el present document, s'adjunta la **Categorització de el Sistema** de l'Ajuntament de Vilabella composta per **l'Inventari i Valoració dels Serveis i de la Informació associada als mateixos**, juntament amb la seva justificació, i la **categorització de el sistema**, segons el que estableix l'annex I de Reial Decret 3/2010.

5 ANÀLISI DE RISCOS

L'Ajuntament de Vilabella ha realitzat un Anàlisi de Riscos, segons el que estableix l'Annex II de Reial Decret en la seva secció [op.pl.1], d'acord amb el que estableix el Perfil de Compliment Específic d'aplicació a Ajuntaments de menys de 20.000 habitants del CCN-CERT.

En **l'Annex III**, de el present document, s'adjunta **l'informe d'Anàlisi de Riscos i acceptació de riscos residuals**. L'anàlisi de riscos ha estat realitzat utilitzant la metodologia MAGERIT en la seva versió 3.0 (MAGERIT és la metodologia d'anàlisi i gestió de riscos elaborada pel Consell Superior d'Administració Electrònica).

6 DECLARACIÓ D'APLICABILITAT

A **l'Annex IV**, del present document, s'adjunta la **Declaració de Aplicabilitat** de l'Ajuntament de Vilabella acord amb el que estableix el Perfil de Compliment Específic d'aplicació a Ajuntaments de menys de 20.000 habitants del CCN-CERT.

7 INFORME D'INSUFICIÈNCIES

A L'**Annex V,** del present document, s'adjunta l'**Informe d'insuficiències** de l'Ajuntament de Vilabella.

8 PLA DE MILLORA DE LA SEGURETAT

A l'**Annex VI**, del present document, s'adjunta el Pla de Millora de la Seguretat de l'Ajuntament de Vilabella, que conté les accions necessàries per a esmenar les mancances detectades en el sistema, i que es troben recollides en **l'informe d'insuficiències** de l'**Annex V**, també inclòs en aquest annex.

SEGURdades

Consultors en protecció de dades personals

Política de Seguretat

Ajuntament de Vilabella

CONTROL DEL DOCUMENT

Nom del document**:** PS001 - Politica de Seguretat Vilabella.docx Nombre de pàgines: 10	
Autor: responsable de seguretat	Revisat per:
Data:	Data:
Aprovat per:	
Classificació de la informació: **SENSE RESTRICCIONS**	
Llista de Distribució: PERSONAL INTERN I EXTERN DE L'AJUNTAMENT DE VILABELLA	

CONTROL DE VERSIONS

Nº Versió	Autor	Data	Canvis realitzats	Comentaris
1.0	Jordi Vidal. Segurdades SL	29/09/2020	Versió inicial	Revisat per els consultors jurídics de SEGURdades
2.0	Miquel de Haro Responsable TIC CC Alt Camp	23/11/2020	Revisió	

1. APROVACIÓ I ENTRADA EN VIGOR

Text aprovat el dia 1 de desembre de 2020 pel Ple de l'Ajuntament de Vilabella.
Aquesta Política de seguretat de la informació és efectiva des d'aquesta data i fins que sigui reemplaçada per una nova Política.

2. INTRODUCCIÓ

L'Ajuntament de Vilabella depèn dels sistemes TIC (Tecnologies d'Informació i Comunicacions) per assolir 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 la disponibilitat, integritat o confidencialitat de la informació tractada i/o els serveis prestats.
L'objectiu de la seguretat de la informació és garantir la qualitat de la informació i la prestació continuada dels serveis, actuant preventivament, supervisant l'activitat diària i reaccionant amb rapidesa enfront incidents.
Els sistemes TIC han d'estar protegits contra amenaces de ràpida evolució amb potencial per incidir sobre la confidencialitat, integritat, disponibilitat i valor de la informació així com dels 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. Aquesta implica que els departaments han d'aplicar les mesures mínimes de seguretat exigides per l'Esquema Nacional de Seguretat, així com realitzar un seguiment continu dels nivells de prestació de serveis mitjançant l'anàlisi de vulnerabilitats reportades i la preparació d'una resposta efectiva als incidents per tal de poder garantir la continuïtat dels serveis prestats.
Els diferents departaments han d'assegurar-se que el paper de la seguretat TIC sigui una part integral de cada etapa del cicle de vida del sistema: des de la seva concepció fins a la retirada de servei passant per les decisions relatives al desenvolupament, adquisició i l'explotació d'activitats.
Els requisits de seguretat i les necessitats de finançament han de ser identificats i inclosos en la planificació, la sol·licitud d'ofertes, i als plecs de licitació per a projectes de TIC.
Els departaments han d'estar preparats per prevenir, detectar, reaccionar i recuperar-se d'incidents, d'acord amb l'article 7 de l'ENS.

3. ABAST

La Política de seguretat de l'Ajuntament de Vilabella és d'obligat compliment per a tots els membres i sistemes TIC de l'Ajuntament sense excepcions.

4. MISSIÓ

L'Ajuntament de Vilabella té com a principal missió impulsar la qualitat de vida al municipi a través de la millora en la prestació dels serveis per aconseguir una major sostenibilitat, participació i integració, tant social com territorialment i, conseqüentment, una major eficiència en la gestió dels recursos.

5. MARC NORMATIU

Per a l'execució de la present política s'ha tingut en compte la legislació que afecta el sistema d'informació objecte d'aquest document, que és:

- 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.
- Reial Decret 3/2010, de 8 de gener, pel qual es regula l'Esquema Nacional de Seguretat en l'àmbit de l'administració electrònica, modificat pel Reial Decret 951/2015, de 23 d'octubre.

- Resolució de 13 d'octubre de 2016, de la Secretaria d'Estat d'Administracions Públiques, per la qual s'aprova la Instrucció tècnica de seguretat de conformitat amb l'Esquema Nacional de Seguretat.
- Resolució de 7 d'octubre de 2016, de la Secretaria d'Estat d'Administracions Públiques, per la qual s'aprova la Instrucció Tècnica de Seguretat de Informe de l'Estat de la Seguretat.
- Resolució de 27 de març de 2018, de la Secretaria d'Estat de Funció Pública, per la qual s'aprova la Instrucció tècnica de seguretat d'auditoria de la seguretat dels sistemes d'informació.
- Resolució de 13 d'abril de 2018, de la Secretaria d'Estat de Funció Pública, per la qual s'aprova la Instrucció tècnica de seguretat de notificació d'incidents de seguretat.
- 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 1671/2009, de 6 de novembre, pel qual es desenvolupa parcialment la Llei 11/2007, de 22 de juny, d'accés electrònic dels ciutadans als serveis públics.
- Reglament (UE) 2016/679 del Parlament Europeu i de Consell, de 27 d'abril de 2016, relatiu a la protecció de les persones físiques pel que fa a el 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, RGPD).
- Llei Orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia de drets digitals.
- Articles 23 i 24 de la Llei Orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal (Disposició Transitòria Quarta de la Llei Orgànica 3/2018 de protecció de dades i garantia drets digitals)
- Llei 34/2002, de 11 de juliol, de serveis de la societat de la informació i de comerç electrònic.
- Llei 37/2007, de 16 de novembre, sobre reutilització de la informació del sector públic.
- Llei 19/2014, de 29 de desembre, de transparència, accés a la informació pública i bon govern.
- Llei 25/2007, de 18 d'octubre, de conservació de dades relatives a les comunicacions electròniques i a les xarxes públiques de comunicacions.
- Llei 56/2007, de 28 de desembre, de mesures d'impuls de la societat de la informació.
- Llei 9/2014, de 9 de maig, general de telecomunicacions.
- Llei 7/1985, de 2 d'abril, reguladora de les bases de règim local, modificada per la llei 11/1999, de 21 d'abril.
- Reial Decret Legislatiu 1/1996, de 12 d'abril, pel qual s'aprova el text refós de la Llei de propietat intel·lectual.
- Reial Decret Legislatiu 5/2015, de 30 d'octubre, pel qual s'aprova el text refós de la Llei de l'estatut bàsic de l'empleat públic.
- Llei 59/2003, de 19 de desembre, de signatura electrònica.
- Reial Decret 1553/2005, de 23 de desembre, pel qual es regula el document nacional d'identitat i els seus certificats de signatura electrònica.
- 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.
- 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.

6. OBJECTIUS

L'Ajuntament de Vilabella, per aconseguir el compliment dels articles del Reial Decret 3/2010, de 8 de gener, pel qual es regula l'Esquema Nacional de Seguretat en l'àmbit de l'administració electrònica, ha establert els següents principis bàsics i requisits mínims de seguretat:

6.1 - PREVENCIÓ

Els departaments han d'evitar, o almenys prevenir en la mesura del possible, que la informació o els serveis es vegin perjudicats per incidents de seguretat. Per a això els departaments han d'implementar les mesures mínimes de seguretat determinades per l'ENS, així com qualsevol control addicional identificat a través d'una avaluació d'amenaces i riscos. Aquests controls, i els rols i responsabilitats de seguretat de tot el personal, han d'estar clarament definits i documentats.
Per garantir el compliment de la política, els departaments han de:

- Autoritzar els sistemes abans d'entrar en operació.
- Avaluar regularment la seguretat, incloent avaluacions dels canvis de configuració realitzats de forma rutinària.
- Sol·licitar la revisió periòdica per part de tercers amb la finalitat d'obtenir una avaluació independent.

6.2 - DETECCIÓ

Atès que els serveis es poden degradar ràpidament a causa d'incidents, que van des d'una simple desacceleració fins a la seva detenció, els serveis han de monitoritzar l'operació de manera contínua per detectar anomalies en els nivells de prestació dels serveis i actuar en conseqüència segons el que estableix l'article 9 de l'ENS.
El monitoratge és especialment rellevant quan s'estableixen línies de defensa d'acord amb l'article 8 de l'ENS. S'estabiran mecanismes de detecció, anàlisi i informe que arribin als responsables regularment i quan es produeix una desviació significativa dels paràmetres que s'hagin preestablert com a normals.

6.3 - RESPOSTA

Els departaments han de:

- Establir mecanismes per respondre eficaçment als incidents de seguretat.
- Designar punt de contacte per a les comunicacions pel que fa a incidents detectats en altres departaments o en altres organismes.
- Establir protocols per a l'intercanvi d'informació relacionada amb l'incident. Això inclou comunicacions, en ambdós sentits, amb els Equips de Resposta a Emergències (CERT).

6.4 - RECUPERACIÓ

Per garantir la disponibilitat dels serveis crítics, els departaments han de desenvolupar plans de continuïtat dels sistemes TIC com a part del seu pla general de continuïtat de negoci i activitats de recuperació.

7. DADES PERSONALS

L'Ajuntament de Vilabella ha de donar compliment a la normativa de protecció de dades, des de la seva condició de responsable de tractament o com a encarregat de tractament vers les dades a les que pot accedir, visionar i tractar dels ciutadans en el marc de la prestació de serveis que realitzen.
Per aquest motiu ha de disposar d'un registre d'activitats actualitzat i s'ha de realitzar regularment un anàlisi de riscos dels tractaments de dades que es poden executar així com les pertinents avaluacions d'impacte sobre les dades personals.
L'Ajuntament, per donar compliment a les obligacions reglamentaries i legals, ha d'aplicar les mesures tècniques i organitzatives necessàries per realitzar un tractament de dades donant compliment a les notes de confidencialitat, disponibilitat i integritat exigida per la normativa de protecció de dades i en el marc de la seva responsabilitat proactiva.

8. COMPROMÍS DE LA DIRECCIÓ

L'alcaldia de l'ajuntament de Vilabella expressa el seu compromís total amb la present Política de Seguretat, mantenint les directrius fixades en el present document i proporcionant els recursos necessaris per a complir els objectius establerts. Així mateix, ha de publicar i lliurarà a tots els empleats i contractistes el present document, perquè tots coneguin els objectius establerts per la

direcció, les polítiques, principis i normes adoptades i la seva importància per a la seguretat de l'organització, les responsabilitats generals i específiques en matèria de seguretat i altres referències per a la documentació que puguin ser útils.

9. ORGANITZACIÓ DE LA SEGURETAT

L'organització de la seguretat de la informació de l'Ajuntament de Vilabella s'estableix en la forma que s'indica a continuació.

9.1 - ROLS O PERFILS DE SEGURETAT

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

- Responsable de la Informació i Serveis
- Responsable de la Seguretat

9.2 - COMITÈ DE SEGURETAT TIC

A l'Ajuntament de Vilabella, s'ha constituït un Comitè de Seguretat de la Informació, com a òrgan col·legiat, i està format pels següents membres:

- L'Alcalde de Vilabella.
- La Secretària Interventora.
- Responsable TIC del Consell Comarcal de l'Alt Camp

El president del Comitè STIC serà l'Alcalde de l'Ajuntament.
El Secretari del Comitè STIC serà el Responsable de Seguretat de l'Ajuntament i tindrà com a funcions:

- Convocar per ordre del president les reunions del Comitè de Seguretat de la Informació.
- Preparar els temes a tractar en les reunions del Comitè, aportant informació puntual per a la presa de decisions.
- Elaborar l'acta de les reunions.

Amb caràcter opcional, altres membres de l'Ajuntament de Vilabella podran incorporar-se a les tasques del Comitè, inclosos grups de treball especialitzats, ja siguin de caràcter intern, extern o mixt.
La Comissió es reunirà en sessió ordinària almenys un cop l'any, amb l'objecte d'elaborar l'informe, que remetrà a l'Alcaldia, i que coincidirà amb el lliurament dels indicadors per a l'Informe de l'Estat de Seguretat (INES). Igualment, podrà reunir-se en sessió extraordinària en cada ocasió en que els assumptes relacionats amb les seves competències ho requereixi. Les reunions seran convocades per la presidència de la Comissió, ja sigui per pròpia iniciativa, ja a petició de qualsevol dels seus components, amb una antelació mínima de 5 dies hàbils en el cas de tractar-se d'una sessió ordinària i de 48 hores quan es tracti d'una sessió extraordinària.
El Comitè de Seguretat TIC reportarà a l'alcaldia del seu Ajuntament.

9.3 - RESPONSABILITATS ASSOCIADES A L'ESQUEMA NACIONAL DE SEGURETAT

9.3.1 - Responsable de la Informació i Serveis

Seran tasques per dur a terme pel Responsable de la Informació i Serveis en relació amb l'Esquema Nacional de Seguretat les següents:

- Identificar, valorar i aprovar la informació i serveis de ciutadans o d'altres administracions públiques que fos tractada pel seu Ajuntament.
- Establir i aprovar els requisits de seguretat aplicables al servei i la informació dins del marc establert en l'annex I de Reial Decret 3/2010, de 8 de gener, prèvia proposta al responsable de seguretat ENS, i / o Comitè de Seguretat de la informació
- Acceptar els nivells de risc residual que afectin al Servei i a la Informació.

- Serà coneixedor de l'estat de la seguretat de la informació tractada, així com dels serveis prestats.
- Ha de comunicar al govern de l'organisme la necessitat de suspendre un servei per aquelles violacions de la seguretat que afectessin a la informació manejada o al propi servei.

9.3.2 - Responsable de Seguretat

Seran tasques per dur a terme pel Responsable de Seguretat en relació amb l'Esquema Nacional de Seguretat les següents:

- Mantenir i verificar el nivell adequat de seguretat de la Informació manejada i dels serveis electrònics prestats pels sistemes d'informació.
- Promoure la formació i conscienciació en matèria de seguretat de la informació.
- Designar responsables de l'execució de l'anàlisi de riscos, de la declaració d'aplicabilitat, identificar mesures de seguretat, determinar configuracions necessàries i elaborar la documentació de sistema.
- Proporcionar assessorament per a la determinació de la categoria de sistema, en col·laboració amb el responsable del Sistema i / o Comitè de Seguretat de la Informació.
- Participar en l'elaboració i implantació dels plans de millora de la seguretat i arribat el cas en els plans de continuïtat, procedint a la seva validació.
- Gestionar les revisions externes o internes del sistema.
- Gestionar els processos de certificació.
- Elevar al Comitè de Seguretat l'aprovació de canvis i altres requisits de sistema.

Quan la complexitat del sistema ho justifiqui, el responsable de Seguretat podrà designar els responsables de sistema delegats que consideri necessaris, que tindran dependència funcional directa d'aquell i seran responsables en el seu àmbit de totes aquelles accions que els delegui el mateix. De la mateixa manera, també podrà delegar en un altre funcions concretes de les responsabilitats que se li atribueixen.

9.3.3 - Comitè STIC

El Comitè de Seguretat TIC tindrà les següents funcions:

- Divulgació de la política i normativa de seguretat de l'Ajuntament.
- Aprovació de la normativa de seguretat de l'Ajuntament.
- Revisió anual de la política de seguretat perquè sigui aprovada per Ple Municipal.
- Desenvolupament del procediment de designació de rols.
- Designació de rols i responsabilitats.
- Promoció, supervisió i aprovació de les tasques de seguiment de l'ENS:
  - Tasques d'adequació
  - Anàlisi de Riscos
  - Plans de millora de seguretat de la informació
- Informar regularment l'estat de la seguretat de la informació a l'alcaldia.
- Elaborar l'estratègia d'evolució pel que fa a seguretat de la informació.
- Elaborar i aprovar els requisits de formació i qualificació d'administradors, operadors i usuaris des del punt de vista de la seguretat de la informació.
- Promoure les auditories periòdiques que permetin verificar el compliment de les obligacions de l'organisme en matèria de seguretat.
- Monitoritzar els principals riscos residuals assumits pel seu Ajuntament i recomanar possibles actuacions respecte a ells.
- Coordinar els esforços de les diferents àrees en matèria de seguretat de la informació, per assegurar que els esforços són consistents, alineats amb l'estratègia decidida en la matèria, i evitar duplicitats.
- Prioritzar les actuacions en matèria de seguretat quan els recursos siguin limitats

9.4 - ASSIGNACIÓ DE ROLS

Es defineix com a Responsable de la informació i Serveis a la Secretària interventora de l'Ajuntament de Vilabella.

Es defineix com a Responsable de la Seguretat al Responsable TIC del Consell Comarcal de l'Alt Camp.

9.5 - PROCEDIMIENTS DE DESIGNACIÓ DE LES PERSONES

La creació del Comitè de Seguretat de la Informació, el nomenament dels seus integrants i la designació dels responsables identificats en aquesta Política ha estat realitzada per l'alcalde de l'Ajuntament de Vilabella, i comunicada a les parts afectades per aprovació del Ple.
Els membres de Comitè, així com els rols de seguretat seran revisats cada quatre anys o en ocasió de vacant.

9.6 - RESOLUCIÓ DE CONFLICTES

El Comitè STIC s'encarregarà de la resolució dels conflictes i/o diferències d'opinions, que poguessin sorgir entre els rols de seguretat.

10. GESTIÓ DE RISCOS

Tots els sistemes subjectes a aquesta Política hauran de realitzar un anàlisi de riscos, avaluant les amenaces i els riscos als que estan exposats.
Aquest anàlisis es repetirà:

- Regularment, al menys un cop a 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 dels anàlisis de riscos, el Comitè STIC establirà una valoració de referència per als diferents tipus d'informació manipulada i els diferents serveis prestats.
El comitè STIC dinamitzarà la disponibilitat dels recursos per atendre a les necessitats de seguretat dels diferents sistemes, promovent inversions de caràcter horitzontal.

11. DESENVOLUPAMENT DE LA POLÍTICA DE SEGURETAT DE LA INFORMACIÓ

El **Comitè STIC** ha aprovat el desenvolupament d'un sistema de gestió, que serà establert, implementat, mantingut i millorat, d'acord amb els estàndards de seguretat.
Aquest sistema s'adequarà servint per a la gestió dels controls de l'Esquema Nacional de Seguretat. El sistema serà documentat i permetrà generar evidències dels controls i de l'acompliment dels objectius marcats pel Comitè. Hi ha d'haver un procediment de gestió documental que establirà les directrius per a l'estructuració de la documentació de seguretat de sistema, la seva gestió i accés.
Correspon al **Comitè STIC** la revisió anual de la present Política proposant, en cas que sigui necessari millores de la mateixa, per a la seva aprovació per part del Ple Municipal per raó de la matèria de l'Ajuntament de Vilabella.

12. OBLIGACIONS DEL PERSONAL

Tot el personal l'Ajuntament de Vilabella, així com el que presti serveis a l'organisme relacionats amb els sistemes d'informació, té l'obligació de conèixer i complir la present Política de seguretat, les normatives i el procediments derivats de la mateixa. Es trobaran entre elles les relatives a la protecció de dades personals.
El responsable de seguretat haurà de disposar dels mecanismes necessaris perquè la informació arribi a tothom.
L'incompliment manifest de la Política de seguretat de la informació o la normativa i procediments derivats d'aquesta podrà implicar l'inici de mesures disciplinàries oportunes i, si s'escau, les responsabilitats legals corresponents.

13. TERCERES PARTS

Quan l'Ajuntament de Vilabella presti serveis a altres organismes o manipuli informació d'altres organismes, se'ls farà partícips d'aquesta Política de seguretat de la informació, establint canals de comunicació entre els respectius Comitès de Seguretat TIC i procediments d'actuació per a la reacció davant incidents de seguretat.

Quan l'Ajuntament de Vilabella utilitzi serveis de tercers o comuniqui informació a tercers, se'ls farà partícips d'aquesta Política de seguretat i de la normativa de seguretat que pertoqui a aquests serveis o informació.

Aquesta tercera part quedarà subjecta a les obligacions establertes en aquesta normativa, podent desenvolupar els seus propis procediments operatius per satisfer-la. S'establiran procediments específics d'informe i resolució d'incidències, que garantiran que el personal dels tercers estan adequadament conscienciats en matèria de seguretat, com a mínim al mateix nivell que l'establert en aquesta Política.

Quan algun aspecte de la Política no pugui ser satisfet per una tercera part d'acord a l'establert anteriorment, es requerirà un informe del responsable de seguretat que indiqui els riscos en què s'incorre i la forma de tractar-los. Es requerirà l'aprovació d'aquest informe pels responsables de la informació i els serveis afectats abans de seguir endavant.

SEGURdades

Consultors en protecció de dades personals

Categorització del Sistema de l'Ajuntament de Vilabella.

Índex

CATEGORITZACIÓ DEL SISTEMA

CONTROL DEL DOCUMENT

Nom del document**: ENS-CS018 VILABELLA** Nombre de Pàgines: **18**
Autor: Jordi Vidal (SEGURdades)
Data: 28/09/2020
Aprovat per: Responsable de la Seguretat
Classificació de la Informació: CONFIDENCIAL
Llista de Distribució: COMITÈ STIC DE L'AJUNTAMENT DE VILABELLA

CONTROL DE VERSIONS

Nº Versió	Autor	Data	Canvis realitzats	Comentaris
1.0	Jordi Vidal (SEGURdades)	28/09/2020	Versió inicial	Pendent de revisió

1 INTRODUCCIÓ

D'acord amb el que disposa el Reial Decret 3/2010 del 8 de gener, pel qual es regula l'Esquema Nacional de Seguretat (ENS, d'ara endavant), aquest document conté el resum de la identificació i valoració de la informació i Serveis que gestiona el SGSI de l'**Ajuntament de Vilabella.**

Aquesta valoració s'ha realitzat utilitzant la GUIA "*CCN-STIC 803 – Valoración de la Información y Servicios*"

L'Esquema Nacional de Seguretat estableix una sèrie de mesures de seguretat en el seu Annex II que estan condicionades a la valoració del nivell de seguretat en cada dimensió, i a la categoria (article 43) del sistema d'informació de què es tracti. Al seu torn, la categoria del sistema es calcula en funció del nivell de seguretat més alt de les dimensions valorades.

2 OBJECTE

El procés de determinació de nivells i categories s'estableix en l'Annex I, que aporta una sèrie de criteris generals per determinar si els requisits de seguretat són de nivell ALT, MIG o BAIX en cadascuna de les dimensions de seguretat: confidencialitat [C] , integritat [i], disponibilitat [D], autenticitat [A], i traçabilitat [T].

L'Esquema Nacional de Seguretat estableix tres categories per als sistemes:

BÀSICA, MITJA i ALTA.

- Un sistema d'informació és de categoria ALTA si alguna de les seves dimensions de seguretat assoleix el nivell ALT.
- Un sistema d'informació és de categoria MITJA si alguna de les seves dimensions de seguretat assoleix el nivell MIG i cap arriba a un nivell superior.
- Un sistema d'informació és de categoria BÀSICA si alguna de les seves dimensions de seguretat assoleix el nivell BAIX i cap arriba a un nivell superior.

3 METODOLOGIA

Per a identificar la informació i serveis que es troben dins de l'abast de l'ENS, s'ha pres com a base l'anàlisi de les competències recollides a l'article 25 i lo establert a l'article 26 de la llei 7/1985, del 2 d'abril, *Reguladora de las Bases de Régimen Local (RBRL),* els tràmits disponibles a la carpeta ciutadana a través del ACTIO de la Diputació de Tarragona i tots els serveis associats del consorci AOC, Diputació de Tarragona, Generalitat de Catalunya i altres proveïdors TIC.

4 PROCEDIMENT DE VALORACIÓ

Un cop identificada tota la Informació i els Serveis, s'ha realitzat la valoració dels actius essencials de l'**Ajuntament de Vilabella** obtinguts anteriorment segons les 5 dimensions de Seguretat:

- [D] disponibilitat
- [I] integritat de les dades
- [C] confidencialitat de les dades
- [A] autenticitat dels usuaris i de la informació
- [T] traçabilitat el servei i de les dades
- [DP] Dades personals

El nivell de seguretat requerit en l'aspecte de **Disponibilitat** s'ha establert en funció de les conseqüències que tindria el qual una persona autoritzada no pogués accedir a la informació quan la necessita.

El nivell de seguretat requerit en l'aspecte d'**Integritat** s'ha establert en funció de les conseqüències que tindria la seva modificació per algú que no està autoritzat a actualitzar la informació.

El nivell de seguretat requerit en l'aspecte de **Confidencialitat** s'ha establert en funció de les conseqüències que tindria la seva revelació a persones no autoritzades o que no necessiten conèixer la informació.

El nivell de seguretat requerit en l'aspecte d'**Autenticitat** s'ha establert en funció de les conseqüències que tindria el fet que la informació no fos autèntica.

El nivell de seguretat requerit en l'aspecte de **Traçabilitat** s'ha establert en funció de les conseqüències que tindria el no poder rastrejar a posteriori qui ha accedit a o modificat una certa informació.

Quan un aspecte no requereix mesures de seguretat, en l'apartat de valoració s'ha indicat SENSE VALORAR.

A cada valoració s'han descrit els criteris que s'han seguit per obtenir el resultat.

5 DOMINIS DE SEGURETAT

L'Ajuntament de Vilabella té externalitzat a tercers la majoria de serveis que donen suport a la tramitació electrònica, així com altres serveis associats. És per això que s'han identificat les següents subsistemes, anomenats a partir d'ara **Dominis de Seguretat**:

- [base] Ajuntament
- [AOC] Consorci AOC
- [DIPTA] Diputació de Tarragona
- [GENCAT] Generalitat de Catalunya

6 IDENTIFICACIÓ DE LA INFORMACIÓ

S'han identificat la següent informació relacionada amb la Tramitació electrònica a l'**Ajuntament de Vilabella** que es troben gestionats per diferents serveis identificats al punt 7 IDENTIFICACIÓ DE SERVEIS d'aquest document**:**

ID	INFORMACIÓ	DESCRIPCIÓ	APLICA

CATEGORITZACIÓ DEL SISTEMA

I 01	GESTIÓ URBANISME MUNICIPAL	Gestió i control dels procediments i activitats realitzats per l'Ajuntament en matèria d'urbanisme, incloent planejament, gestió, restauració de la legalitat urbanística, expropiacions urbanístiques i altres qüestions de competència municipal.	s
I 02	LLICÈNCIES, AUTORITZACIONS I CONCESSIONS	Gestió i tramitació dels expedients de llicències, permisos, concessions i autoritzacions de qualsevol tipus gestionades des de l'Ajuntament.	s
I 03	ATENCIÓ A LA CIUTADANIA	Tramitació i gestió de sol·licituds d'informació, queixes, reclamacions i iniciatives rebudes a l'Ajuntament. Gestió de les sol·licituds d'accés a la informació pública i de la publicitat activa (transparència) de l'Ajuntament.	s
I 04	ATENCIONS I PRESTACIONS SOCIALS	Gestió de la història social per a la prestació dels serveis socials en l'àmbit municipal. Assistència i assessorament dirigits al col·lectiu de dones víctimes de violència de gènere o en risc d'exclusió social. Desenvolupament de polítiques d'atenció a la infància, igualtat, majors	n
I 05	AJUDES I SUBVENCIONS	Tramitació i gestió dels ajuts, beques i subvencions existents en els diferents programes o línies de subvenció de l'Ajuntament.	s
I 06	POLICIA LOCAL	Gestió i control dels procediments i activitats realitzats per la Policia Local en l'àmbit de les seves competències, incloent atestats, policia judicial, seguretat ciutadana, trànsit, mobilitat, objectes perduts, així com el servei de grua i dipòsit de vehicles. Així com la gestió dels sistemes de videovigilància per garantir la seguretat a les vies públiques.	n
I 07	PROTECCIÓ CIVIL	Gestió de les actuacions i intervencions de Protecció Civil.	n
I 08	PROCEDIMENTS SANCIONADORS	Descripció finalitat gestió i control de tota classe de procediments sancionadors oberts a conseqüència d'infraccions tipificades en les ordenances municipals i la resta de normativa reguladora de les competències de l'Ajuntament.	s
I 09	SERVEIS TELEMÀTICS I COMUNICACIONS	Gestió de les persones usuàries dels serveis telemàtics posats a disposició de la ciutadania: serveis web; equips d'ús públic; altres serveis tecnològics municipals posats a disposició de la ciutadania. Serveis de comunicacions informatives.	s
I 10	GESTIÓ DE SERVEIS FUNERARIS	Gestió del cementiri municipal i dels serveis funeraris.	s
I 11	GESTIÓ D'INGRESSOS PÚBLICS	Gestió de la recaptació de taxes i impostos municipals executada en termini voluntari o executiu, gestió dels diferents padrons municipals i actuacions d'inspecció tributària.	s
I 12	GESTIÓ DE SERVEIS ESPORTIUS	Gestió de les instal·lacions esportives i activitats esportives desenvolupades en les mateixes, així com el foment, promoció de l'esport al municipi.	s
I 13	GESTIÓ DE SERVEIS CULTURALS	Gestió de les activitats culturals organitzades o promocionades per l'Ajuntament, inclosa la gestió de les biblioteques municipals.	s
I 14	GESTIÓ DE SERVEIS EDUCATIUS	Gestió dels serveis, activitats i esdeveniments educatius organitzats i promoguts per l'Ajuntament.	n
I 15	GESTIÓ DE L'ARXIU MUNICIPAL	Organització, arxiu d'expedients, documents, continguts audiovisuals, fons o registres de l'Ajuntament que han passat a l'Arxiu Municipal. Gestió de les peticions d'accés, consultes, còpies i extraccions de documents.	s
I 16	CONTRACTACIÓ PÚBLICA	Gestió de el procés de contractació municipal i seguiment dels licitadors per al compliment del servei contractat.	s
I 17	GESTIÓ DE PERSONAL	Gestió de la nòmina de personal funcionari i laboral de l'Ajuntament, així com l'obtenció de tots els productes derivats de la mateixa. Gestió de personal de l'Ajuntament: Control d'incompatibilitats; situació laboral; formació dels empleats municipals. Compliment de les obligacions en matèria de prevenció de riscos laborals. [Categories especials de dades]	s
I 18	GESTIÓ PRESSUPOSTÀRIA ECONÒMICA I COMPTABLE	Gestió econòmica i comptable de l'Ajuntament per tal de fiscalitzar els ingressos i despeses de la mateixa. Realització de pagaments corresponents, gestió de la facturació, control pressupostari i gestió fiscal.	s

I 19	GESTIÓ DELS ÒRGANS MUNICIPALS DE GOVERN	Gestió de les dades dels membres de la corporació de l'Ajuntament amb la finalitat de realitzar un seguiment i control sobre els actes municipals, pagament de les remuneracions per les funcions exercides, control d'incompatibilitats, registre de béns i interessos.	s
I 20	PADRÓ MUNICIPAL D'HABITANTS	Gestió del padró municipal d'habitants d'acord als fins que estableix al respecte la Llei de Bases de Règim Local i altra normativa local aplicable. Gestió de el cens electoral segons estableix la Llei de règim electoral general i usos també amb fins històrics, estadístics i científics.	s
I 21	REGISTRE D'ENTRADA I SORTIDA DE DOCUMENTS	Gestió del registre d'entrada i sortida de documents a l'Ajuntament en els termes i condicions establertes en la Llei de procediment administratiu comú i en la normativa reguladora del funcionament de les entitats locals.	s
I 22	DEFENSA JURÍDICA I RESPONSABILITAT PATRIMONIAL	Gestió dels expedients de responsabilitat patrimonial de l'Ajuntament. Gestió i seguiment dels expedients administratius, així com d'altres actuacions realitzades des de la Secretaria Municipal.	s
I 23	SEGURETAT D'INSTAL·LACIONS MUNICIPALS	Sistemes de videovigilància i control d'accessos per tal de garantir la seguretat béns i instal·lacions municipals, així com de les persones que accedeixen o treballen en les mateixes.	s
I 24	GESTIÓ DE SERVEIS JUVENILS MUNICIPALS	Gestió i control dels serveis, programes, activitats i recursos adreçats a la població juvenil del municipi i dels participants.	s
I 25	GESTIÓ DE LA PARTICIPACIÓ CIUTADANA	Gestió i control del registre municipal d'entitats ciutadanes i de les consultes populars, pressupostos participatius, i altres procediments i activitats de participació ciutadana realitzats o promoguts per l'Ajuntament.	s
I 26	VOLUNTARIAT	Gestió i control de les persones que realitzen algun tipus d'activitat de voluntariat a l'Ajuntament i de les activitats realitzades.	n
I 27	GESTIÓ DE LES OBRES MANTENIMENT I INFRAESTRUCTURES	Gestió de la informació relacionada amb el manteniment de les vies públiques i instal·lacions municipals.	s
I 28	GESTIÓ DE LA PROMOCIÓ LOCAL I EL TURISME	Gestió de les activitats de promoció de l'entitat local i de la promoció del turisme.	s
I 29	GESTIÓ D'ACTIVITATS EN TRANSPARÈNCIA	Gestió de l'Acompliment de la Llei de Transparència, Accés a la Informació Pública i Bon Govern a l'entitat local.	s
I 30	SISTEMES D'INFORMACIÓ I COMUNICACIONS	Gestió interna dels sistemes d'informació i comunicacions de l'Ajuntament per garantir el seu correcte funcionament i el compliment de les obligacions de seguretat i protecció de dades legalment establertes.	s
I 31	REGISTRE D'ANIMALS	Registre dels animals domèstics (gossos, gats i fures) i d'animals potencialment perillosos.	s
I 32	UTILITZACIÓ DE BENS I ESPAIS MUNICIPALS	Gestió de la utilització de bens i espais municipals. Cessió d'espais propietat de l'Ajuntament, equipament, etc.	s
I33	ALUMNES D'ESCOLES BRESSOLS	Dades dels alumnes, progenitors i persones de contacte als que se'ls hi presta serveis. Gestió d'altes i baixes, modificacions, pagaments de quotes	s

7 IDENTIFICACIÓ DELS SERVEIS

A continuació identifiquem els Actius Essencials (Serveis TIC) que suporten i gestionen els serveis al ciutadà i la informació referent a la tramitació electrònica de l'**Ajuntament de Vilabella:**

ID	Descripció	Servei	Domini
STIC01	Pagina Web	Hosting Altanet	DIPTA
STIC02	Perfil del contractant	CONTRACTACIÓ PUBLICA	GENCAT
STIC03	Seu electrònica	SEU-E.CAT	AOC
STIC04	Registre entrada sortida	ERES	DIPTA
STIC05	Gestor Expedients	ACTIO	DIPTA
STIC06	Comptabilitat	ABSIS	Ajuntament
STIC07	Padró Habitants	EPADRO	DIPTA
STIC08	Gestió de Subvencions	PORTAL DE TRANSPARÈNCIA	AOC
STIC09	Finestra Única Empresarial	FUE	GENCAT
STIC10	Facturació Electrònica	EFACT	AOC
STIC11	Notificacions Electròniques	ENOTUM	AOC
STIC12	Tauler Electrònic	ETAULER	AOC
STIC13	Registre públic de Contractes	RPC	GENCAT
STIC14	Consulta de Dades Interadministrativa	VIA OBERTA	AOC
STIC15	Extranet Administracions Catalanes	EACAT	AOC
STIC17	Correu electrònic	ALTANET	DIPTA

8 VALORACIÓ DE LA INFORMACIÓ I SERVEIS

La valoració de la Informació i Serveis obtinguda és la desenvolupada en els punts a continuació:

8.1 Informació del ciutadà

Capa	Actiu	[D]	[I]	[C]	[A]	[T]
[INF] INFORMACIÓ DEL CIUTADA						
	[I01] GESTIÓ URBANISME MUNICIPAL		[M]	[M]	[M]	[M]
	[I02] LLICÈNCIES, AUTORITZACIONS I CONCESSIONS		[M]	[M]	[M]	[M]
	[I03] ATENCIÓ A LA CIUTADANIA		[M]	[B]	[M]	[M]
	[I05] AJUDES I SUBVENCIONS		[M]	[M]	[M]	[M]
	[I08] PROCEDIMENTS SANCIONADORS		[M]	[M]	[M]	[M]
	[I09] SERVEIS TELEMÀTICS I COMUNICACIONS		[M]	[M]	[M]	[M]
	[I10] GESTIÓ DE SERVEIS FUNERARIS		[M]	[M+]	[B]	[M]
	[I11] GESTIÓ D'INGRESSOS PÚBLICS		[M]	[M]	[M]	[M]
	[I12] GESTIÓ DE SERVEIS ESPORTIUS		[B]	[M]	[B]	[B]
	[I13] GESTIÓ DE SERVEIS CULTURALS		[B]	[B]	[B]	[B]
	[I15] GESTIÓ DE L'ARXIU MUNICIPAL		[M]	[M]	[M]	[M]
	[I16] CONTRACTACIÓ PÚBLICA		[M]	[B]	[M]	[M]
	[I17] GESTIÓ DE PERSONAL		[M]	[M+]	[M]	[M]
	[I18] GESTIÓ PRESSUPOSTÀRIA ECONÒMICA I COMPTABLE		[M]	[M]	[M]	[M]
	[I19] GESTIÓ DELS ÒRGANS MUNICIPALS DE GOVERN		[M]	[M]	[M]	[M]
	[I20] PADRÓ MUNICIPAL D'HABITANTS		[M]	[M]	[M]	[M]
	[I21] REGISTRE D'ENTRADA I SORTIDA DE DOCUMENTS		[M]	[M]	[M]	[M]
	[I22] DEFENSA JURÍDICA I RESPONSABILITAT PATRIMONIAL		[M]	[M]	[M]	[M]
	[i23] SEGURETAT D'INSTAL·LACIONS MUNICIPALS		[B]	[M]	[B]	[B]
	[I24] GESTIÓ DE SERVEIS JUVENILS MUNICIPALS		[M]	[M]	[M]	[M]
	[I25] GESTIÓ DE LA PARTICIPACIÓ CIUTADANA		[B]	[B]	[B]	[B]
	[i27] GESTIÓ DE LES OBRES MANTENIMENT I INFRAESTRUCTURES		[B]	[B]	[B]	[B]
	[I28] GESTIÓ DE LA PROMOCIÓ LOCAL I EL TURISME		[B]	[B]	[B]	[B]
	[I29] GESTIÓ D'ACTIVITATS EN TRANSPARÈNCIA		[B]	[0]	[B]	[B]
	[I30] SISTEMES D'INFORMACIÓ I COMUNICACIONS		[B]	[B]	[B]	[B]
	[I31] REGISTRE D'ANIMALS		[M]	[M]	[M]	[M]
	[I32] UTILITZACIÓ DE BENS I ESPAIS MUNICIPALS		[B]	[B]	[B]	[B]
	[I33] ALUMNES D'ESCOLES BRESSOLS		[M]	[M]	[M]	[M]
	NIVELL MÀXIM DE LA INFORMACIÓ		**[M]**	**[M]**	**[M]**	**[M]**

8.2 Valoració Serveis

La Valoració dels Serveis TIC ha sigut realitzada segons la unió de la informació amb els serveis que tracten identificats al punt anterior:

Actius	[D]	[I]	[C]	[A]	[T]
[STIC01] Pàgina Web	[M]	[B]	[B]	[B]	[B]
[STIC02] Perfil del Contractant	[M]	[M]	[B]	[M]	[M]
[STIC03] Seu Electrònica	[M]	[B]	[0]	[B]	[B]
[STIC04] Registre entrada sortida	[M]	[M]	[M]	[M]	[M]
[STIC05] ACTIO - Gestor Expedients i Documentació	[M]	[M]	[M]	[M]	[M]
[STIC06] ABSIS (comptabilitat)	[M]	[M]	[M]	[M]	[M]
[STIC07] ePADRO Padró d'Habitants	[B]	[M]	[M]	[M]	[M]
[STIC08] PORTAL TRANSPARÈNCIA (Gestió de Subvencions)	[B]	[B]	[0]	[B]	[B]
[STIC09] FUE - Finestra Única Empresarial	[M]	[B]	[B]	[B]	[B]
[STIC10] eFACT - Facturació electrònica	[M]	[B]	[B]	[B]	[B]
[STIC11] eNOTUM - Notificacions electròniques	[M]	[M]	[M]	[M]	[M]
[STIC12] eTAULER - Tauler Electrònic	[M]	[M]	[M]	[M]	[M]
[STIC13] RPC - Registre Públic de Contractes	[B]	[B]	[B]	[B]	[B]
[STIC14] VIA OBERTA - Consulta de Dades Interadministratives	[B]	[B]	[B]	[B]	[B]
[STIC15] EACAT - Extranet Administracions Catalanes	[M]	[M]	[M]	[M]	[M]
[STIC17] Servei Correu Electronic - ALTANET	[M]	[M]	[M]	[M]	[M]
NIVELL MÀXIM DELS SERVEIS	**[M]**	**[M]**	**[M]**	**[M]**	**[M]**

8.3 Justificació de la Valoració

La justificació de la valoració atorgada en cadascuna de les dimensions afectades s'ha realitzat en base a les conseqüències que tindria un incident de seguretat, sent la exposada a continuació.

8.3.1 Justificació Disponibilitat

La justificació de la valoració dels Serveis s'ha realitzat en base a les conseqüències que tindria un incident de seguretat en la dimensió de disponibilitat [D], sent la exposada a continuació.

S'ha determinat que les **conseqüències d'un incident de seguretat que afectés a la dimensió de Disponibilitat [D]** de tots els Serveis, impedint que una persona autoritzada pogués accedir al servei provocaria:

VALORACIÓ DELS SERVEIS		[D]
SENSE VALORAR	Quan el RTO és superior a 5 dies laborables Quan la informació és prescindible per temps indefinit.	
CAPACITAT (Assolir els seus objectius)	Perjudici molt greu [A] L'anul·lació de la capacitat de l'organització per atendre alguna de les seves obligacions fonamentals i que aquestes segueixin portant a terme	
	Perjudici greu [M]	X

	Reducció significativa de la capacitat de l'organització per atendre eficaçment a les seves obligacions fonamentals, encara que aquestes segueixin portant a terme	
	Perjudici limitat [B] Reducció apreciable de la capacitat de l'organització per atendre eficaçment les seves obligacions corrents, encara que aquestes segueixin portant a terme	X
DANY ACTIU (Protecció de l'actiu)	Perjudici molt greu [A] El patiment d'un dany molt greu, i fins i tot irreparable, pels actius de l'organització.	
	Perjudici greu [M] El patiment d'un dany significatiu pels actius de l'organització	X
	Perjudici limitat [B] El patiment d'un dany menor pels actius de l'organització	X
COMPLIMENT SERVEI (Obligacions diàries de el servei)	Perjudici molt greu [A] Anul·lada la capacitat per complir amb les obligacions diàries de el servei	
	Perjudici greu [M] Reducció significativa de la capacitat per complir amb les obligacions diàries de el servei	X
	Perjudici limitat [B] Reducció apreciable de la capacitat per complir amb les obligacions diàries de el servei	X
COMPLIMENT LLEI (Legislació vigent)	Perjudici molt greu [A] L'incompliment greu d'alguna llei o regulació	
	Perjudici greu [M] L'incompliment material d'alguna llei o regulació o l'incompliment formal que no tingui el caràcter de reparable	X
	Perjudici limitat [B] L'incompliment formal d'alguna llei o regulació, que tingui el caràcter de reparable	X
CIUTADANIA (Respecte dels drets de les persones)	Perjudici molt greu [A] Causar un perjudici greu a algun individu, de difícil o impossible reparació	
	Perjudici greu [M] Causar un perjudici significatiu a algun individu, de difícil reparació	X
	Perjudici limitat [B]	X

	Causar un perjudici menor a algun individu, que tot i ser molest, pugui ser fàcilment reparable	
RTO (Temps de Recuperació de el Servei)	<4 hores [A]	
	4 hores <RTO <a 1 dia [M]	X
	A 1 dia <RTO <5 dies [B]	X

8.3.2 Justificació Confidencialitat

S'ha determinat que les **conseqüències que tindria un incident de seguretat que afectés la dimensió de Confidencialitat [C]** de la Informació provocant la seva revelació a persones no autoritzades o que no necessiten conèixer la informació, ocasionaria un:

VALORACIÓ DE LA INFORMACIÓ		[C]
SENSE VALORAR	Perjudici menyspreable [S] Informació de caràcter públic, accessible per qualsevol persona.	X
CAPACITAT (Assolir els seus objectius)	Perjudici molt greu [A] L'anul·lació de la capacitat de l'organització per atendre alguna de les seves obligacions fonamentals i que aquestes segueixin portant a terme	
	Perjudici greu [M] El patiment d'un dany significatiu pels actius de l'organització	X
	Perjudici limitat [B] Reducció apreciable de la capacitat de l'organització per atendre eficaçment les seves obligacions corrents, encara que aquestes segueixin portant a terme	X
DANY ACTIU (Protecció de l'actiu)	Perjudici molt greu [A] El patiment d'un dany molt greu, i fins i tot irreparable, pels actius de l'organització.	
	Perjudici greu [M] El patiment d'un dany significatiu pels actius de l'organització	X
	Perjudici limitat [B] El patiment d'un dany menor pels actius de l'organització	X
COMPLIMENT SERVEI (Obligacions diàries de el servei)	Perjudici molt greu [A] Anul·lada la capacitat per complir amb les obligacions diàries de el servei	
	Perjudici greu [M] Reducció significativa de la capacitat per complir amb les obligacions diàries de el servei	X
	Perjudici limitat [B] Reducció apreciable de la capacitat per complir amb les obligacions diàries de el servei	X
COMPLIMENT LLEI	Perjudici molt greu [A]	

(Legislació vigent) [1]	L'incompliment greu d'alguna llei o regulació	
	Perjudici greu [M] L'incompliment material d'alguna llei o regulació o l'incompliment formal que no tingui el caràcter de reparable	X
	Perjudici limitat [B] L'incompliment formal d'alguna llei o regulació, que tingui el caràcter de reparable	X
CIUTADANIA (Respecte dels drets de les persones)	Perjudici molt greu [A] Causar un perjudici greu a algun individu, de difícil o impossible reparació	
	Perjudici greu [M] Causar un perjudici significatiu a algun individu, de difícil reparació	X
	Perjudici limitat [B] Causar un perjudici menor a algun individu, que tot i ser molest, pugui ser fàcilment reparable	X

[1] Entre altres normes d'aplicació a la informació, s'ha tingut en compte el compliment de la normativa de Protecció de Dades Personals

8.3.3 Justificació Integritat

S'ha determinat que les **conseqüències que tindria un incident de seguretat que afectés a la dimensió d'Integritat [I]** de la Informació provocant que pogués ser modificada per algú que no està autoritzat, ocasionaria un:

VALORACIÓ DE LA INFORMACIÓ		[I]
SENSE VALORAR	Perjudici menyspreable [S] Quan els errors en el seu contingut no tenen conseqüències o són fàcil o ràpidament reparables	
CAPACITAT (Assolir els seus objectius)	Perjudici molt greu [A] L'anul·lació de la capacitat de l'organització per atendre alguna de les seves obligacions fonamentals i que aquestes segueixin portant a terme	
	Perjudici greu [M] El patiment d'un dany significatiu pels actius de l'organització	X
	Perjudici limitat [B] Reducció apreciable de la capacitat de l'organització per atendre eficaçment les seves obligacions corrents, encara que aquestes segueixin portant a terme	X
DANY ACTIU (Protecció de l'actiu)	Perjudici molt greu [A] El patiment d'un dany molt greu, i fins i tot irreparable, pels actius de l'organització.	
	Perjudici greu [M] El patiment d'un dany significatiu pels actius de l'organització	X
	Perjudici limitat [B]	X

	El patiment d'un dany menor pels actius de l'organització	
COMPLIMENT SERVEI (Obligacions diàries de el servei)	Perjudici molt greu [A] Anul·lada la capacitat per complir amb les obligacions diàries de el servei	
	Perjudici greu [M] Reducció significativa de la capacitat per complir amb les obligacions diàries de el servei	X
	Perjudici limitat [B] Reducció apreciable de la capacitat per complir amb les obligacions diàries de el servei	X
COMPLIMENT LLEI *(Legislació vigent) [1]*	Perjudici molt greu [A] L'incompliment greu d'alguna llei o regulació	
	Perjudici greu [M] L'incompliment material d'alguna llei o regulació o l'incompliment formal que no tingui el caràcter de reparable	X
	Perjudici limitat [B] L'incompliment formal d'alguna llei o regulació, que tingui el caràcter de reparable	X
CIUTADANIA (Respecte dels drets de les persones)	Perjudici molt greu [A] Causar un perjudici greu a algun individu, de difícil o impossible reparació	
	Perjudici greu [M] Causar un perjudici significatiu a algun individu, de difícil reparació	X
	Perjudici limitat [B] Causar un perjudici menor a algun individu, que tot i ser molest, pugui ser fàcilment reparable	X

[1] Entre altres normes d'aplicació a la informació, s'ha tingut en compte el compliment de la normativa de Protecció de Dades Personals

8.3.4 Justificació Autenticitat

S'ha determinat que les **conseqüències que tindria un incident de seguretat que afectés la dimensió d'Autenticitat [A]** de la Informació provocant que aquesta no sigui autèntica, ocasionaria un:

VALORACIÓ DE LA INFORMACIÓ		[A]
SENSE VALORAR	Perjudici menyspreable [S] Quan l'origen és irrellevant o àmpliament conegut per altres mitjans.	

	Quan el destinatari és irrellevant, per exemple per tractar-se d'informació de difusió anònima.	
CAPACITAT (Assolir els seus objectius)	Perjudici molt greu [A] L'anul·lació de la capacitat de l'organització per atendre alguna de les seves obligacions fonamentals i que aquestes segueixin portant a terme	
	Perjudici greu [M] El patiment d'un dany significatiu pels actius de l'organització	X
	Perjudici limitat [B] Reducció apreciable de la capacitat de l'organització per atendre eficaçment les seves obligacions corrents, encara que aquestes segueixin portant a terme	X
DANY ACTIU (Protecció de l'actiu)	Perjudici molt greu [A] El patiment d'un dany molt greu, i fins i tot irreparable, pels actius de l'organització.	
	Perjudici greu [M] El patiment d'un dany significatiu pels actius de l'organització	X
	Perjudici limitat [B] El patiment d'un dany menor pels actius de l'organització	X
COMPLIMENT SERVEI (Obligacions diàries de el servei)	Perjudici molt greu [A] Anul·lada la capacitat per complir amb les obligacions diàries de el servei	
	Perjudici greu [M] Reducció significativa de la capacitat per complir amb les obligacions diàries de el servei	X
	Perjudici limitat [B] Reducció apreciable de la capacitat per complir amb les obligacions diàries de el servei	X
COMPLIMENT LLEI (Legislació vigent) [1]	Perjudici molt greu [A] L'incompliment greu d'alguna llei o regulació	
	Perjudici greu [M] L'incompliment material d'alguna llei o regulació o l'incompliment formal que no tingui el caràcter de reparable	X
	Perjudici limitat [B] L'incompliment formal d'alguna llei o regulació, que tingui el caràcter de reparable	X
CIUTADANIA (Respecte dels drets de les persones)	Perjudici molt greu [A] Causar un perjudici greu a algun individu, de difícil o impossible reparació	
	Perjudici greu [M] Causar un perjudici significatiu a algun individu, de difícil reparació	X

	Perjudici limitat [B] Causar un perjudici menor a algun individu, que tot i ser molest, pugui ser fàcilment reparable	X

[1] Entre altres normes d'aplicació a la informació, s'ha tingut en compte el compliment de la normativa de Protecció de Dades Personals

8.3.5 Justificació Traçabilitat

S'ha determinat que les **conseqüències que tindria un incident de seguretat que afectés la dimensió de Traçabilitat [T]** de la Informació impedint que es pugui rastrejar a posteriori qui ha accedit o modificat certa informació, ocasionaria un:

VALORACIÓ DE LA INFORMACIÓ		[T]
SENSE VALORAR	Perjudici menyspreable [S] Quan no es poden produir errors d'importància, o són fàcilment reparables per altres mitjans. Quan no es poden perpetrar delictes rellevants, o la seva investigació és fàcilment realitzable per altres mitjans	
CAPACITAT (Assolir els seus objectius)	Perjudici molt greu [A] L'anul·lació de la capacitat de l'organització per atendre alguna de les seves obligacions fonamentals i que aquestes segueixin portant a terme	
	Perjudici greu [M] El patiment d'un dany significatiu pels actius de l'organització	X
	Perjudici limitat [B] Reducció apreciable de la capacitat de l'organització per atendre eficaçment les seves obligacions corrents, encara que aquestes segueixin portant a terme	X
DANY ACTIU (Protecció de l'actiu)	Perjudici molt greu [A] El patiment d'un dany molt greu, i fins i tot irreparable, pels actius de l'organització.	
	Perjudici greu [M] El patiment d'un dany significatiu pels actius de l'organització	X
	Perjudici limitat [B] El patiment d'un dany menor pels actius de l'organització	X
COMPLIMENT SERVEI (Obligacions diàries de el servei)	Perjudici molt greu [A] Anul·lada la capacitat per complir amb les obligacions diàries de el servei	
	Perjudici greu [M] Reducció significativa de la capacitat per complir amb les obligacions diàries de el servei	X
	Perjudici limitat [B]	X

	Reducció apreciable de la capacitat per complir amb les obligacions diàries de el servei	
COMPLIMENT LLEI (Legislació vigent) [1]	Perjudici molt greu [A] L'incompliment greu d'alguna llei o regulació	
	Perjudici greu [M] L'incompliment material d'alguna llei o regulació o l'incompliment formal que no tingui el caràcter de reparable	X
	Perjudici limitat [B] L'incompliment formal d'alguna llei o regulació, que tingui el caràcter de reparable	X
CIUTADANIA (Respecte dels drets de les persones)	Perjudici molt greu [A] Causar un perjudici greu a algun individu, de difícil o impossible reparació	
	Perjudici greu [M] Causar un perjudici significatiu a algun individu, de difícil reparació	X
	Perjudici limitat [B] Causar un perjudici menor a algun individu, que tot i ser molest, pugui ser fàcilment reparable	X

[1] Entre altres normes d'aplicació a la informació, s'ha tingut en compte el compliment de la normativa de Protecció de Dades Personals

9 VALORACIÓ DELS DOMINIS DE SEGURETAT

Un cop valorats els actius essencials del SGSI de l'**Ajuntament de Vilabella**, els dominis de seguretat on estan allotjats aquests serveis, agafaran el valor màxim de cadascuna de les dimensions de seguretat:

Dominis de Seguretat	[D]	[I]	[C]	[A]	[T]
[base] Ajuntament	[M]	[M]	[M]	[M]	[M]
[AOC] Consorci AOC	[M]	[M]	[M]	[M]	[M]
[DIPTA] Diputació de Tarragona	[M]	[M]	[M]	[M]	[M]
[GENCAT] Generalitat de Catalunya	[M]	[M]	[B]	[M]	[M]

10 CATEGORIA DEL SISTEMA

A continuació es recull la categorització del Sistema de l'**Ajuntament de Vilabella,** realitzat per el **Responsable de la Seguretat,** que ha determinat que la categoria del Sistema que suporta els Serveis i Informació es MITJA, tal i com s'estableix al determinar els nivells màxims obtinguts per a aquests actius, els quals s'exposen a continuació:

DIMENSIÓ	[D]	[A]	[C]	[I]	[T]	CATEGORÍA
NIVELL ASSIGNAT	MIG	MIG	MIG	MIG	MIG	MITJA

SEGURdades

Consultors en protecció de dades personals

Anàlisi de Riscos

Índex

CONTROL DEL DOCUMENT

Nom del document**: Analisi de Riscos - Plantilla** Nombre de Pàgines: **12**	
Autor: Jordi Vidal	Revisat per:
Data:	Data:
Aprovat per:	
Classificació de la Informació: **CONFIDENCIAL**	
Llista de Distribució: COMITÈ STIC i DIRECCIÓ	

CONTROL DE VERSIONS

Nº Versió	Autor	Data	Canvis realitzats	Comentaris
1.0	Jordi Vidal	06/7/2020	Versió inicial	Pendent de revisió

1 INTRODUCCIÓ

D'acord amb el que disposa el Reial Decret 3/2010, de 8 de gener, pel qual es regula l'Esquema Nacional de Seguretat (ENS, d'ara endavant), aquest document conté la Gestió dels Riscos que gestiona el SGSI de l'**Ajuntament de Vilabella.**

Aquest document s'ha realitzat utilitzant la GUIA "*CCN-STIC 882 – Guía de Análisis de Riesgos para Entidades Locales*".

L'Esquema Nacional de Seguretat estableix que s'ha de realitzar una gestió de la seguretat basada en els riscos que té i pot tenir una organització. És per això que aquest document descriu *l'Anàlisi de Riscos* realitzat i el seu corresponent *Pla de Tractament dels Riscos*.

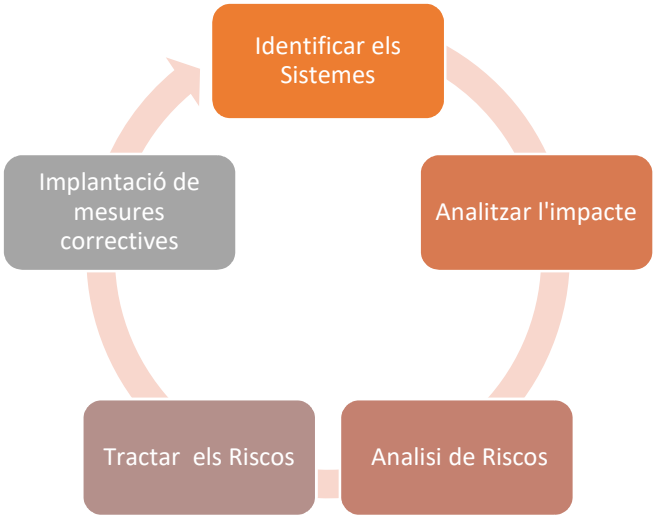
2 OBJECTE

L'objecte d'aquest document "*Anàlisi de Riscos"* és desenvolupar el procés d'Anàlisi i Gestió de Riscos de l'**Ajuntament de Vilabella** i posteriorment definir una estratègia de seguretat basada en els riscos obtinguts.

3 METODOLOGIA

Per a la realització de l'Anàlisi del Risc i el seu posterior Tractament del Risc s'ha fet servir la metodologia MAGERIT v3.

MAGERIT v3 realitza de forma cíclica les següents activitats:



Aquest cicle serà anual, de tal manera que un cop l'any es revisaran els nous serveis i amenaces per a ser categoritzats i incorporats en l'Anàlisi del Risc. Els serveis retirats seran eliminats de l'Anàlisi del Risc.

Identificar els sistemes

S'identificaran els processos / serveis de negoci que entrin en l'Abast del SGSI. Un cop identificats els processos / serveis, s'identificaran tots els actius (Infraestructura, serveis, persones, edificis...) dels quals depengui cada servei, creant així un arbre de dependències.

Analitzar l'impacte

Es realitzarà un anàlisi d'impacte sobre les 5 dimensions de seguretat de cadascun dels serveis / Informació que gestiona l'Ajuntament de Vilabella (Autenticitat, Confidencialitat, Disponibilitat, Integritat i Traçabilitat).

NOTA: Aquestes dues activitats es realitzen durant la FASE de Identificació, Valoració i Categorització del Sistema.

Anàlisi de Riscos

S'identificaran les principals amenaces que podrien materialitzar-se i les vulnerabilitats que podrien ser explotades per les amenaces. S'estimarà la probabilitat de que es produeixi cada amenaça, i es generarà una matriu de riscos.

Tractament del Risc

Un cop obtinguda la matriu de risc, s'establirà un llindar en el qual els riscos són assumibles o no. Dels riscos no assumibles, es decidirà quin tractament es farà:

- Mitigar Risc
- Traslladar Risc a tercers
- Assumir el Risc

Implantació de mesures Correctives

De cada Risc a Mitigar, s'escolliran les salvaguardes oportunes i/o s'aplicaran els controls de **l'Esquema Nacional de Seguretat** o de la **ISO/IEC 27002** que aconsegueixin reduir al risc a mode de salvaguarda.

Aquest cicle serà anual, de tal manera que com a mínim un cop l'any es revisaran els nous serveis i amenaces per a ser categoritzats i incorporats en l'Anàlisi del Risc. Els serveis retirats seran eliminats de l'Anàlisi del Risc.

4 ANÀLISI DE RISCOS

S'han identificat i classificat tots els actius segons la tipologia (Hardware, Sistema Operatiu, Xarxa, PC, Servidor...) ja que l'eina PILAR proposa una sèrie de riscos a cada actiu segons el tipus (si és un ordinador Portàtil, se li associa un risc de pèrdua o robatori per exemple) i el tipus d'informació que té (Informació Sensible, Dades personals, etc).

A l'ANNEX I es troben els Factors atenuants i agreujants. Pilar permet definir una sèrie de factors agreujants i atenuants que fan variar el factor de risc que té la nostra organització i aplica automàticament una sèrie de Riscos específics segons l'actiu i segons l'agreujant identificat. A continuació mostrem els principals factors identificats per a cadascuna de les Dimensions de Seguretat.

Amb aquestes dades, PILAR ens dóna una visió inicial sobre els principals riscos que apliquen a l'organització segons l'entorn i naturalesa d'aquesta.

4.1 Interpretació de l'Anàlisi

Alhora d'interpretar el present anàlisi, s'ha de diferenciar els següents termes:

Risc Potencial: és el Risc que pot arribar a tenir un actiu donada la seva naturalesa i entorn.

Risc actual: és el Risc que té un actiu amb les possibles salvaguardes i mesures implementades en el moment exacte que es realitza l'anàlisi, ja que depèn de l'organització, aquest risc ja pot variar considerablement del Risc Potencial.

Risc Residual: és el Risc que queda un cop implementades totes les salvaguardes escollides per mitigar/evitar el risc. Un Risc mai s'elimina al 100%, però es baixa fins a un nivell acceptable per a l'organització.

ARO: Sigles en anglès (Anual Rate of Occurrency), Tasa Anual d'ocurrència. És el nombre de cops que un esdeveniment/amenaça succeeixi de mitja en un any.

4.2 Definició de Risc

El risc es calcula que prenent en consideració el valor acumulat i l'efecte directe de les amenaces sobre l'actiu.

Com que hi ha dependències entre actius, els actius inferiors acumulen el valor dels actius superiors.

El risc és la valoració del dany per a l'organització, avaluat en els actius inferiors o del propi domini de seguretat.

Per calcular el risc acumulat que utilitzem:

- l'impacte
- la probabilitat

Risc = Impacte * Probabilitat

A l'Arxiu PILAR es troba la relació dels Riscos de cada actiu amb el seu Impacte i probabilitat.

4.3 Resum de Riscos Potencials

Explicació dels grups de riscos

[N] – Origen Natural
[I] – Origen Industrial
[E] – Error
[A] – Atac deliberat
[PR] – Privacitat

A continuació mostrem els principals riscos que afecten a algun dels actius del sistema i en el seu valor màxim. Per veure quins són els riscos que afecta cada amenaça i en quin valor, cal accedir a través de l'eina PILAR i l'arxiu de configuració .car corresponent.

Amenaces	[D]	[I]	[C]	[A]	[T]
[N.1] Fuego	3,3				
[N.2] Daños por agua	3,3				
[N.*] Desastres naturales	3,1				
[I.1] Fuego	3,3				
[I.2] Daños por agua	3,3				
[I.*] Desastres industriales	3,3				
[I.3] Contaminación medioambiental	2,8				
[I.4] Contaminación electromagnética	1,6				
[I.5] Avería de origen físico o lógico	2,8				
[I.6] Corte del suministro eléctrico	3,3				
[I.7] Condiciones inadecuadas de temperatura o humedad	3,3				
[I.8] Fallo de servicios de comunicaciones	3,3				
[I.9] Interrupción de otros servicios o suministros esenciales	2,8				
[I.10] Degradación de los soportes de almacenamiento de la información	3,3				
[I.11] Emanaciones electromagnéticas			0,75		
[E.1] Errores de los usuarios	0,8	1,3	1,8		
[E.2] Errores del administrador del sistema / de la seguridad	2,1	2,1	2,1		
[E.3] Errores de monitorización (log)		0,75			
[E.4] Errores de configuración		0,8			
[E.8] Difusión de software dañino	1,8	1,8	1,8		
[E.9] Errores de [re-]encaminamiento			1,6		
[E.10] Errores de secuencia		1,6			
[E.15] Alteración de la información		1,8			
[E.18] Destrucción de la información	3,6				
[E.19] Fugas de información			1,8		
[E.20] Vulnerabilidades de los programas (software)	0,75	2,1	2,1		
[E.21] Errores de mantenimiento / actualización de programas (software)	0,98	0,98			
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	3,6				
[E.24] Caída del sistema por agotamiento de recursos	3,9				
[E.25] Pérdida de equipos	3,6		3,7		
[E.28] Indisponibilidad del personal	1,6				
[A.3] Manipulación de los registros de actividad (log)		4,6			

[A.4] Manipulación de los ficheros de configuración	2,7	2,7	2,7	
[A.5] Suplantación de la identidad		3,7	4,1	4,6
[A.6] Abuso de privilegios de acceso	1,9	2,8	4,1	
[A.7] Uso no previsto	3,2	1,9	1,9	
[A.8] Difusión de software dañino	3,7	3,7	3,7	
[A.9] [Re-]encaminamiento de mensajes			1,7	
[A.10] Alteración de secuencia		1,7		
[A.11] Acceso no autorizado	3,7	3,7	4,9	5,5
[A.12] Análisis de tráfico			0,89	
[A.13] Repudio (negación de actuaciones)				3,4
[A.14] Interceptación de información (escucha)			1,9	
[A.15] Modificación de la información		4,3		
[A.18] Destrucción de la información	3,7			
[A.19] Revelación de información			3,4	
[A.22] Manipulación de programas	3,2	3,7	3,7	
[A.23] Manipulación del hardware	3,1		2,8	
[A.24] Denegación de servicio	4,6			
[A.25] Robo de equipos	4		4	
[A.26] Ataque destructivo	3,4			
[A.27] Ocupación enemiga	3,4			
[A.28] Indisponibilidad del personal	2,6			
[A.29] Extorsión	1,8	2,3	3	
[A.30] Ingeniería social (picaresca)	1,6	2,1	2,8	

[A.51] Inyección de código malicioso (a través de una frontera lógica)

[A.52] Extracción de información (a través de una frontera lógica)

[A.53] Acceso no autorizado (a través de una frontera lógica)

[A.55] Introducción de objetos (a través del perímetro físico)

[A.56] Retirada de objetos (a través del perímetro físico)

[A.57] Acceso no autorizado (a través del perímetro físico)

[A.58] Destrucción del perímetro físico

4.4 Resum de riscos potencials repercutits a cada actiu

A continuació mostrem el valor del risc repercutit a cada actiu. Aquest és el valor màxim de la taula anterior del punt 4.3 però des de la perspectiva que aplica dels actius. Per veure quins són els riscos que afecta cada amenaça i en quin valor, cal accedir a través de l'eina PILAR i l'arxiu de configuració .car corresponent.

ACTIVOS	4,6	4,6	4,9	5,5	3,4
[essential] Actius essencials	3,7	3,7	3,7	2,8	3,3
[STIC01] Pàgina Web	3,4	3,5	3,5	2,8	3,3
[STIC02] Perfil del Contractant	3,4	3,5	1,7	2,8	3,3
[STIC03] Seu Electrònica	3,4	3,5	3,5	2,8	3,3
[STIC04] Registre entrada sortida	3,4	3,5	3,5	2,8	3,3
[STIC05] ACTIO - Gestor Expedients i Documentació	3,4	3,5	3,5	2,8	3,3
[STIC06] ABSIS - Comptabilitat	3,7	3,7	3,7		

[STIC07] ePADRO Padró d'Habitants	3,4	3,5	3,5	2,8	3,3
[STIC08] PORTAL TRANSPARÈNCIA (Gestió de Subvencions)	3,4	3,5	3,5	2,8	3,3
[STIC09] FUE - Finestra Única Empresarial	3,4	3,5	3,5	2,8	3,3
[STIC10] eFACT - Facturació electrònica	3,4	3,5	3,5	2,8	3,3
[STIC11] eNOTUM - Notificacions electròniques	3,4	3,5	3,5	2,8	3,3
[STIC12] eTAULER - Tauler Electrònic	3,4	3,5	3,5	2,8	3,3
[STIC13] RPC - Registre Públic de Contractes	3,4	3,5	3,5	2,8	3,3
[STIC14] VIA OBERTA - Consulta de Dades Interadministratives	3,4	3,5	3,5	2,8	3,3
[STIC15] EACAT - Extranet Administracions Catalanes	3,4	3,5	3,5	2,8	3,3
[STIC17] Servei Correu Electronic - ALTANET	2,9	2,8	2,8	2,8	3,3
[HW] Equipament informàtic (hardware)	4	4,6	4,9	4,6	
[HW.pc] PCs Ajuntament	4	4,6	4,9	4,6	
[HW.mobile] Portàtils	4	3,7	4,9	4,6	
[HW.peripheral.print] Impresores_Scaner	4	1,9	3,2		
[SRV] SERVIDOR AJUNTAMENT	4	3,7	4,9	4,6	
[HW.backup] BACKUPS	4	4,3	4,9	4,6	
[COM] Xarxes de comunicacions	4,6	4,6	4,9	5,5	3,4
[ISP1] Servei Línia d'Internet	4,6	3,7	3,7	3,7	3,4
[ISP2] Servei línia d'Internet Altanet BA	4,6	3,7	3,7	3,7	3,4
[COM.wifi] WiFi	4,6	4,6	4,9	5,5	
[LAN] XARXA LOCAL	4,6	2,1	3,2	3,7	
[FW] Firewall	4,1	4,6	4,9	5,5	
[Media] Mitjans d'informació	3,7	4,3	3,4		
[Media.electronic.usb] memòries USB	3,7	4,3	3,4		
[Media.non_electronic.printed] material imprès	3,7	4,3	3,4		
[L] Instal·lacions	3,4	1,9	3,2		
[AYTO] Casa consistorial	3,4	1,9	3,2		
[P] Personal	2,6	3,2	3,4		
[P.ui] usuaris interns	2,6	3,2	3,4		
[P.pr] proveïdors	1,9	3,2	3,2		

4.5 Tractament del Risc

Un cop obtinguts els Riscos potencials que afecten a l'Ajuntament de Vilabella, cal realitzar un correcte tractament del risc. Aquest tractament consistirà en dues parts:

- Establir un nivell de risc acceptable
- Tractar els riscos no acceptables / Seleccionar Salvaguardes
- Acceptar els riscos residuals

4.5.1 Nivell de Risc Acceptable

El SGSI de l'Ajuntament de Vilabella, ha decidit considerar que el llindar Màxim de risc acceptable és aquell inferior a 3:

Risc Assumible	<3
Risc no assumible	3 – 5.9
Risc intolerable	6 - 10

Es defineix que per als Riscos de Nivell 1.6 fins a 5, serà obligatori implantar controls/salvaguardes per mitigar el risc.

Es defineix que per als Riscos de nivell 6-10 serà obligatori implantar i auditar els controls/salvaguardes per mitigar, monitoritzar i avaluar el risc.

4.5.2 Selecció de Salvaguardes

Per consultar en més profunditat les salvaguardes de cada classe, cal accedir a l'aplicació **PILAR** a l'apartat:

Análisis Cualitativo → A. Análisis de Riesgo → A.5 Medidas técnicas y organizativas: Seguridad de la Información → A.5.1 valoración (dominios).

4.5.3 Nivell de Risc Residual

Un cop s'apliquen els controls i salvaguardes per mitigar els riscos, quedaran una sèrie de Riscos Residuals, ja que els riscos mai s'acaben d'eliminar. Aquest nivells de riscos residuals, queden a un nivell suficientment baix com per a que el SGSI decideixi acceptar-los.

A continuació mostrem els principals Riscos Residuals resultants un cop s'apliquin els controls de l'ANNEX II de l'ENS i les diferents Salvaguardes proposades per el propi PILAR:

Amenaces	[D]	[I]	[C]	[A]	[T]
Valor MAX	0,97	0,96	1,2	1,7	0,72
[N.1] Fuego	0,75				
[N.2] Daños por agua	0,75				
[N.*] Desastres naturales	0,7				
[I.1] Fuego	0,75				
[I.2] Daños por agua	0,75				
[I.*] Desastres industriales	0,75				
[I.3] Contaminación medioambiental	0,64				
[I.4] Contaminación electromagnética	0,37				
[I.5] Avería de origen físico o lógico	0,62				
[I.6] Corte del suministro eléctrico	0,76				
[I.7] Condiciones inadecuadas de temperatura o humedad	0,75				
[I.8] Fallo de servicios de comunicaciones	0,72				
[I.9] Interrupción de otros servicios o suministros esenciales	0,63				
[I.10] Degradación de los soportes de almacenamiento de la información	0,72				
[I.11] Emanaciones electromagnéticas			0,03		
[E.1] Errores de los usuarios	0,07	0,32	0,43		
[E.2] Errores del administrador del sistema / de la seguridad	0,46	0,46	0,46		
[E.3] Errores de monitorización (log)		0,01			
[E.4] Errores de configuración		0,05			
[E.8] Difusión de software dañino	0,4	0,41	0,4		
[E.9] Errores de [re-]encaminamiento			0,35		
[E.10] Errores de secuencia		0,36			
[E.15] Alteración de la información		0,43			

[E.18] Destrucción de la información	0,78				
[E.19] Fugas de información			0,43		
[E.20] Vulnerabilidades de los programas (software)	0,01	0,46	0,45		
[E.21] Errores de mantenimiento / actualización de programas (software)	0,22	0,23			
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	0,77				
[E.24] Caída del sistema por agotamiento de recursos	0,84				
[E.25] Pérdida de equipos	0,77		0,77		
[E.28] Indisponibilidad del personal	0,38				
[A.3] Manipulación de los registros de actividad (log)		0,96			
[A.4] Manipulación de los ficheros de configuración	0,59	0,58	0,58		
[A.5] Suplantación de la identidad		0,81	0,87	0,98	
[A.6] Abuso de privilegios de acceso	0,46	0,63	0,87		
[A.7] Uso no previsto	0,71	0,43	0,43		
[A.8] Difusión de software dañino	0,78	0,78	0,78		
[A.9] [Re-]encaminamiento de mensajes			0,38		
[A.10] Alteración de secuencia		0,38			
[A.11] Acceso no autorizado	0,79	0,79	1,2	1,7	
[A.12] Análisis de tráfico			0,15		
[A.13] Repudio (negación de actuaciones)					0,72
[A.14] Interceptación de información (escucha)			0,44		
[A.15] Modificación de la información		0,93			
[A.18] Destrucción de la información	0,8				
[A.19] Revelación de información			0,74		
[A.22] Manipulación de programas	0,68	0,79	0,78		
[A.23] Manipulación del hardware	0,67		0,64		
[A.24] Denegación de servicio	0,97				
[A.25] Robo de equipos	0,82		0,83		
[A.26] Ataque destructivo	0,76				
[A.27] Ocupación enemiga	0,76				
[A.28] Indisponibilidad del personal	0,58				
[A.29] Extorsión	0,43	0,54	0,68		
[A.30] Ingeniería social (picaresca)	0,38	0,49	0,63		

ANNEX I – AGREUJANTS I ATENUANTS

[base] Ajuntament

[101] Identificació de l'atacant
[101.a] públic en general
[101.c] proveïdor de serveis
[101.d] grups de pressió política / activistes / extremistes
[102] Motivació de l'atacant
[102.a] econòmica (beneficis en diners)
[106] Atracció de l'objectiu
[106.b] objectiu poc atractiu
[104] Motivació de personal intern
[104.c] sobrecarregats de treball
[105] Permisos dels usuaris (drets)
[105.a] es permet l'accés a Internet
[105.b] es permet l'execució de programes sense autorització prèvia
[105.c] es permet la instal·lació de programes sense autorització prèvia
[105.d] es permet la connexió de dispositius extraïbles
[111] Connectivitat del sistema d'informació
[111.d] connectat a Internet

[AOC] Consorci AOC

[101] Identificació de l'atacant
[101.a] públic en general
[101.c] proveïdor de serveis
[101.d] grups de pressió política / activistes / extremistes
[102] Motivació de l'atacant
[102.a] econòmica (beneficis en diners)
[106] Atracció de l'objectiu
[106.b] objectiu poc atractiu
[104] Motivació de personal intern
[104.c] sobrecarregats de treball
[111] Connectivitat del sistema d'informació
[111.d] connectat a Internet
[112] {xor} Ubicació del sistema d'informació
[112.a] dins d'una zona controlada

[DIPTA] Diputació de Tarragona

[101] Identificació de l'atacant
[101.a] públic en general
[101.c] proveïdor de serveis
[101.d] grups de pressió política / activistes / extremistes
[102] Motivació de l'atacant
[102.a] econòmica (beneficis en diners)
[106] Atracció de l'objectiu
[106.b] objectiu poc atractiu
[104] Motivació de personal intern
[104.c] sobrecarregats de treball
[111] Connectivitat del sistema d'informació
[111.d] connectat a Internet
[112] {xor} Ubicació del sistema d'informació
[112.a] dins d'una zona controlada

[GENCAT] Generalitat de Catalunya

[101] Identificació de l'atacant
[101.a] públic en general

[101.c] proveïdor de serveis
[101.d] grups de pressió política / activistes / extremistes
[102] Motivació de l'atacant
[102.a] econòmica (beneficis en diners)
[106] Atracció de l'objectiu
[106.b] objectiu poc atractiu
[104] Motivació de personal intern
[104.c] sobrecarregats de treball
[111] Connectivitat del sistema d'informació
[111.d] connectat a Internet
[112] {xor} Ubicació del sistema d'informació
[112.a] dins d'una zona controlada

SEGURdades

Consultors en protecció de dades personals

Declaració d'Aplicabilitat

Ajuntament de Vilabella

DECLARACIÓ D'APLICABILITAT

ÍNDEX

CONTROL DEL DOCUMENT

Nom del document**:** Declaració d'Aplicabilitat Nombre de Pàgines: 7	
Autor: Jordi Vidal	Revisat per:
Data:	Data:
Aprovat per:	
Classificació de la Informació: **US INTERN**	
Llista de Distribució: COMITÈ STIC	

CONTROL DE VERSIONS

Nº Versió	Autor	Data	Canvis realitzats	Comentaris
1.0	Jordi Vidal	06/12/2020	Versió inicial	

1 INTRODUCCIÓ

La declaració d'aplicabilitat es el conjunt de mesures que son d'aplicació a l'Ajuntament de Vilabella per al compliment de l'Esquema Nacional de Seguretat. El conjunt de mesures dependrà dels nivells de seguretat associats als nivells de seguretat i categoria del Sistema.

2 NIVELLS DE SEGURETAT I CATEGORIA

S'ha determinat per a l'Ajuntament de Vilabella que els nivells i categoria de seguretat del sistema son els següents:

DIMENSIÓ	[D]	[A]	[C]	[I]	[T]	CATEGORÍA
NIVELL ASSIGNAT	MITJANA	MITJANA	MITJANA	MITJANA	MITJANA	**MITJANA**

El resultat de cada dimensió correspon al nivell mes alt obtingut en la valoració per a cadascun dels actius del SGSI mitjançant l'eina PILAR. Al document "**FASE 2 - Categoria del Sistema**", es podrà trobar una relació detallada de la valoració per a cada actiu, servei i domini de seguretat del SGSI.

Els criteris que s'han seguit estan descrits en el document "**FASE 2 - Categoria del Sistema**", on es justifica cadascuna de les categories obtingudes per a cada actiu.

En funció dels anteriors nivells, s'ha determinat si la mesura és d'aplicació o no i, en cas d'aplicar, el nivell d'exigència en la maduresa de la mesura.

Per a la selecció de les mesures de seguretat s'ha tingut en compte el que indica l'annex II Mesures de seguretat en el seu apartat 2, on s'estableix:

1. Per a la selecció de les mesures de seguretat es seguiran els passos següents:

a) Identificació dels tipus d'actius presents.
b) Determinació de les dimensions de seguretat rellevants, tenint en compte el que estableix l'annex I.
c) Determinació del nivell corresponent a cada dimensió de seguretat, tenint en compte el que estableix l'annex I.
d) Determinació de la categoria de sistema, segons el que estableix l'Annex I.
e) Selecció de les mesures de seguretat apropiades d'entre les contingudes en aquest annex, d'acord amb les dimensions de seguretat i els seus nivells, i, per a determinades mesures de seguretat, d'acord amb la categoria de sistema.

Per tant, per a cadascuna de les mesures de seguretat, s'indicarà, les dimensions de seguretat afectades, la seva aplicació per a nivell mitjà, segons sigui el cas, si s'aplica o no, amb la justificació i el document principal de referència on s'explica com es troba implementada la mesura. En cas, d'utilitzar mesures compensatòries s'indicarà en aquest camp.

3 DECLARACIÓ D'APLICABILITAT

A continuació, es mostra la Declaració de Aplicabilitat dels sistemes d'informació propietat de l'Ajuntament de Vilabella:

Dimensions Afectades	CAT B	CAT M	CAT A	CONTROLS ENS	
				Control	Descripció
				MARC ORGANIZATIU	
D I C A T	aplica	=	=	[org.1]	Política de Seguretat
D I C A T	aplica	=	=	[org.2]	Normativa de Seguretat
D I C A T	aplica	=	=	[org.3]	Procediments de Seguretat
D I C A T	aplica	=	=	[org.4]	Procés d'Autorització
				MARC OPERACIONAL	
				PLANIFICACIÓ	
D I C A T	**Aplica***	**+**	**++**	**[op.pl.1]**	**Anàlisis de Riscos***
D I C A T	aplica	+	++	[op.pl.2]	Arquitectura de Seguretat
D I C A T	**Aplica***	**=**	**=**	**[op.pl.3]**	**Adquisició de nous components***
D	**n.a.**	**aplica***	**=**	**[op.pl.4]**	**Dimensionament / Gestió de capacitats***
categoria	n.a.	n.a.	aplica	[op.pl.5]	Componentes certificats
				CONTROL D'ACCÉS	
A T	aplica	=	=	[op.acc.1]	Identificació
I C A T	aplica	=	=	[op.acc.2]	Requisits d'accés
I C A T	**n.a.**	**aplica***	**=**	**[op.acc.3]**	**Segregació de funcions y tasques***
I C A T	aplica	=	=	[op.acc.4]	Procés de gestió de drets d'accés
I C A T	aplica	+	++	[op.acc.5]	Mecanisme d'autenticació
I C A T	aplica	+	++	[op.acc.6]	Accés local (local logon)
I C A T	aplica	+	=	[op.acc.7]	Accés remot (remote login)
				EXPLOTACIÓ	
D I C A T	aplica	=	=	[op.exp.1]	Inventario de actius
D I C A T	aplica	=	=	[op.exp.2]	Configuració de seguretat
D I C A T	n.a.	aplica	=	[op.exp.3]	Gestió de la configuració
D I C A T	aplica	=	=	[op.exp.4]	Manteniment
D I C A T	**n.a.**	**aplica***	**=**	**[op.exp.5]**	**Gestió de canvis***
D I C A T	aplica	=	=	[op.exp.6]	Protecció front a codi nociu
D I C A T	n.a.	aplica	=	[op.exp.7]	Gestió d'incidents
T	**aplica***	**+**	**++**	**[op.exp.8]**	**Registre de l'activitat dels usuaris***
D I C A T	n.a.	aplica	=	[op.exp.9]	Registre de la gestió d'incidents
T	n.a.	n.a.	aplica	[op.exp.10]	Protecció dels registres d'activitat

D I C A T	aplica	+	=	[op.exp.11]	Protecció de claus criptogràfiques
				SERVEIS EXTERNS	
D I C A T	n.a.	aplica	=	[op.ext.1]	Contractació i acords de nivell de servei
D I C A T	n.a.	aplica	=	[op.ext.2]	Gestió diària
D	n.a.	n.a.	aplica	[op.ext.9]	Mitjans alternatius
				CONTINUITAT DEL SERVEI	
D	**n.a.**	**Aplica***	**=**	**[op.cont.1]**	**Anàlisis d'impacte***
D	n.a.	n.a.	aplica	[op.cont.2]	Pla de continuïtat
D	n.a.	n.a.	aplica	[op.cont.3]	probes periòdiques
				MONITORITZACIÓ DEL SISTEMA	
D I C A T	n.a.	aplica	=	[op.mon.1]	Detecció d'intrusió
D I C A T	aplica	+	++	[op.mon.2]	Sistema de mètriques
				MESURES DE PROTECCIÓ	
				INSTALACIONS I INFRAESTRUCTURA	
D I C A T	aplica	=	=	[mp.if.1]	Àrees separades i amb control de l'accés
D I C A T	aplica	=	=	[mp.if.2]	Identificació de les persones
D I C A T	aplica	=	=	[mp.if.3]	Condicionament dels locals
D	aplica	+	=	[mp.if.4]	Energia elèctrica
D	aplica	=	=	[mp.if.5]	Protecció enfront d'incendis
D	**n.a.**	**aplica***	**=**	**[mp.if.6]**	**Protecció en front d'inundacions***
D I C A T	aplica	=	=	[mp.if.7]	Registre d'entrada i sortida d' equipament
D	n.a.	n.a.	aplica	[mp.if.9]	Instal·lacions alternatives
				GESTIÓ DE PERSONAL	
D I C A T	**n.a.**	**aplica***	**=**	**[mp.per.1]**	**Caracterització del lloc de treball***
D I C A T	aplica	=	=	[mp.per.2]	Deures i obligacions
D I C A T	aplica	=	=	[mp.per.3]	Conscienciació
D I C A T	aplica	=	=	[mp.per.4]	Formació
D	n.a.	n.a.	aplica	[mp.per.9]	Personal alternatiu
				PROTECCIÓ DELS EQUIPS	
D I C A T	aplica	+	=	[mp.eq.1]	Lloc de treball buidat
A	n.a.	aplica	+	[mp.eq.2]	Bloqueig del lloc de treball
D I C A T	aplica	=	+	[mp.eq.3]	Protecció d'equips portàtils
D	n.a.	aplica	=	[mp.eq.9]	Mitjans alternatius
				PROTECCIÓ DE LES COMUNICACIONS	
D I C A T	aplica	=	+	[mp.com.1]	Perímetre segur
C	n.a.	aplica	+	[mp.com.2]	Protecció de la confidencialitat

I A	aplica	+	++	[mp.com.3]	Protecció de l'autenticitat i de la integritat
D I C A T	**n.a.**	**n.a.**	**aplica***	**[mp.com.4]**	**Segregació de xarxes***
D	n.a.	n.a.	aplica	[mp.com.9]	Mitjans alternatius
				PROTECCIÓ DELS SUPORTS DE LA INFORMACIÓ	
C	**Aplica***	**=**	**=**	**[mp.si.1]**	**Etiquetat***
I C	n.a.	aplica	+	[mp.si.2]	Criptografia
D I C A T	aplica	=	=	[mp.si.3]	Custodia
D I C A T	aplica	=	=	[mp.si.4]	Transporte
C	**Aplica***	**+**	**=**	**[mp.si.5]**	**Esborrat i destrucció***
				PROTECCIÓ DE LES APLICACIONS INFORMÀTIQUES	
D I C A T	**n.a.**	**Aplica***	**=**	**[mp.sw.1]**	**Desenvolupament d'aplicacions***
D I C A T	aplica	+	++	[mp.sw.2]	Acceptació i posada en servei
				PROTECCIÓ DE LA INFORMACIÓ	
D I C A T	aplica	=	=	[mp.info.1]	Dades de caràcter personal
C	aplica	+	=	[mp.info.2]	Qualificació de la informació
C	n.a.	n.a.	aplica	[mp.info.3]	Xifrat de la informació
I A	aplica	+	++	[mp.info.4]	Firma electrònica
T	n.a.	n.a.	aplica	[mp.info.5]	Segells de temps
C	aplica	=	=	[mp.info.6]	Neteja de documents
D	aplica	=	=	[mp.info.9]	Còpies de seguretat (backup)
				PROTECCIÓ DELS SERVEIS	
D I C A T	aplica	=	=	[mp.s.1]	Protecció del correu electrònic (e-mail)
D I C A T	aplica	=	+	[mp.s.2]	Protecció de serveis i aplicacions web
D	n.a.	aplica	+	[mp.s.8]	Protecció enfront a la denegació de serveis
D	n.a.	n.a.	aplica	[mp.s.9]	Mitjans alternatius

4 CRITERIS D'APLICACIÓ DE MESURES

4.1 [OP.PL.1] Anàlisi de riscos

Seran d'aplicació els requisits de nivell mitjà, en el cas de serveis proporcionats directament per l'Ajuntament.

En el cas de serveis de l'Ajuntament que són proporcionats per l'òrgan competent, seran d'aplicació a el sistema d'informació de l'Ajuntament els requisits de NIVELL BAIX, mentre que, en el sistema d'informació de l'òrgan competent, aquesta mesura estarà aplicada al disposar aquest de la conformitat ENS en categoria MITJANA.

4.2 [OP.PL.3] Adquisició de nous components

Seran d'aplicació els requisits de categoria MITJANA, en el cas de serveis proporcionats directament per l'Ajuntament.

En el cas de serveis de l'Ajuntament que són proporcionats per l'òrgan competent, no són aplicables a el sistema d'informació de l'Ajuntament, mentre que en el sistema d'informació de l'òrgan competent aquesta mesura estarà aplicada al disposar aquest de la conformitat ENS en categoria MITJANA .

4.3 [OP.PL.4] Dimensionament / Gestió de capacitats

Seran d'aplicació els requisits de nivell MITJÀ, en el cas de serveis proporcionats directament per l'Ajuntament.

En el cas de serveis de l'Ajuntament que són proporcionats per l'òrgan competent, no són aplicables a el sistema d'informació de l'Ajuntament, mentre que en el sistema d'informació de l'òrgan competent aquesta mesura estarà aplicada al disposar aquest de la conformitat ENS en categoria MITJANA .

4.4 [OP.ACC.3] Segregació de funcions i tasques

Seran d'aplicació els requisits de nivell MITJÀ, en el cas de serveis proporcionats directament per l'Ajuntament.

En el cas de serveis de l'Ajuntament que són proporcionats per l'òrgan competent, no són aplicables a el sistema d'informació de l'Ajuntament, mentre que en el sistema d'informació de l'òrgan competent aquesta mesura estarà aplicada al disposar aquest de la conformitat ENS en categoria MITJANA .

4.5 [OP.EXP.5] Gestió de canvis

No són aplicables els requisits de nivell MITJÀ, en el cas de serveis proporcionats directament per l'Ajuntament.

En el cas de serveis de l'Ajuntament que són proporcionats per l'òrgan competent, no són aplicables a el sistema d'informació de l'Ajuntament, mentre que en el sistema d'informació de l'òrgan competent aquesta mesura estarà aplicada al disposar aquest de la conformitat ENS en categoria MITJANA .

4.6 [OP.EXP.8] Registre d'activitat dels usuaris

Seran d'aplicació els requisits de nivell MITJÀ, en el cas de serveis proporcionats directament per l'Ajuntament.

En el cas de serveis de l'Ajuntament que són proporcionats per l'òrgan competent, seran d'aplicació al sistema d'informació de l'Ajuntament els requisits de nivell BAIX, mentre que en el sistema d'informació de l'òrgan competent aquesta mesura estarà aplicada, al disposar aquest de la conformitat ENS en categoria MITJANA.

4.7 [OP.CONT.1] Anàlisi d'impacte

No són aplicables els requisits de nivell MITJÀ, en el cas de serveis proporcionats directament per l'Ajuntament.

En el cas de serveis de l'Ajuntament que són proporcionats per l'òrgan competent, no són aplicables a el sistema d'informació de l'Ajuntament, mentre que en el sistema d'informació de l'òrgan competent aquesta mesura estarà aplicada al disposar aquest de la conformitat ENS en categoria MITJANA .

4.8 [MP.IF.6] Protecció enfront d'inundacions

No són aplicables els requisits de nivell MITJÀ, en el cas de serveis proporcionats directament per l'Ajuntament.

En el cas de serveis de l'Ajuntament que són proporcionats per l'òrgan competent, no són aplicables a el sistema d'informació de l'Ajuntament, mentre que en el sistema d'informació de l'òrgan competent aquesta mesura estarà aplicada al disposar aquest de la conformitat ENS en categoria MITJANA .

4.9 [MP.PER.1] Caracterització de el lloc de treball

No són aplicables els requisits de nivell MITJÀ, en el cas de serveis proporcionats directament per l'Ajuntament.

En el cas de serveis de l'Ajuntament que són proporcionats per l'òrgan competent, no són aplicables a el sistema d'informació de l'Ajuntament, mentre que en el sistema d'informació de l'òrgan competent aquesta mesura estarà aplicada al disposar aquest de la conformitat ENS en categoria MITJANA .

4.10 [MP.COM.4] Segregació de xarxes

Seran d'aplicació els requisits de nivell ALT, en el cas de serveis proporcionats directament per l'Ajuntament, de la següent forma:

- Els fluxos d'informació es separaran en segments de manera que:
  - El trànsit per la xarxa es segregarà perquè cada equip només tingui accés a la informació que necessita.
  - Si s'utilitzen comunicacions wifi, serà en un segment separat.

En el cas de serveis de l'Ajuntament que són proporcionats per l'òrgan competent, seran d'aplicació a el sistema d'informació de l'Ajuntament els requisits de nivell ALT, en la forma indicada en el paràgraf anterior, mentre que en el sistema d'informació de l'òrgan competent correspondrà a aquest l'aplicació d'aquesta mesura.

4.11 [MP.SI] Protecció dels suports d'informació

Per al conjunt de mesures de "mp.si Protecció dels suports d'informació", són aplicables a nivell MITJÀ i categoria MITJANA, en ambdós casos (serveis proporcionats directament per l'Ajuntament i serveis de l'Ajuntament que són proporcionats per l'òrgan competent) , amb les següents particularitats:

- La mesura "[mp.si.1] Etiquetatge" s'aplicarà als dispositius removibles (CD, DVD, discs extraïbles, pendrives, memòries USB, o altres de naturalesa anàloga) quan aquests continguin informació relacionada amb els serveis dins de l'abast de l'ENS ja els documents (format electrònic i suport paper) que formen part de el Sistema de Gestió de la Seguretat de la Informació (SGSI).
- La mesura "[mp.si.5] Esborrat i destrucció", també serà d'aplicació per als discs durs de l'equipament.

4.12 [MP.SW.1] Desenvolupament d'aplicacions

Seran d'aplicació els requisits de categoria MITJANA, en el cas de serveis proporcionats directament per l'Ajuntament.

En el cas de serveis de l'Ajuntament que són proporcionats per l'òrgan competent, no són aplicables a el sistema d'informació de l'Ajuntament, mentre que en el sistema d'informació de l'òrgan competent aquesta mesura estarà aplicada al disposar aquest de la conformitat ENS en categoria MITJANA .

5 CONFORMITAT DEL RESPONSABLE

El Responsable de Seguretat de l'Ajuntament de Vilabella declara la seva conformitat amb el present declaració d'Aplicabilitat.

<<INCLOURE AQUÍ LA FIRMA DEL RESPONSABLE DE SEGURETAT, INDICANT LA SEVA CONFORMITAT A LO PREVIAMENT INDICAT EN EL DOCUMENT>>.

SEGURdades

Consultors en protecció de dades personals

Informe d'insuficiències ENS

Ajuntament de Vilabella

Índex

1 INTRODUCCIÓ

Aquest document es l'informe d'Insuficiències del compliment de les mesures de l'Annex II del Reial Decret de l'Esquema Nacional de Seguretat que l'Ajuntament de Vilabella te implementats.

Aquesta avaluació és la que atorga una valoració inicial de l'estat d'implantació actual dels esmentats controls o mesures de seguretat, i d'altra banda permet establir l'horitzó de compliment objectiu per a l'Ajuntament de Vilabella en el marc de l'esmentat Reial Decret, i posteriorment servirà per avaluar en les auditories corresponents a la norma part de l'estat actual de la mateixa

Les qüestions plantejades pretenen analitzar la situació de l'Ajuntament de Vilabella quant a la seva implicació en la Seguretat de la Informació.

2 DADES DE L'INFORME

Descripció Auditoria			
ID AUDITORIA	**AENS_CCAC_018**	Dates Auditoria	Novembre 2020
Nom	**FASE 5 - Informe Insuficiències - Vilabella**		
Objectiu de l'Auditoria	- Analitzar i avaluar el grau de maduresa dels controls de l'Annex II de l'ENS. - Identificar desviacions i opcions de millora		
Norma d'aplicació	Real Decret 3/2010 – Esquema Nacional de Seguretat		
Equip Auditor	Jordi Vidal – Amat Altès		
Període Cobert	Exercici 2020		
Metodologia	- Entrevistes amb els principals responsables dels departaments. - Sol·licitud de documents (polítiques, guies, normes, registres de KPIs, procediments, etc) per a l'anàlisi i verificació del compliment dels requisits de la norma. - Revisió de tots els controls de la Declaració d'aplicabilitat		
Tipus	Confidencial		
Destinatari	Comitè STIC		

3 RESUM EXECUTIU

El sistema actual es troba en un grau de maduresa molt inicial ja que manca la definició dels pilars bàsics d'un sistema de gestió com son una bona *Política de Seguretat* i unes *Normes de Seguretat* a seguir per part de tots els usuaris.

En general manca la conscienciació en la importància de la seguretat TIC en el dia a dia dels treballadors ja que es manipulen dades dels ciutadans de confidencials, i s'

Es percep una falta de conscienciació generalitzada sobre la importància que tenen les TIC en les tasques i dades del ciutadà que s'estan manipulant, així de com cal protegir-les durant tot el cicle de vida. Es tendeix a creure que pel fet de ser un ajuntament petit, els riscos son menors i tot es mes "flexible".

En general la falta de formació en les TIC, la falta de personal dedicat i sobretot la manca de disposar d'unes responsabilitats ben definides, fan que les TIC es trobin en cert estat de "deixadesa", amb sistemes sense actualitzar, alguns cops obsolets i amb un estat de configuració que no garanteixen els mínims de seguretat.

4 MODELS

4.1 MADURESA DEL CONTROL

La present auditoria s'ha realitzat segons el Model de Maduresa de Capacitat (CMM) que es descriu a la següent taula:

% efectivitat	CMM	SIGNIFICAT	DESCRIPCIÓ
0%	L0	Inexistent	Carència completa de qualsevol procés que reconeguem. No s'ha reconegut que existeixi cap problema a resoldre.
10%	L1	Inicial	Estat inicial on l'èxit de les activitats dels processos es basa la major part dels cops en un esforç personal. Els procediments son inexistents o localitzats en àrees concretes. No existeixen plantilles definides a nivell corporatiu
50%	L2	Reproduïble però intuïtiu	Els processos similars es porten a terme de manera similar per diferents persones amb la mateixa tasca. Es normalitzen les "bones practiques" en base a l'experiència i al mètode. No hi ha comunicació o entreteniment formal, les responsabilitats queden a càrrec de cada individu. Es depèn del grau de coneixement de cada individu.
90%	L3	Procés Definit	La organització sencera participa al procés. Els processos estan implantats, documentats i comunicats mitjançant entreteniment.
95%	L4	Gestionat i mesurable	Es pot seguir amb indicadors numèrics i estadístics l'evolució dels processos. Es disposa de tecnologia per automatitzar el flux de treball, s'ha de tenir eines per a millorar la qualitat i la eficiència.
100%	L5	Optimitzat	Els processos estan sota constant millora. En base criteris quantitatius es determinen les desviacions més comunes i s'optimitzen els processos.

5 INFORME D'INSUFICIÈNCIES

5.1 Mitjana dels grups de controls

Descripció	Estat Actual	Objectiu
Compliment dels Articles	1,25	3
[org] - Organització	1,67	3

[op.pl] - Planificació	1,00	3
[op.acc] - Control d'Accés	0,50	3
[op.exp] - Explotació	0,00	3
[op.ext] - Serveis Externs	1,00	3
[op.cont] – Continuïtat del Servei	0,00	3
[op.mon]- Monitorització del Sistema	1,00	3
[mp.inf] - Instal·lacions i infraestructura	0,50	3
[mp.per] - Gestió del Personal	0,50	3
[mp.eq] - Mesures de protecció dels equips	1,33	3
[mp.com] - Protecció de les comunicacions	0,00	3
[mp.si] - Protecció dels suports de la informació	0,00	3
[mp.sw] - Protecció de les Aplicacions	0,60	3
[mp.info] - Protecció de la Informacion	1,67	3
[mp.s] - Protecció dels serveis	1,50	3

5.2 Maduresa dels controls

Dimensions								
Afectades	CAT B	CAT M	CAT A	CONTROLS ENS		Model CMM		
				Control	Descripció	Objectiu	Estat	Falta
				MARCO ORGANIZATIVO				
D I C A T	aplica	=	=	[org.1]	Política de Seguridad	3	3	0
D I C A T	aplica	=	=	[org.2]	Normativa de Seguridad	3	0	3

D I C A T	aplica	=	=	[org.3]	Procedimientos de Seguridad	3	1	2
D I C A T	aplica	=	=	[org.4]	Proceso de Autorización	3	1	2
					Media de los controles [org]		1,25	
				MARCO OPERACIONAL				
				PLANIFICACION				
D I C A T	aplica	+	++	[op.pl.1]	Análisis de Riesgos	3	3	0
D I C A T	aplica	+	++	[op.pl.2]	Arquitectura de Seguridad	3	1	2
D I C A T	aplica	=	=	[op.pl.3]	Adquisición de nuevos componentes	3	1	2
D	n.a.	aplica	=	[op.pl.4]	Dimensionamiento / Gestión de capacidades	3	0	3
categoria	n.a.	n.a.	aplica	[op.pl.5]	Componentes certificados	-5	0	-5
					Media de los controles [op.pl]		1,67	
				CONTROL DE ACCESO				
A T	aplica	=	=	[op.acc.1]	Identificación	3	2	1
I C A T	aplica	=	=	[op.acc.2]	Requisitos de acceso	3	1	2
I C A T	n.a.	aplica	=	[op.acc.3]	Segregación de funciones y tareas	3	1	2
I C A T	aplica	=	=	[op.acc.4]	Proceso de gestión de derechos de acceso	3	1	2
I C A T	aplica	+	++	[op.acc.5]	Mecanismo de autenticación	3	1	2
I C A T	aplica	+	++	[op.acc.6]	Acceso local (local logon)	3	1	2
I C A T	aplica	+	=	[op.acc.7]	Acceso remoto (remote login)	3	0	3
					Media de los controles [op.acc]		1,00	
				EXPLOTACION				
D I C A T	aplica	=	=	[op.exp.1]	Inventario de activos	3	1	2
D I C A T	aplica	=	=	[op.exp.2]	Configuración de seguridad	3	1	2
D I C A T	n.a.	aplica	=	[op.exp.3]	Gestión de la configuración	3	0	3
D I C A T	aplica	=	=	[op.exp.4]	Mantenimiento	3	0	3
D I C A T	n.a.	aplica	=	[op.exp.5]	Gestión de cambios	3	1	2
D I C A T	aplica	=	=	[op.exp.6]	Protección frente a código dañino	3	3	0
D I C A T	n.a.	aplica	=	[op.exp.7]	Gestión de incidentes	3	0	3
T	aplica	+	++	[op.exp.8]	Registro de la actividad de los usuarios	3	1	2
D I C A T	n.a.	aplica	=	[op.exp.9]	Registro de la gestión de incidentes	3	0	3
T	n.a.	n.a.	aplica	[op.exp.10]	Protección de los registros de actividad	-5		-5
D I C A T	aplica	+	=	[op.exp.11]	Protección de claves criptográficas	3	3	0
					Media de los controles [op.exp]		1,00	
				SERVICIOS EXTERNOS				
D I C A T	n.a.	aplica	=	[op.ext.1]	Contratación y acuerdos de nivel de servicio	3	1	2
D I C A T	n.a.	aplica	=	[op.ext.2]	Gestión diaria	3	0	3
D	n.a.	n.a.	aplica	[op.ext.9]	Medios alternativos	-5		-5
					Media de los controles [op.ext]		0,50	

				CONTINUIDAD DEL SERVICIO				
D	n.a.	aplica	=	[op.cont.1]	Análisis de impacto	3	0	3
D	n.a.	n.a.	aplica	[op.cont.2]	Plan de continuidad	-5		-5
D	n.a.	n.a.	aplica	[op.cont.3]	Pruebas periódicas	-5		-5
					Media de los controles [op.cont]		0,00	
				MONITORIZACIÓN DEL SISTEMA				
D I C A T	n.a.	aplica	=	[op.mon.1]	Detección de intrusión	3	0	3
D I C A T	aplica	+	++	[op.mon.2]	Sistema de métricas	3	0	3
					Media de los controles [op.mon]		0,00	
				MEDIDAS DE PROTECCIÓN				
				INSTALACIONES E INFRAESTRUCTURA				
D I C A T	aplica	=	=	[mp.if.1]	Áreas separadas y con control de acceso	3	1	2
D I C A T	aplica	=	=	[mp.if.2]	Identificación de las personas	3	1	2
D I C A T	aplica	=	=	[mp.if.3]	Acondicionamiento de los locales	3	0	3
D	aplica	+	=	[mp.if.4]	Energía eléctrica	3	2	1
D	aplica	=	=	[mp.if.5]	Protección frente a incendios	3	1	2
D	n.a.	aplica	=	[mp.if.6]	Protección frente a inundaciones	3	2	1
D I C A T	aplica	=	=	[mp.if.7]	Registro de entrada y salida de equipamiento	3	0	3
D	n.a.	n.a.	aplica	[mp.if.9]	Instalaciones alternativas	-5		-5
					Media de los controles [mp.inf]		1,00	
				GESTIÓN DE PERSONAL				
D I C A T	n.a.	aplica	=	[mp.per.1]	Caracterización del puesto de trabajo	3	0	3
D I C A T	aplica	=	=	[mp.per.2]	Deberes y obligaciones	3	0	3
D I C A T	aplica	=	=	[mp.per.3]	Concienciación	3	1	2
D I C A T	aplica	=	=	[mp.per.4]	Formación	3	1	2
D	n.a.	n.a.	aplica	[mp.per.9]	Personal alternativo	-5		-5
					Media de los controles [mp.per]		0,50	
				PROTECCIÓN DE LOS EQUIPOS				
D I C A T	aplica	+	=	[mp.eq.1]	Puesto de trabajo despejado	3	0	3
A	n.a.	aplica	+	[mp.eq.2]	Bloqueo de puesto de trabajo	3	1	2
D I C A T	aplica	=	+	[mp.eq.3]	Protección de equipos portátiles	3	0	3
D	n.a.	aplica	=	[mp.eq.9]	Medios alternativos	3	1	2
					Media de los controles [mp.eq]		0,50	
				PROTECCIÓN DE LAS COMUNICACIONES				
D I C A T	aplica	=	+	[mp.com.1]	Perímetro seguro	3	1	2
C	n.a.	aplica	+	[mp.com.2]	Protección de la confidencialidad	3	1	2
I A	aplica	+	++	[mp.com.3]	Protección de la autenticidad y de la integridad	3	2	1
D I C A T	n.a.	n.a.	aplica	[mp.com.4]	Segregación de redes	-5		-5
D	n.a.	n.a.	aplica	[mp.com.9]	Medios alternativos	-5		-5

[Document confidencial]
INFORME D'INSUFICIÈNCIES

					Media de los controles [mp.com]		1,33	
				PROTECCIÓN DE LOS SOPORTES DE LA INFORMACIÓN				
C	aplica	=	=	[mp.si.1]	Etiquetado	3	0	3
I C	n.a.	aplica	+	[mp.si.2]	Criptografía	3	0	3
D I C A T	aplica	=	=	[mp.si.3]	Custodia	3	0	3
D I C A T	aplica	=	=	[mp.si.4]	Transporte	3	0	3
C	aplica	+	=	[mp.si.5]	Borrado y destrucción	3	0	3
					Media de los controles [mp.si]		0,00	
				PROTECCIÓN DE LAS APLICACIONES INFORMATICAS				
D I C A T	n.a.	aplica	=	[mp.sw.1]	Desarrollo de aplicaciones	3	0	3
D I C A T	aplica	+	++	[mp.sw.2]	Aceptación y puesta en servicio	3	0	3
					Media de los controles [mp.sw]		0,00	
				PROTECCIÓN DE LA INFORMACION				
D I C A T	aplica	=	=	[mp.info.1]	Datos de carácter personal	3	0	3
C	aplica	+	=	[mp.info.2]	Calificación de la información	3	2	1
C	n.a.	n.a.	aplica	[mp.info.3]	Cifrado de la información	-5		-5
I A	aplica	+	++	[mp.info.4]	Firma electrónica	3	0	3
T	n.a.	n.a.	aplica	[mp.info.5]	Sellos de tiempo	-5		-5
C	aplica	=	=	[mp.info.6]	Limpieza de documentos	3	0	3
D	aplica	=	=	[mp.info.9]	Copias de seguridad (backup)	3	1	2
					Media de los controles [mp.info]		0,60	
				PROTECCIÓN DE LOS SERVICIOS				
D I C A T	aplica	=	=	[mp.s.1]	Protección del correo electrónico (e-mail)	3	0	3
D I C A T	aplica	=	+	[mp.s.2]	Protección de servicios y aplicaciones web	3	5	-2
D	n.a.	aplica	+	[mp.s.8]	Protección frente a la denegación de servicio	3	0	3
D	n.a.	n.a.	aplica	[mp.s.9]	Medios alternativos	-5		-5
					Media de los controles [mp.s]		1,67	

SEGURdades

Consultors en protecció de dades personals

PLA DE MILLORA DE LA SEGURETAT

Ajuntament de Vilabella

[Document confidencial]

Esquema Nacional de Seguretat

Índex

CONTROL DEL DOCUMENT

Nom del document**: FASE 6 - Pla de Millores - Vilabella** Nombre de Pàgines: **21**
Autor: SEGURdades
Data: 1/12/2020
Classificació de la Informació: CONFIDENCIAL
Llista de Distribució: COMITÈ STIC DE L'Ajuntament de Vilabella

1 INTRODUCCIÓ

Per a iniciar la implantació del Sistema de Gestió basat en un model PDCA (*Plan – Do – Check – Act*) ha sigut necessari realitzar les tasques prèvies de les anteriors fases (*Definir Política de Seguretat, Rols i Funcions, Valorar i categoritzar el Sistema, Analitzar els Riscos, Analitzar les insuficiències del sistema*), així es disposa de suficient coneixement del sistema per poder elaborar el present Pla de Millora de la Seguretat.

2 OBJECTE

El propòsit d'aquest document es la de proposar un pla de millores de seguretat a executar per corregir les desviacions de compliment de l'Esquema Nacional de Seguretat.

La responsabilitat de la seva execució i la provisió de recursos recauen sobre l'Ajuntament de Vilabella ja siguin propis o mitjançant externalització. El Responsable de Seguretat s'encarregarà de la supervisió de la seva execució. Les tasques a realitzar s'organitzaran en tres grups:

- **Tasques prioritàries**: tasques que s'han d'afrontar inicialment, ja sigui motivat per l'anàlisi de riscos o perquè presenten un compliment molt baix, o per tractar-se d'algun incompliment normatiu.
- **Tasques d'implantació de l'ENS**: la resta de tasques que es necessari dur a terme per realitzar la implantació efectiva de l'ENS. Per tant, s'aniran revisant i documentant les mesures de seguretat, seguint l'ordre establert en l'Annex II del Real decret de l'ENS. D'aquesta manera, s'anirà implantant el Sistema de Gestió (SGSI) que donarà compliment a aquestes mesures.
- **Tasques periòdiques:** Tasques per a dur a terme aquelles mesures de seguretat que s'han de realitzar de forma periòdica.

NOTA: Les tasques prioritàries mostren a la descripció les tasques de forma orientativa. Cal entrar a analitzar en mes profunditat cadascun dels controls que s'afrontarà durant la tasca. Per obtenir mes informació sobre cada control/mesura de protecció, cal consultar:

- ANEX II del RD 3/2010: https://www.boe.es/buscar/act.php?id=BOE-A-2010-1330
- CCN-STIC 804 - ENS. Guía de implantación.

3 PLA DE MILLORES DE LA SEGURETAT

3.1 Tasques Prioritàries

Llegenda: RINF (Responsable de la Informació); RSER (Responsable del Servei); RSEG (Responsable de Seguretat); RSIS (Responsable del Sistema); CSTIC (Comitè STIC); RSSIM (Responsable de Seguretat dels Sistemes d'Informació Municipals); SC (Sense Cost);

Les següents tasques descrites a continuació s'abordaran de forma prioritària:

Les tasques valorades en hores tindran un cost segons el preu públic dels serveis del Consell Comarcal o el cost que tingui d'externalitzar a tercers.

TASQUES PRIORITÀRIES	CONTROL/CUMPLIMENT	RESPONSABLE	2021	2022	2023	Cost aproximat
Desenvolupar i aprovar la normativa de seguretat dels recursos TIC (correu, internet, etc.) posats a disposició de personal que reguli també, entre altres, l'ús de dispositius portàtils, suports extraïbles, la necessitat que els usuaris bloquegin el seu lloc de treball davant les absències, la necessitat de netejar els documents de metadades no necessaris, la necessitat d'utilitzar xarxes privades virtuals per garantir l'autenticitat i la integritat de la informació abans del seu intercanvi. Desenvolupar un procediment de gestió de personal que descrigui la forma en la qual es traslladen els deures a el personal propi o de tercers. Aprovar formalment i difondre a tot personal: publicació al portal de l'empleat. Elaborar de pla anual de difusió / sensibilització i de formació. -Utilitzar **GUIA CCN-STIC 821 – Apèndix I**	Normativa de seguretat [org.2] Deures i obligacions [mp.per.2] Lloc de treball buidat [mp.eq.1] Bloqueig de lloc de treball [mp.eq.2] Protecció de dispositius portàtils [mp.eq.3] Protecció dels suports [mp.si] Neteja de metadades [mp.info.6] Protecció de l'autenticitat i de la integritat [mp.com.3]	CSTIC	X			5H

PLA DE MILLORES

TASQUES PRIORITÀRIES	CONTROL/CUMPLIMENT	RESPONSABLE	2021	2022	2023	Cost aproximat
Definir un pla de Formació anual per als treballadors en especial èmfasi en els Responsables de l'ENS per a la correcte operació del SGSI. Aprofitar el Pla de formació Anual de Diputació de Tarragona i completar-lo amb tasques pròpies. Incloure en el Pla de Formació les sessions de conscienciació en matèria de seguretat i definir el contingut. En les sessions de conscienciació incloure informació de la normativa de seguretat (definida al punt anterior) relacionat amb els usuaris i la operació diària.	Conscienciació [mp.per.3] Formació [mp.per.4]	CSTIC	X			500€
Revisar el procediment de còpies i assegurar-se que les polítiques implementades donen suport tota la informació, aplicacions, logs, etc. En cas de serveis externalitzats: completar amb procediments documentats proporcionats per l'òrgan competent de la política de còpies de seguretat i de restauració.	Còpies de seguretat (backup) [mp.info.9]	CSTIC	X			0-600€
Revisar les mesures de protecció enfront de codi nociu, en tot l'equipament inclòs: PCS, portàtils, etc. Es recomana implementar les solucions de mesures EDR (Endpoint Defense and Response) que indica diputació així. Desenvolupar un procediment que descrigui la forma en qual es gestiona i es manté la solució de protecció enfront de codi nociu segons les indicacions de Diputació de Tarragona.	Protecció contra codi nociu [op.exp.6]	CSTIC	x			0-50€

TASQUES PRIORITÀRIES	CONTROL/CUMPLIMENT	RESPONSABLE	2021	2022	2023	Cost aproximat
Segmentar les xarxes de tal manera que cada equip només tingui accés a la informació que necessita, es compartimenten els diferents grups d'usuaris per evitar la propagació de malware i les xarxes sense fils disposi del seu propi segment de xarxa. Desenvolupar els procediments associats. *Nota: El Wifi es el punt mes feble dels Ajuntaments petits. Per tant, en els ajuntaments mes petits on no existeixen ni VLANs ni segmentació de xarxa cal aïllar i fortificar les Wifis tractant de:* - La xarxa Wifi no ha de tenir accés a la LAN dels PCs. - Adquirir un AP Wifi i connectar-lo directament o al tallafocs o al router del proveïdor ISP - Deshabilitar la wifi per defecte dels Routers (movistar, Vodafone, etc). - Si per algun motiu s'ha de mantenir algun wifi per que hi ha algun portàtil i no es possible connectar per cable, ocultar el BSSID del WIFI, activar filtrat per MAC i configurar el portàtil per a que pugui seguir funcionant.	Segregació de xarxes [mp.com.4]	CSTIC	X	X		200€
Assegurar-se que tots els usuaris o processos disposen d'un identificador únic. Establir un "període de retenció" dels comptes. Desenvolupar un procediment de control d'accés detallant els mecanismes d'identificació implementats En cas de serveis externalitzats: completar amb els procediments documentats proporcionats per l'òrgan competent de configuració de rols / perfils d'accés als serveis	Identificació [op.acc.1]	CSTIC	X			0-300€
Ficar ordre a les carpetes compartides i documents compartits. Definir carpetes per departaments i configurar Grups de Seguretat (OU) Moure tota la informació important dels "escriptoris locals" a les carpetes corporatives.		CSTIC	X			0-5H

PLA DE MILLORES

TASQUES PRIORITÀRIES	CONTROL/CUMPLIMENT	RESPONSABLE	2021	2022	2023	Cost aproximat
Organitzar, completar i mantenir actualitzada documentació sobre: àrees i punts d'accés (plànols físics); a nivell de sistema, línies de defensa, identificació i autenticació, controls tècnics, relacions amb tercers, perquè formin part de l'SGSI. En cas de serveis externalitzats: completar amb la documentació proporcionada per l'òrgan competent sobre les comunicacions amb l'Ajuntament, i amb altres sistemes interconnectats comunicacions amb l'Ajuntament, i amb altres sistemes interconnectats	Arquitectura de Seguretat [op.pl.2]	CSTIC	X			0-5H
Desenvolupar i implementar una política d'accés desenvolupant un procediment de gestió dels drets d'accés complint el requisit de "mínim privilegi". Realitzar controls aleatoris de compliment. Registrar aquestes accions i els seus resultats. Desenvolupar un procediment de gestió dels drets d'accés, que garanteixi que s'assignen els mínims privilegis i que són acords als establerts per al control Requisits d'accés [op.acc.2] i establir tasques periòdiques de revisió dels permisos atorgats. En cas de serveis externalitzats: completar amb els procediments documentats proporcionats per l'òrgan competent de configuració de rols / perfils d'accés als serveis	Requisits d'accés [op.acc.2] Procés de gestió dels drets d'accés [op.acc.4]	CSTIC	X			0-5H
Desenvolupar Instruccions Tècniques de configuració segura (enduriment) dels principals components de sistema: equipament (seguretat perimetral, electrònica de xarxa, servidors (físics, virtuals), bases de dades), equips d'usuaris (PC, portàtils, Smartphone, pastilles), dispositius connectats a la xarxa (impressores, etc.). Migrar els sistemes obsolets (Windows XP, Windows 7, 2008 Server, Servidors Fisics Antics com HPE sens suport, etc.) a sistemes que disposin de suport de seguretat dels fabricants.	Configuració de seguretat [op.exp.2] Gestió de la configuració [op.exp.3] Protecció d'equips portàtils [mp.eq.3]	CSTIC	X	X	X	0-5000€
Identificar els mecanismes d'autenticació de cada recurs i documentar com es troba implementat el doble factor d'autenticació. Desenvolupar el procediment associat. Si s'utilitzen contrasenyes: utilitzar contrasenyes segures, definir una política de caducitat. **En cas de serveis externalitzats**: completar amb procediments documentats proporcionats per l'òrgan competent dels mecanismes d'autenticació d'accés als serveis	Mecanisme d'autenticació [op.acc.5]	CSTIC	X	X		2H-??

TASQUES PRIORITÀRIES	CONTROL/CUMPLIMENT	RESPONSABLE	2021	2022	2023	Cost aproximat
Establir i procedimentar com realitzar els accessos remots (teletreball). Inventariar els accessos remots (inclosos els WIFI de l'Ajuntament). Realitzar un procediment que permeti mantenir aquest inventari, com s'autoritzen, etc. Realitzar unes normes per als accessos remots que regulen les condicions en les quals ha de realitzés aquest accés. Revisar que els accessos remots, es realitzen, implementant doble factor d'autenticació. Revisar configuracions del WIFI local i garantir que l'accés es únicament per les persones autoritzades. Realitzar un procediment que descrigui la forma en la qual es protegeix la confidencialitat de la informació que fa aquesta discorre per xarxes fora del propi domini de seguretat. Consultar guies: - CCN-CERT BP/18 Recomendaciones de seguridad para situaciones de teletrabajo y refuerzo en vigilancia - Guía CCN-STIC-807 Criptografía de empleo en el ENS - Guía CCN-STIC-827 - Gestión y uso de dispositivos móviles - Guía CCN-STIC-406 - Seguridad en Redes Inalámbricas - Guía CCN-STIC-416 - Seguridad en redes privadas virtuales	Accés remot (remote login) [op.acc.7] Protecció de la confidencialitat. [mp.com.2] Protecció de l'autenticitat i de la integritat [mp.com.3)	CSTIC	X	X		10-15H --------- 500-700€ PER PORTÀTIL A determinar costos llicencies VPN
Desenvolupar i implantar un procediment de gestió de la seguretat amb tercers: abans, durant i després de la contractació: Requisits de solvència tècnica. Exigència de declaració / certificació de conformitat amb l'ENS, contractes d'encarregat de tractament de dades personals i / o confidencialitat, acords de nivell de servei, etc. Inventariar tercers i regular la seva situació.	Contractació i acords de nivell de servei [op.ext.1] Gestió diària [op.ext.2]	CSTIC	x			5H

TASQUES PRIORITÀRIES	CONTROL/CUMPLIMENT	RESPONSABLE	2021	2022	2023	Cost aproximat
Instal·lar l'eina Lucia eina desenvolupada pel CCN-CERT per a la Gestió de Ciberincidents Desenvolupar un procediment integral de gestió d'incidents de seguretat amb les obligacions establertes per l'ENS i RGPD. **En cas de serveis externalitzats**: completar amb els procediments documentats de coordinació amb l'Ajuntament per a la gestió incidents i de comunicació dels mateixos a les autoritats de control.	Gestió d'incidents [op.exp.7] Registre de la gestió d'incidents [op.exp.9]	CSTIC	X			2H
Configura les directives d'accés al domini de manera que: • S'estableixi una limitació d'intents d'accés. • Només es mostri informació, un cop validat en el domini, per tant, no es guardarà la informació de l'últim usuari validat. • S'informa a l'usuari de les seves obligacions. • Es mostri la informació sobre l'última entrada amb èxit i els possibles intents d'accés. **En cas de serveis externalitzats**: completar amb procediments documentats proporcionats per l'òrgan competent de configuració dels requisits del control: limitació d'intents d'accés, avís d'obligacions, informació sobre l'última entrada	Accés local (local logon) [op.acc.6]	CSTIC	X	X		5H

TASQUES PRIORITÀRIES	CONTROL/CUMPLIMENT	RESPONSABLE	2021	2022	2023	Cost aproximat
Implementar un mecanisme d'accés al CPD que permeti identificar les persones (inclòs l'accés de tercers). Desenvolupar el procediment associat. Revisar les mesures de condicionament del CPD. Implantar un registre d'entrada / sortida d'equipament al CPD. Desenvolupar el procediment associat. Nota: Si no existeix el CPD i no es possible aïllar el servidor de cap de les maneres tractar de: Ficar el Servidor a l'armari de comunicacions Si no hi cap el servidor a l'armari, tractar de comprar-ne un de 22U. Tancar l'armari amb clau SEMPRE i guardar-la en lloc segur Realitzar el registre de persones cada cop que es demana la clau per fer alguna acció a l'armari sigui qui sigui. Pentinar l'armari i eliminar tots els dispositius innecessaris Etiquetar i identificar tots els actius i cables.	Identificació de les persones [mp.inf.2] Condicionament dels locals [mp.if.3] Registre d'entrada i sortida d'equipament [mp.if.7]	CSTIC		X		15H Armari Rack 300€ Aprox

TASQUES PRIORITÀRIES	CONTROL/CUMPLIMENT	RESPONSABLE	2021	2022	2023	Cost aproximat
Habilitar registres de les activitats dels usuaris realitzades sobre els servidors, de manera que Indiqui qui les realitza, quan i sobre quina informació. Desenvolupar procediment associat. Especialment els dels administradors de sistema per monitoritzar la seva activitat com a mesura compensatòria de op.acc.3. **En cas de serveis externalitzats**: completar amb procediments documentats de configuració dels registres d'activitat dels usuaris als serveis Informació / plataforma de visualització proporcionada per l'òrgan competent dels accessos dels administradors de sistema que suporta els serveis (en cas que s'hagin requerit) Es recomana Implantar un sistema automàtic de recollida d'esdeveniments de seguretat. Valorar que permeti la correlació dels mateixos. (Eina GLÒRIA CCN) Consultar Guía CCN-STIC-434 - Herramientas para el análisis de ficheros de log	Registres de l'activitat dels usuaris [op.exp.8]	CSTIC		X	X	5H
Recopilar els procediments documentats proporcionats per l'òrgan competent de coordinació amb l'Ajuntament per a la realització de proves d'acceptació i posada en servei. Informes resultats proves i pla d'acció i els informes proporcionats per l'òrgan competent amb resultats de les inspeccions periòdiques realitzades i pla d'acció.	Acceptació i posada en servei [mp.sw.2] Protecció dels serveis i aplicacions web [mp.s.2]	CSTIC		X	X	SC

3.2 Tasques d'implantació de l'ENS

Durant els 2 Anys següents es procedirà a implantar i documentar la resta de mesures de protecció que ens apliquen al nostre sistema.

TASQUES	CONTROL	RESPONSABLE	2021	2022	2023
MARC ORGANITZATIU					
NORMATIVA D'SEGURETAT- (INCLÒS EN MESURES PRIORITZADES)	org.2				
PROCEDIMENTS DE SEGURETAT- Desenvolupar procediments operatius que recullin les principals tasques sobre el sistema. Indicant els responsables de la seva realització i com identificar i reportar comportaments anòmals. Integrar en un Sistema de Gestió de Seguretat de la Informació que de suport a l'acompliment de l'ENS. (SGSIENS)	org.3	RSEG RSIS	X	X	X
PROCESSOS D'AUTORITZACIÓ- Implantar i documentar un procés d'autorització per a la introducció d'elements en el sistema: instal·lacions, equips, aplicacions, mitjans de comunicació, utilització de suports, portàtils, mòbils, etc. i serveis de tercers.	org.4	RSIS		X	X
MARC OPERACIONAL - PLANIFICACIÓ					
ANÀLISI DE RISCOS ENS - (INCLÒS EN MESURES PRIORITZADES).Desenvolupar el procediment d'anàlisi de riscos d'acord a la categoria de sistema	op.pl.1	RSEG RSIS	X	X	X
ARQUITECTURA DE SEGURETAT - (INCLÒS EN MESURES PRIORITZADES) - Recopilar, organitzar, completar i mantenir actualitzada documentació sobre: àrees i punts d'accés, de sistema, línies de defensa, identificació i autenticació, controls tècnics, relacions amb tercers, perquè formin part de l'SGSENS. En cas de serveis externalitzats: completar amb la documentació proporcionada per l'òrgan competent sobre les comunicacions amb l'Ajuntament, i amb altres sistemes interconnectats comunicacions amb l'Ajuntament, i amb altres sistemes interconnectats	op.pl.2	RSIS	X		

TASQUES	CONTROL	RESPONSABLE	2021	2022	2023
ADQUISICIÓ DE NOUS COMPONENTS- Aquest control no es aplicable als ajuntaments si no tenen els serveis propis, per tant no caldrà implementar tots els requisits del control, només s'aconsella definir un estàndard de compres des de consell comarcal per a PCs, Servidor, switchos, Telefonia). Implantar un procediment que analitzi els riscos, avaluï la necessitat de requisits abans de l'adquisició de nous components. Registrar aquestes accions i els seus resultats.	op.pl.3	RSIS			X
DIMENSIONAMENT I GESTIÓ DE LA CAPACITAT – Si no tenen serveis propis, no aplica **En cas de que disposin serveis propis:** Implantar un procediment per a la realització d'un estudi d'aquests paràmetres abans de l'entrada en producció de nous elements. **En cas de serveis externalitzats**: completar amb la documentació regular proporcionada per l'òrgan competent sobre els recursos disponibles i consumits	op.pl.4	RSIS		X	
MARC OPERACIONAL - CONTROL D'ACCÉS					
IDENTIFICACIÓ- (INCLÒS EN MESURES PRIORITZADES)	op.acc.1				
REQUISITS ACCÉS- (INCLÒS EN MESURES PRIORITZADES)	op.acc.2				
PROCÉS DE GESTIÓ DELS DRETS DE ACCÉS- (INCLÒS EN MESURES PRIORITZADES).	op.acc.4	RIS			
MECANISMES DE AUTENTICACIÓN- (INCLÒS EN MESURES PRIORITZADES).	op.acc.5	RIS			
ACCÉS LOCAL (LOCAL LOGON) - (INCLÒS EN MESURES PRIORITZADES).	op.acc.6	RIS			
ACCÉS REMOT (REMOTE LOGIN) - (INCLÒS EN MESURES PRIORITZADES).	op.acc.7	RIS			
MARC OPERACIONAL - EXPLOTACIÓ					

PLA DE MILLORES

TASQUES	CONTROL	RESPONSABLE	2021	2022	2023
INVENTARI D'ACTIUS- Desenvolupar un procediment que descrigui la forma en què es gestionen els actius. Realitzar un inventari de programari (es recomana utilitzar una eina que faci un inventari d'actius maquinari, programari de forma automàtica).	op.exp.1	RIS		X	
CONFIGURACIÓ DE SEGURETAT) - (INCLÒS EN MESURES PRIORITZADES). Elaborar un procediment d'enduriment que reculli la configuració bàsica de seguretat de l'equipament (seguretat perimetral, electrònica de xarxa, servidors (físics, virtuals), bases de dades), equips d'usuaris (PC, portàtils, Smartphone, pastilles), dispositius connectats a la xarxa (impressores, etc.), abans d'entrar en operació.	op.exp.2	RIS		X	X
GESTIÓ DE LA CONFIGURACIÓ DE SEGURETAT- (INCLÒS EN MESURES PRIORITZADES). Establir revisions periòdiques de la configuració de la seguretat: identificar vulnerabilitats, incidències, etc. Registrar aquestes accions i els seus resultats.	op.exp.3	RIS			X
MANTENIMENT- Documentar totes les accions de manteniment (físic i lògic). Registrar aquestes accions i els seus resultats. Desenvolupar un procediment per analitzar, prioritat l'aplicació d'actualitzacions de seguretat, errors, millores, etc. EN CAS DE SERVEIS EXTERNALITZATS: completar amb procediments documentats de coordinació amb l'Ajuntament per realitzar accions de manteniment sobre el sistema que	op.exp.4	RIS		X	X
GESTIÓ DE CANVIS No s'haurà de fer res per als serveis interns de l'Ajuntament. -EN CAS DE SERVEIS EXTERNALITZATS: recopilar la informació aportada pel l'òrgan competent de coordinació amb l'Ajuntament per realitzar canvis sobre el sistema que suporta els serveis	op.exp.5	RIS		X	X
PROTECCIÓ DAVANT CODI DAÑINO- (INCLÒS EN MESURES PRIORITZADES).	op.exp.6	RIS			
GESTIÓ DE INCIDENTES- (INCLÒS EN MESURES PRIORITZADES).	op.exp.7	RIS			
REGISTRE DE L'ACTIVITAT DELS USUARIS - [INCLÒS EN MESURES PRIORITZADES}	op.exp.8	RIS			

TASQUES	CONTROL	RESPONSABLE	2021	2022	2023
REGISTRE DE LA GESTIÓ DE INCIDENCIAS- (INCLÒS EN MESURES PRIORITZADES).	op.exp.9	RIS			
PROTECCIÓ DE LES CLAUS CRIPTOGRÀFIQUES- Documentar les mitjanes de seguretat implementades per garantir la protecció de les claus criptogràfiques durant tot el seu cicle de vida. Per a sistemes de categoria mitjana s'ha d'assegurar la utilització de programes avaluats o dispositius criptogràfics avaluats que empren algoritmes acreditats pel CCN. EN CAS DE SERVEIS EXTERNALITZATS: completar amb procediments documentats de protecció de les claus criptogràfiques de l'Ajuntament que es trobin allotjades en el sistema que suporta els serveis	op.exp.11	RIS		X	
MARC OPERACIONAL - SERVEIS EXTERNS					
CONTRACTACIÓ I ACORDS DE NIVELL DE SERVEI - (INCLÒS EN MESURES PRIORITZADES)	op.ext.1	RIS		X	
GESTIÓ DIÀRIA - (INCLÒS EN MESURES PRIORITZADES)	op.ext.2	RIS		X	
MARC OPERACIONAL - MONITORITZACIÓ DEL SISTEMA					
DETECCIÓ D'INTRUSIÓ Verificar amb diputació de Tarragona si els Fortinet disposen de funcionalitat IDS i qui ho gestiona. Instal·lar un IDS de xarxa si no ho fa Diputació.	op.mon.1	RIS		X	X
MARC OPERACIONAL - SITEMA DE MÈTRIQUES					
SISTEMA D'MÈTRIQUES - Realitzar un procediment que estableixi els indicadors, mètrica associada i designació de responsables per a la seva recopilació dels elements per donar resposta a l'enquesta INES (re-querit per l'article 35).	op.mon.2	RIS		X	
MARC DE PROTECCIÓ - PROTECCIÓ DE LES INSTAL·LACIONS I INFRAESTRUCTURES					

PLA DE MILLORES

TASQUES	CONTROL	RESPONSABLE	2021	2022	2023
ÀREES SEPARADES I CONTROL D'ACCÉS- Realitzar un procediment que continguin un inventari de totes les àrees on es concentra el sistema d'informació i que detall els mecanismes implementats en cada cas per controlar l'accés a les mateixes i les autoritzacions pertinents en cas que sigui necessari	mp.if.1	RIS	X	X	
IDENTIFICACIÓ LES PERSONES- (INCLÒS EN MESURES PRIORITZADES).	mp.if.2	RIS		X	
CONDICIONAMENT DELS LOCALS- Documentar les mesures implementades per assegurar el condicionament de l'CPD: sensors de temperatura, humitat, protecció del cablejat, etc. Com es monitoritzen i responsables. - (inclòs en mesures prioritzades).	mp.if.3	RIS	X	X	
ENERGIA ELÈCTRICA- Documentar les mesures implementades per garantir el subministrament elèctric al CPD. En cas que sigui d'aplicació descriure les mesures addicionals implementades (SAI, grup electrònic, la forma i quan entren en funcionament, proves de contingència realitzades per determinar els càlculs de temps.)	mp.if.4	RIS		X	X
PROTECCIÓ DAVANT INCENDIS- Desenvolupar un procediment que reculli la forma en la qual es protegeixen els locals d'acord amb la normativa industrial, la ubicació dels cartells, extintors, materials no inflamables, etc. Els controls periòdics realitzats, etc. Mantenir de forma centralitzada tota la documentació relacionada mantenir de forma centralitzada tota la documentació relacionada)	mp.if.5	RIS	X	X	X
REGISTRE D'ENTRADA I SORTIDA DE EQUIPAMENT- (INCLÒS EN MESURES PRIORITZADES)	mp.if.7	RIS			
MARC DE PROTECCIÓ - GESTIÓ DE PERSONAL					
CARACTERITZACIÓ DE EL LLOC DE TREBALL	Mp.per.1	RIS		X	X
DEURES I OBLIGACIONS- (INCLÒS EN MESURES PRIORITZADES)Desenvolupar un procediment de gestió de personal que descrigui la forma en la qual es traslladen els deures a el personal propi o de tercers.	mp.per.2	RIS	X		

TASQUES	CONTROL	RESPONSABLE	2021	2022	2023
CONCIENCIACIÓN- (INCLÒS EN MESURES PRIORITZADES) Desenvolupar un procediment que descrigui la com es desenvoluparà el Pla Conscienciació en matèria de seguretat de la informació per a tot el personal, amb periodicitat anual. (INCLÒS TAMBÉ EN MESURES PERIODICITAT ANUAL)	mp.per.3	RIS	X		
FORMACIÓ-(INCLÒS EN MESURES PRIORITZADES) Desenvolupar un procediment que descrigui la com es desenvoluparà el Pla de Formació específic en seguretat de la informació per al personal amb responsabilitat en l'operació de el sistema, amb periodicitat anual. (INCLÒS TAMBÉ EN MESURES PERIODICITAT ANUAL)	mp.per.4	RIS	x		
MARC DE PROTECCIÓ - PROTECCIÓ DELS EQUIPS					
LLOC DE TREBALL NET - (INCLÒS EN MESURES PRIORITZADES) Obligació recollida a la Normativa de seguretat [org.2]	mp.eq.1	RIS	X		
BLOQUEIG DE LLOC DE TREBALL- (INCLÒS EN MESURES PRIORITZADES) Obligació recollida a la Normativa de seguretat [org.2]	mp.eq.2	RIS	X		
PROTECCIÓ DELS EQUIPS PORTÀTILS-- (INCLÒS EN MESURES PRIORITZADES) Desenvolupar un procediment que descrigui la forma en què fer l'inventari dels equips portàtils (inclòs Smartphones, tabletes, etc.)	mp.eq.3	RIS	X		
MARC DE PROTECCIÓ - PROTECCIÓ DE LES COMUNICACIONS					
PERÍMETRE SEGUR- Documentar la seguretat perimetral i les excepcions implementades en els tallafocs. Procés d'autorització i que descrigui la separació de fluxos implementada. NOTA: els ajuntaments que encara no disposin del tallafocs de diputació, ficar-se en contacte amb el consell comarcal i diputació per fer la correcte instal·lació	mp.com.1	RIS	x		

PLA DE MILLORES

TASQUES	CONTROL	RESPONSABLE	2021	2022	2023
PROTECCIÓ DE LA CONFIDENCIALITAT- Realitzar un procediment que descrigui la forma en la qual es protegeix la confidencialitat de la informació que fa aquesta discorre per xarxes fora del propi domini de seguretat. EN CAS DE SERVEIS EXTERNALITZATS: completar amb documents proporcionats per l'òrgan competent amb informació sobre els mecanismes de xifrat implementats en les comunicacions.	mp.com.2	RIS	X		
PROTECCIÓ DE L'AUTENTICITAT I DE LA INTEGRITAT - Realitzar un procediment / norma que estableixi la necessitat d'utilitzar xarxes privades virtuals per garantir l'autenticitat i la integritat de la informació abans del seu intercanvi. EN CAS DE SERVEIS EXTERNALITZATS: completar amb documents proporcionats per l'òrgan competent amb informació sobre els mecanismes implementats per protegir l'autenticitat i de la integritat	mp.com.3	RIS	x		
SEGMENTACIÓ DE XARXES - (INCLÒS EN MESURES PRIORITZADES)	mp.com.4	RIS			
MARC DE PROTECCIÓ - PROTECCIÓ DELS SUPORTS D'INFORMACIÓ					
ETIQUETATGE - Desenvolupar un procediment per a l'etiquetatge de suports extraïbles d'acord amb la qualificació de la informació que contenen. Difondre a el personal afectat.	mp.si.1	RIS		X	
CRIPTOGRAFÍA - Desenvolupar un procediment que descrigui la forma en què s'aplicaran mecanismes de xifrat als suports d'informació. Difondre a el personal afectat.	mp.si.2	RIS		X	
CUSTÒDIA- Desenvolupar un procediment per a la custòdia de suports d'informació. Difondre a el personal afectat.	mp.si.3	RIS		X	
TRANSPORT- - (EN CAS QUE APLIQUI) Desenvolupar un procediment que descrigui les mesures de seguretat a aplicar durant el transport als suports d'informació. Difondre a el personal afectat.	mp.si.4	RIS		X	
ESBORRAT I DESTRUCCIÓ- Desenvolupar un procediment que descrigui el procediment a seguir per a l'esborrat i destrucció en funció de el suport. Elaborar instrucció tècnica d'esborrat i de destrucció	mp.si.5	RIS		X	
MARC OPERACIONAL - PROTECCIÓ DE LES APLICACIONS INFORMÀTIQUES					
DESENVOLUPAMENT- -(EN CAS QUE APLIQUI) (INCLÒS EN MESURES PRIORITZADES)	mp.sw.1	RIS			

PLA DE MILLORES

TASQUES	CONTROL	RESPONSABLE	2021	2022	2023
ACCEPTACIÓ I POSADA EN SERVEI- (EN CAS QUE APLIQUI) (INCLÒS EN MESURES PRIORITZADES)	mp.sw.2	RIS			
MARC OPERACIONAL - PROTECCIÓ DE LA INFORMACIÓ					
DADES DE CARÀCTER PERSONAL - Desenvolupar les accions de seguretat necessàries per a dur a terme la implantació de la normativa de protecció de dades (RAT, designació DPD, Anàlisi de Regs RGPD, Avaluació d'Impacte, contractes d'encarregat de tractament, alinear mesures de seguretat amb les de l'ENS) . EN CAS DE SERVEIS EXTERNALITZATS: recopilar documents / plataformes en línia, proporcionats per l'òrgan competent, amb evidències de compliment de la normativa de protecció de dades	mp.info.1	RIS	X	X	X
QUALIFICACIÓ DE LA INFORMACIÓ - Desenvolupar i implantar un procediment de qualificació de la informació. Elaborar procediments que defineixin la manera que cal tractar la documentació en consideració a el nivell de seguretat requerit	mp.info.2	RIS			
SIGNATURA ELECTRÒNICA Desenvolupar, aprovar i donar publicitat a la Política de Signatura Electrònica. Realitzar un procediment que reculli els requisits que han de complir els mecanismes de signatura electrònica EN CAS DE SERVEIS EXTERNALITZATS: completar amb documents proporcionats per l'òrgan competent amb informació sobre les mesures de protecció de la signatura implementades	mp.info.4	RIS			X
NETEJA DE DOCUMENTS- Desenvolupar i implantar un procediment on s'estableixi la forma en la qual s'ha de procedir per a la neteja dels documents electrònics.	mp.info.6	RIS			X
CÒPIA DE SEGURETAT- (INCLÒS EN MESURES PRIORITZADES)	mp.info.9	RIS			
MARC OPERACIONAL - PROTECCIÓ DELS SERVEIS					
PROTECCIÓ DEL CORREU ELECTRÒNIC-(EN CAS QUE APLIQUI) Desenvolupar un procediment que descrigui la forma en la qual es protegeix el correu.	mp.s.1	RIS		X	
PROTECCIÓ DE SERVEIS I APLICACIONS WEB -(EN CAS QUE APLIQUI) - (INCLÒS EN MESURES PRIORITZADES)	mp.s.2	RIS		X	

PLA DE MILLORES

[Document confidencial]
Esquema Nacional de Seguretat

3.3 Tasques periòdiques

TASQUES PERIODICITAT ANUAL	CONTROL	PERIODICITAT
Revisió de la Política de Seguretat de la Informació	Política de Seguretat de la Informació [org.1]	Anual
Elaboració de el Pla de Conscienciació i Pla de Formació	Conscienciació [mp.per.3] Formació [mp.per.4]	Anual
Revisió de la Normativa de seguretat,	Normativa de seguretat [org.2]	Anual
Revisió de la Informació i el Serveis, la seva valoració i procés de categorització de sistema	Article 43. Categories i 44. Facultats de el Reial Decret ENS	Permanent
Actualització de l'anàlisi de riscos	Anàlisi de riscos [op.pl.1]	Anual / canvis rellevants
Revisió de la Declaració d'aplicabilitat o del Perfil de Compliment	Article 27. Compliment de requisits mínims. 2. Selecció de mesures de seguretat -Annex II Mesures de seguretat	Anual
Realització d'auditories internes. Revisió de mesures de seguretat i procediments	Tots	Al menys anual
Revisió de el Pla de Millora de la Seguretat	-	mensual / trimestral
Revisió de l'Estat de la Seguretat. INÉS	article 35 Sistema de Mètriques [op.mon.2]	Anual
Auditoria ENS (certificació conformitat ENS).	Article 34. Auditoria de la seguretat.	Biennal (després de la primera certificació al 2023)