



# SGSI01 – Política de Seguretat de la Informació

## Classificació de la Informació:

<b>Nivell del Document</b>	Registre
<b>Nom del Fitxer</b>	PoliticaDeSeguretat.pdf
<b>Tipus</b>	RESTRINGIT
<b>Àmbit de Difusió</b>	Tots els empleats i col·laboradors externs de l'AJUNTAMENT DE VILLANUEVA DE CASTELLÓN
<b>Responsable</b>	Responsable de Seguretat de la Informació de l'AJUNTAMENT DE VILLANUEVA DE CASTELLÓN



**CONTROL DE MODIFICACIONS**

<b>Descripció</b>	<b>Versió</b>	<b>Data</b>
Versió preliminar del document	1.0.	<input type="text"/>



## Contingut

Contingut.....	3
1. Introducció.....	5
2. La seguretat com a procés integral.....	6
2.1. Prevenció.....	7
2.2. Detecció.....	7
2.3. Resposta.....	7
2.4. Recuperació.....	8
3. Abast.....	8
4. Marc normatiu complementari.....	8
5. Organització de la seguretat.....	8
5.1. Comitè de gestió i coordinació de la seguretat de la informació.....	9
5.2. Responsable de la Informació.....	10
5.3. Responsables dels Servicis.....	11
5.4. Responsable de Seguretat de la Informació.....	11
5.5. Tècnic de seguretat dels sistemes.....	12
5.6. Responsables dels Sistemes.....	12
5.7. Procediments de designació.....	13
6. Dades de caràcter personal.....	13
7. Gestió de riscos.....	14
8. Desenvolupament de la Política de Seguretat.....	15
8.1. Classificació de la informació.....	16
8.2. Separació de funcions.....	16
8.3. Planificació i coordinació.....	16
8.4. Accés a la informació.....	16
8.5. Registre d'activitat.....	16
8.6. Confidencialitat i deure de secret.....	17
8.7. Uso de instal·lacions i equipament.....	17
8.8. Característiques dels sistemes d'informació.....	17
8.9. Protecció de la informació emmagatzemada i en trànsit.....	17
9. Obligacions del personal.....	18
10. Terceres parts.....	18



11. Entrada en vigor.....	19
Annex A. Glossari de termes.....	20
Annex B. Abreviatures.....	21
Annex C. Referències.....	21



## 1. Introducció

La informació constitueix un actiu de primer ordre per a l'AJUNTAMENT DE VILLANUEVA DE CASTELLÓN, des del moment en què resulta essencial per a la prestació de gran part dels serveis. D'altra banda, les tecnologies de la informació i les comunicacions s'han fet imprescindibles també cada vegada més per a les administracions públiques. No obstant açò, les indiscutibles millores que aporten al tractament de la informació vénen acompanyades de nous riscos, i per tant és necessari introduir mesures específiques per a protegir tant la informació com els serveis que depenguen d'ella.

La seguretat de la informació té com a objectiu protegir la informació i els serveis reduint els riscos als quals estan sotmesos fins a un nivell que resulte acceptable. Dins de cada organització només els seus màxims directius tenen les competències necessàries per a fixar aquest nivell, ordenar les actuacions i habilitar els mitjans per a dur-les a terme. En aquest sentit, establir una política de seguretat de la informació, i fer el subsegüent repartiment de tasques i responsabilitats, són actuacions prioritàries, ja que són els dos instruments principals per al govern de la seguretat i constitueixen el marc de referència per a totes les actuacions posteriors.

La Llei Orgànica 15/1999, de 13 de desembre, de Protecció de Dades de Caràcter Personal, en el seu article 9.1 obliga al Responsable del Fitxer a adoptar les mesures d'índole tècnica i organitzativa necessàries que garantisquen la seguretat de les dades de caràcter personal i eviten la seua alteració, pèrdua, tractament o accés no autoritzat. Llei 40/2015, de Règim Jurídic del Sector Públic estableix que les Administracions Públiques es relacionaran entre si i amb els seus òrgans, organismes públics i entitats vinculats o dependents a través de mitjans electrònics, que asseguren la interoperabilitat i seguretat dels sistemes i solucions adoptades per cadascuna d'elles, garantiran la protecció de les dades de caràcter personal, i facilitaran preferentment la prestació conjunta de serveis als interessats i arreplega l'Esquema Nacional de Seguretat en el seu article 156. Mentre que la Llei 39/2015, del Procediment Administratiu Comú de les Administracions Públiques, arreplega en el seu article 13 sobre drets de les persones en les seues relacions amb les Administracions Públiques el relatiu a la protecció de dades de caràcter personal, i en particular a la seguretat i confidencialitat de les dades que figuren en els fitxers, sistemes i aplicacions de les Administracions Públiques.

Tot açò motiva el compliment de l'Esquema Nacional de Seguretat, aprovat mitjançant Reial decret 3/2010, i modificat recentment pel Reial decret 951/2015. La present Política de Seguretat de la Informació s'elabora en compliment de l'exigència del Reial decret 3/2010, de 8 de gener, pel qual es regula l'Esquema Nacional de Seguretat (ENS) en l'àmbit de l'Administració Electrònica, que en el seu article 11 estableix l'obligació per a les Administracions Públiques de disposar d'una Política de Seguretat i indica els requisits mínims que ha de complir. Aquesta Política de Seguretat segueix també les indicacions de la guia CCN-STIC-



805 del Centre Criptològic Nacional (CCN), centre adscrit al Centre Nacional d'Intel·ligència (CNI).

La finalitat del ENS és la creació de les condicions necessàries de confiança en l'ús dels mitjans electrònics, a través de mesures per a garantir la seguretat dels sistemes, les dades, les comunicacions, i els serveis electrònics, que permeta als ciutadans i a les Administracions públiques, l'exercici de drets i el compliment de deures a través d'aquests mitjans.

L'adaptació al ENS implica que l'AJUNTAMENT DE VILLANUEVA DE CASTELLÓN i el seu personal han d'aplicar les mesures mínimes de seguretat exigides pel propi ENS, 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 a garantir la continuïtat dels serveis prestats. Les diferents unitats de gestió de l'AJUNTAMENT DE VILLANUEVA DE CASTELLÓN han de cerciorar-se que la seguretat TIC és una part integral de cada etapa del cicle de vida del sistema, des de la seua concepció fins a la seua retirada de servei, passant per les decisions de desenvolupament o adquisició i les activitats d'exploació.

Els requisits de seguretat i els costos associats 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.

Les unitats de gestió de l'AJUNTAMENT DE VILLANUEVA DE CASTELLÓN han d'estar preparades per a prevenir, detectar, reaccionar i recuperar-se d'incidentes, d'acord a l'Article 7 del ENS.

## 2. La seguretat com a procés integral

La seguretat de la informació és el resultat d'un procés que depèn de tots i cada un dels elements humans, tècnics, materials i organitzatius que intervenen en el tractament. Els que participen en qualsevol fase del tractament hauran de respondre, en la mesura de les seues responsabilitats, de la seguretat i bon ús de la informació. De manera especial, hauran de col·laborar en la prevenció, detecció i control dels riscos derivats d'actuacions negligents, ignorància de les normes, fallades tècniques, d'organització o de coordinació, o instruccions inadequades.

L'AJUNTAMENT DE VILLANUEVA DE CASTELLÓN, a través dels distints agents amb responsabilitats específiques en matèria de seguretat de la informació, s'encarregarà de proporcionar els canals de participació adequats que facen efectiva la col·laboració mencionada en el paràgraf anterior. De la mateixa manera, l'AJUNTAMENT DE VILLANUEVA DE CASTELLÓN, s'ocuparà de mantindre permanentment informats, a tots els destinataris d'esta política, del propòsit i contingut de la mateixa, així com dels documents que la desenvolupen i dels canals de participació habilitats.

El procés de gestió de la seguretat de la informació haurà d'estar sotmés a monitorització, control i millora continus per a confirmar la seua eficiència davant de la constant evolució dels riscos i dels sistemes de protecció.



## 2.1. Prevenció

L'AJUNTAMENT DE VILLANUEVA DE CASTELLÓN ha d'evitar, o almenys previndre en la mesura que siga possible, que la informació o els servicis es vegem perjudicats per incidents de seguretat. Per a això, s'han d'implementar les mesures mínimes de seguretat determinades per l'ENS, així com qualsevol control addicional identificat a través d'una avaluació d'amenaques i riscos. Estos controls, i els rols i responsabilitats de seguretat de tot el personal, han d'estar clarament definits i documentats. Per a garantir el compliment de la política, l'organització deu:

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

## 2.2. Detecció

Atés que els servicis es poden degradar ràpidament a causa d'incidentes, s'ha de monitoritzar l'operació de manera continuada per a detectar anomalies en els nivells de prestació dels servicis i actuar en conseqüència segons el que estableix l'Article 9 de l'ENS.

La monitorització és especialment rellevant quan s'establixen línies de defensa d'acord amb l'Article 8 de l'ENS. S'establiran mecanismes de detecció, anàlisi i report que arriben als responsables regularment i quan es produïx una desviació significativa dels paràmetres que s'hagen preestablert com normals.

## 2.3. Resposta

L'AJUNTAMENT DE VILLANUEVA DE CASTELLÓN deu:

- Establir mecanismes per a respondre eficaçment als incidents de seguretat.
- Designar punts de contacte per a les comunicacions respecte a incidents detectats en àrees de l'entitat o en altres organismes relacionats amb l'AJUNTAMENT DE VILLANUEVA DE CASTELLÓN.
- Establir protocols per a l'intercanvi d'informació relacionada amb l'incident. Açò inclou comunicacions, en ambdós sentits, amb els Equips de Resposta a Emergències (CERT) reconeguts a nivell nacional com a Iris-CERT, CEN-CERT i altres equivalents.

## 2.4. Recuperació

Per a restaurar la disponibilitat dels servicis, s'hauran de desenvolupar plans de contingència dels sistemes TIC que incloguen activitats de recuperació de la informació que contribuïsquen a la continuïtat del servici.



### 3. Abast

L'AJUNTAMENT DE VILLANUEVA DE CASTELLÓN aplicarà la present Política de Seguretat sobre aquells sistemes que estan relacionats amb l'exercici de drets per mitjans electrònics, amb el compliment de deures per mitjans electrònics o amb l'accés a la informació o al procediment administratiu.

De forma concreta, atesa la missió de l'AJUNTAMENT DE VILLANUEVA DE CASTELLÓN definida en el punt 2, la present Política de Seguretat és aplicable sobre els següents Sistemes d'Informació TIC i Servicis que els conformen:

- [SIS-SE] Seu electrònica (<http://villanuevadecastellon.sedelectronica.es/>)
  - [S-PERF] Perfil del contractant
  - [S-PER] Servici expedients personal
  - [S-FACE] Factura electrònica
  - [S-CAR] Carpeta ciutadana
  - [S-REG] Registre electrònic
  - [S-SUG] Suggestiments i queixes
  - [S-TAB] Tauler anuncis
  - [S-TRIB] Gestió tributària
  - [S-VAL] Validació de documents

L'organització desestima l'aplicació de la present Política de Seguretat sobre aquells sistemes d'informació no reflectits en este apartat.

### 4. Marc normatiu complementari

En el desenvolupament i implementació d'esta política es tindran en compte els Estatuts de l'AJUNTAMENT DE VILLANUEVA DE CASTELLÓN així com les seues normatives de desenvolupament relacionades amb els objectius del mateix.

### 5. Organització de la seguretat

Poden distingir-se tres (3) nivells en l'organigrama de l'AJUNTAMENT DE VILLANUEVA DE CASTELLÓN:

- Nivell 1 – Òrgans de Govern:





Consell de Govern, que entén la missió de l'organització, determina els objectius que es proposa aconseguir i respon que s'aconseguixen.

- Nivell 2 – Direcció Executiva:

Servicis, que entenen què fa cada unitat de gestió i com les diferents unitats es coordinen entre si per a assolir els objectius marcats per la Direcció.

- Nivell 3: Operacional

Se centra en una activitat concreta i controla com es fan les coses.

Seguint el mateix esquema i d'acord amb l'ENS s'estructura un organigrama de seguretat de l'AJUNTAMENT DE VILLANUEVA DE CASTELLÓN en 3 nivells:

- Nivell 1:
  - Comité de Gestió i Coordinació de la Seguretat de la Informació.
  - Responsable de la Informació.
  - Responsables dels Servicis.
- Nivell 2:
  - Responsable de la Seguretat de la Informació.
- Nivell 3:
  - Tècnic de Seguretat dels Sistemes.
  - Responsables dels Sistemes d'Informació.

L'especificació de requisits de seguretat (Nivell 1) correspon als responsables de la informació i dels servicis, junt amb el responsable del fitxer si hi haguera dades de caràcter personal. L'operació (nivell 3) correspon als responsables dels sistemes, mentres que la supervisió correspon al responsable de la seguretat (nivell 2) i al tècnic de seguretat (nivell 3).

Per damunt de tots ells hi ha el Comité de Coordinació i Gestió de la Seguretat (nivell 1). Este Comité de Seguretat pot assumir també la responsabilitat de la Informació i dels Servicis.

### **5.1. Comité de gestió i coordinació de la seguretat de la informació**

El Comité de Gestió i Coordinació de la Seguretat de la Informació, d'ara en avant **Comité de Seguretat**, coordina la seguretat de la informació a nivell d'organització.

D'acord amb l'ENS les funcions indicades que corresponen al Comité de Seguretat són:

- Elaborar (i revisar periòdicament) la Política de Seguretat de la informació perquè siga aprovada pel Consell de Govern de l'AJUNTAMENT DE VILLANUEVA DE CASTELLÓN.



- Aprovar i divulgar els procediments de seguretat de l'AJUNTAMENT DE VILLANUEVA DE CASTELLÓN.
- Promoure la millora contínua de la gestió de la seguretat de la informació de l'AJUNTAMENT DE VILLANUEVA DE CASTELLÓN.
- Coordinar els esforços de les diferents àrees en matèria de seguretat de la informació, per a assegurar que els esforços siguin consistents, alineats amb l'estratègia decidida en la matèria, i evitar duplicitats.
- Avaluar els principals riscos residuals assumits per l'AJUNTAMENT DE VILLANUEVA DE CASTELLÓN i recomanar possibles actuacions respecte d'ells.
- Avaluar l'exercici dels processos de gestió d'incidents de seguretat i recomanar possibles actuacions respecte d'ells. En particular, vetlar per la coordinació de les diferents àrees de seguretat en la gestió d'incidents de seguretat de la informació.
- Promoure la realització de les auditories periòdiques i avaluar el compliment de les obligacions de l'organisme en matèria de seguretat.
- Prioritzar les actuacions en matèria de seguretat d'acord amb els recursos disponibles.
- Vetlar perquè la seguretat de la informació es tinga en compte en tots els projectes TIC des de la seua especificació inicial fins a la seua posada en operació. En particular haurà de vetlar per la creació i utilització de servicis horitzontals que reduïsquen duplicitats i recolzen un funcionament homogeni de tots els sistemes TIC.
- Resoldre els conflictes de responsabilitat que puguen aparéixer entre els diferents responsables i/o entre diferents àrees de l'AJUNTAMENT DE VILLANUEVA DE CASTELLÓN, elevant aquells casos en què no tinga prou autoritat per a decidir.
- Avaluar les necessitats de recursos requerits per al compliment dels plans d'actuació derivats de l'aplicació de la Política de Seguretat.
- Elaborar un informe anual que elevarà al Consell de Direcció de l'AJUNTAMENT DE VILLANUEVA DE CASTELLÓN.

El Comité de Seguretat estarà format per:

- Responsable de la Regidoria amb competències en Tecnologies de la Informació i les Comunicacions, que presidirà el comité.
- Responsable de Seguretat de la Informació, que actuarà com a secretari del comité.
- Responsables dels Servicis.

El Comité de Seguretat no és un comité tècnic, però demanarà regularment del personal tècnic propi o extern, la informació pertinent per a prendre decisions. El Comité de Seguretat s'assessorarà en els temes sobre els quals haja de decidir o emetre una opinió.



## 5.2. Responsable de la Informació

El Responsable de la Informació establirà els requisits sobre la informació proporcionada per mitjans electrònics a través dels servicis de l'AJUNTAMENT DE VILLANUEVA DE CASTELLÓN i, per tant, tindrà l'última paraula a l'hora de decidir el tipus d'informació accessible i l'ús que se li puga donar, en virtut de la reglamentació vigent i de les bones pràctiques en matèria de protecció de dades. Li corresponen les funcions següents:

- Establiment dels requisits de la informació en matèria de seguretat.
- Treball en col·laboració amb el responsable de seguretat i els responsables dels sistemes en el manteniment dels sistemes catalogats segons l'annex I de l'Esquema Nacional de Seguretat.

El responsable de la informació serà el Sr. Alcalde - President de l'AJUNTAMENT DE VILLANUEVA DE CASTELLÓN.

## 5.3. Responsables dels Servicis

Els Responsables dels Servicis establiran els requisits de seguretat aplicables als servicis proporcionats per l'AJUNTAMENT DE VILLANUEVA DE CASTELLÓN a través de mitjans electrònics i, en este sentit, tindran com a funcions:

- Establiment dels requisits dels servicis TIC en matèria de seguretat.
- Treball en col·laboració amb el Responsable de Seguretat i els Responsables dels Sistemes on s'englobe el/els servicis per al manteniment dels sistemes catalogats segons l'annex I de l'Esquema Nacional de Seguretat.

## 5.4. Responsable de Seguretat de la Informació

El Cap del Servicis d'Informàtica tindrà el rol de Responsable de Seguretat de la Informació de l'AJUNTAMENT DE VILLANUEVA DE CASTELLÓN. Tenint per funcions les següents:

- Mantindre la seguretat de la informació manejada i dels servicis prestats pels sistemes TIC.
- Realitzar les auditories periòdiques que permeten verificar el compliment de les obligacions de l'organisme en matèria de seguretat.
- Promoure la formació i conscienciació de la Seguretat de la Informació dins del seu àmbit de responsabilitat.
- Verificar que les mesures de seguretat establides són adequades per a la protecció de la informació manejada i els servicis prestats.
- Aprovar tota la documentació relacionada amb la seguretat dels sistemes.
- Verificar els informes de monitorització i auditoria dels estats de seguretat dels sistemes.
- Recolzar i supervisar la investigació dels incidents de seguretat des de la seua notificació fins a la seua resolució.



- Elaborar l'informe periòdic de seguretat per al Comitè de Seguretat incloent els incidents més rellevants del període.
- Aprovació dels procediments de seguretat elaborats pels Responsables dels Sistemes quan en virtut del contingut no requerisca l'aprovació del Comitè de Seguretat.
- Proposar la redacció d'aquella normativa de seguretat de l'AJUNTAMENT DE VILLANUEVA DE CASTELLÓN que considere necessari formalitzar.
- Determinar la categorització dels sistemes i els requisits de seguretat amb caràcter previ a la posada en marxa d'un nou servici vinculat a l'ENS.

Esta figura de Responsable de Seguretat de la Informació descrita per l'ENS coincideix amb la del Responsable de Seguretat dels fitxers amb dades de caràcter personal de l'AJUNTAMENT DE VILLANUEVA DE CASTELLÓN.

### 5.5. Tècnic de seguretat dels sistemes

El Tècnic de Seguretat dels Sistemes és una figura operativa que depèn del Responsable de la Seguretat de la Informació. Té com a missió principal assistir al responsable de seguretat en el nivell operatiu que suposa la supervisió integral de la seguretat dels sistemes d'informació inclosos en l'abast d'esta política.

El Tècnic de Seguretat té per funcions les següents:

- Verificar l'aplicació dels procediments operatius de seguretat en els sistemes d'informació.
- Supervisar les instal·lacions de maquinari i programari, les seues modificacions i millores perquè la seguretat no estiga compromesa i que en tot moment s'ajusten als procediments establits.
- Supervisar l'estat de la seguretat dels sistemes.
- Informar el Responsable de Seguretat i als Responsables dels Sistemes d'Informació sobre qualsevol anomalia, compromís o vulnerabilitat relacionada amb la seguretat.
- Col·laborar en la investigació i resolució d'incidents de seguretat, des de la seua detecció fins a la seua resolució.
- Assessorar els responsables dels sistemes per a complir els requisits de seguretat establits.

El Tècnic de Seguretat dels Sistemes serà designat pel Responsable de la Seguretat de la Informació.

### 5.6. Responsables dels Sistemes

Es designarà un responsable para cada un dels sistemes d'informació definits en l'apartat d'Abast d'este document.

Dins de les seues àrees d'actuació i en el marc és esta Política de Seguretat, els Responsables dels Sistemes duran a terme les funcions següents:



- Vetlar pel funcionament correcte del Sistema durant tot el seu cicle de vida, de les seues especificacions i instal·lació, incorporant els requisits de seguretat necessaris per a l'operativa en el sistema.
- Definir la topologia i política de gestió del Sistema establint els criteris d'ús i els servicis disponibles en el mateix.
- Definir la política de connexió o desconnexió d'equips i usuaris nous en el Sistema.
- Proposar al Responsable de Seguretat els canvis que afecten la seguretat del sistema.
- Decidir les mesures de seguretat que aplicaran els subministradors de components del Sistema durant les etapes de desenrotllament, instal·lació i prova del mateix.
- Implantar i controlar les mesures específiques de seguretat del Sistema i cerciorar-se de que estes s'integren adequadament dins del marc general de seguretat.
- Determinar els requisits de la configuració autoritzada del maquinari i programari a utilitzar en el Sistema, en el que afecte la seua seguretat.
- Aprovar qualsevol modificació substancial de la configuració de qualsevol element del Sistema que afecte la seguretat i disponibilitat del servici.
- Dur a terme el preceptiu procés de revisió periòdica de l'anàlisi i gestió de riscos en el Sistema.
- Elaborar i aprovar la documentació de seguretat del Sistema.
- Delimitar les actuacions que afecten la Política de Seguretat de cada entitat involucrada en el manteniment, explotació, implantació i supervisió del Sistema.
- Investigar els incidents de seguretat que afecten el Sistema, i si és el cas, comunicació al Responsable de Seguretat o a qui este determine.
- Establir plans de contingència i emergència.
- A més, el responsable del sistema pot acordar la suspensió del maneig d'una certa informació o la prestació d'un cert servici si és informat de deficiències greus de seguretat que pogueren afectar la satisfacció dels requisits establits. Esta decisió ha de ser acordada amb els responsables de la informació afectada, del servici afectat i el responsable de seguretat, abans de ser executada.

### **5.7. Procediments de designació**

L'exercici de les responsabilitats definides en esta Política de Seguretat vindrà determinat per l'accés als diferents càrrecs que s'han vinculat a elles. En el cas que desapareguera o canviara de denominació d'algun d'estos càrrecs serà competència del Sr. Alcalde - President de l'AJUNTAMENT DE VILLANUEVA DE CASTELLÓN assignar el nou lloc de treball al que quedarà vinculada la figura.



## 6. Dades de caràcter personal

L'EXCEL·LENTÍSSIM AJUNTAMENT DE VILLANUEVA DE CASTELLÓN realitza tractaments en què fa ús de dades de caràcter personal sotmesos al que disposa pel Reial Decret 1720/2007, de 21 de desembre, pel qual s'aprova el Reglament de desplegament de la llei Orgànica 15/1999, de 13 de desembre, de Protecció de Dades de Caràcter Personal. Les polítiques de seguretat aplicables a estos fitxers i tractaments es regixen pel Document de Seguretat de l'EXCEL·LENTÍSSIM AJUNTAMENT DE VILLANUEVA DE CASTELLÓN. En ell s'indexen els fitxers afectats per la normativa, amb indicació del nivell de seguretat aplicable i mesures tècniques i organitzatives que siguen aplicables.

Tots els sistemes d'informació de l'EXCEL·LENTÍSSIM AJUNTAMENT DE VILLANUEVA DE CASTELLÓN s'ajustaran als nivells de seguretat requerits per la normativa per a la naturalesa i finalitat de les dades de caràcter personal arreplegats en el mencionat Document de Seguretat.

## 7. Gestió de riscos

Tots els sistemes subjectes a esta Política de Seguretat realitzaran una anàlisi de riscos, avaluant les amenaces i els riscos a què estan exposats. El govern i la gestió de la seguretat de la informació es guiaran pels resultats dels processos d'anàlisi i gestió de riscos.

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

El Responsable de Seguretat de la Informació elaborarà un informe anual sobre l'estat de la seguretat, els riscos previsibles i els plans d'actuació recomanats. Estos informes s'elevaran al Responsable de la Informació, qui fixarà el nivell de risc acceptable i ordenarà les actuacions oportunes.

La reducció dels nivells de risc es realitzarà per mitjà de l'aplicació de controls. La selecció i aplicació dels controls ponderaran el valor dels actius amb els nivells de risc i el cost de la seguretat.

Els controls hauran de ser eficaços abans, durant o després que ocórrega un incident de seguretat. El seu objectiu és evitar que succeïsqnen incidències i controlar els danys si és que finalment arriben a produir-se.

L'anàlisi i la gestió de riscos hauran d'estar presents en totes les fases del cicle de vida de les aplicacions i servicis relacionats amb el tractament de la informació, començant per la de l'estudi de viabilitat.

La selecció i aplicació dels controls de seguretat, així com l'avaluació de la seua eficiència, hauran de tindre's en compte durant el disseny, construcció,



contractació, adquisició, explotació, tancament, terminació, cancel·lació o alienació de les aplicacions i servicis mencionats.

Els òrgans competents de l'EXCEL·LENTÍSSIM AJUNTAMENT DE VILLANUEVA DE CASTELLÓN valoraran en les contractacions aquelles empreses, productes i servicis que puguen acreditar un nivell de qualitat o seguretat. El compliment d'un nivell mínim determinat podrà ser un requisit imprescindible.

Esta anàlisi de riscos es repetirà:

- Regularment, almenys una vegada a l'any.
- Quan canvie la informació manejada.
- Quan canvien els servicis prestats.
- Quan ocorrega un incident greu de seguretat.
- Quan es reporten vulnerabilitats greus.

## 8. Desenvolupament de la Política de Seguretat

Esta Política es desenvolupa per mitjà de **Normativa de Seguretat** que afronte aspectes específics. La Normativa de Seguretat estarà a disposició de tots els membres de l'organització que necessiten conèixer-la, en particular per a aquells que utilitzen, operen o administren els sistemes d'informació i comunicacions.

Altres documents que complementen esta Política de Seguretat són:

- El Manual del Sistema de Gestió de la Privacitat de l'EXCEL·LENTÍSSIM AJUNTAMENT DE VILLANUEVA DE CASTELLÓN.
- Normes d'ús personal dels recursos informàtics i telemàtics de l'EXCEL·LENTÍSSIM AJUNTAMENT DE VILLANUEVA DE CASTELLÓN.
- Els acords del Consell de Govern de l'EXCEL·LENTÍSSIM AJUNTAMENT DE VILLANUEVA DE CASTELLÓN posteriors a l'aprovació d'esta política en la mesura en què puguen produir algun efecte sobre ella.

La normativa de seguretat estarà disponible en el sistema d'arxius en xarxa de l'EXCEL·LENTÍSSIM AJUNTAMENT DE VILLANUEVA DE CASTELLÓN.

La present política es desenvoluparà en un conjunt de documents l'objectiu del qual és facilitar que el tractament d'informació es realitze d'acord amb els objectius i principis exposats en els següents punts.

Els documents mencionats en el paràgraf anterior hauran d'abordar, almenys, els procediments següents:

- Condicions per a l'accés a la informació.



- Ús de l'equipament informàtic i de comunicacions.
- Gestió d'incidents i problemes.
- Continuitat d'operacions.
- Seguretat amb tercers.
- Classificació i tractament de la informació.
- Anàlisi i gestió de riscos.
- Seguretat física i del personal.
- Prevenició de virus i codi maliciós.
- Cicle de vida dels sistemes d'informació.
- Millora contínua.
- Elaboració, publicació i revisió de la política de seguretat de la informació i dels documents complementaris.

A continuació, es detallen les polítiques que han de concretar-se a través de la Normativa de Seguretat i els Procediments associats:

### **8.1. Classificació de la informació**

Els actius d'informació hauran d'estar inventariats i classificats. El nivell de protecció i les mesures a aplicar es basaran en el resultat de la dita classificació.

### **8.2. Separació de funcions**

La seguretat de la informació exigeix un repartiment de tasques i responsabilitats amb una clara separació de funcions. En particular, s'haurà de mantindre una clara distinció entre els tres papers següents: Responsable de la Informació, Responsable del Servei i Responsable de Seguretat, que seran definits en l'esquema organitzatiu.

### **8.3. Planificació i coordinació**

Els objectius a mitjà termini per a la millora de la seguretat de la informació s'explicitaran en els corresponents plans estratègics. Estos plans contindran una descripció de les línies d'actuació previstes, projectes, indicadors de compliment i de progrés, així com mètriques per a avaluar l'efectivitat. Estos plans es revisaran anualment tenint en compte els resultats de les auditories i de les avaluacions de riscos. Els plans estratègics, els informes de seguiment i les revisions anuals se sotmetran a l'aprovació del Responsable de la Informació.





La coordinació entre tots els agents de què depèn la seguretat de la informació ha de formar part de totes les iniciatives i actuacions. L'EXCEL·LENTÍSSIM AJUNTAMENT DE VILLANUEVA DE CASTELLÓN, habilitarà els mitjans tècnics necessaris per a facilitar eixa coordinació. El Responsable de Seguretat actuarà de manera coordinada amb l'aplicació i control de les mesures de seguretat.

Les empreses de servicis, organitzacions i entitats amb accés a informació situada sota la responsabilitat de l'EXCEL·LENTÍSSIM AJUNTAMENT DE VILLANUEVA DE CASTELLÓN, hauran d'anomenar un Responsable de Seguretat que actue com a interlocutor vàlid als efectes de la coordinació en esta matèria.

#### **8.4. Accés a la informació**

Els que tracten informació que no haja sigut classificada d'accés públic hauran d'estar degudament identificats i tindran els privilegis d'accés a la informació estrictament imprescindibles per a exercir la seua comesa.

Cada intent d'accés haurà de quedar registrat amb el suficient nivell de detall.

#### **8.5. Registre d'activitat**

Les actuacions de les persones, en tant que formen part de determinat tractament d'informació, podran ser registrades en compliment de les exigències legals de traçabilitat. També podran ser-ho per a monitoritzar el compliment de la present política. En tot cas, el registre de tals actuacions es realitzarà preservant els drets dels afectats i respectant la normativa laboral aplicable.

#### **8.6. Confidencialitat i deure de secret**

Els que per raó de l'exercici de les seues funcions accedisquen a dades que no siguen d'accés públic hauran d'observar la necessària reserva, confidencialitat i sigil respecte a estes dades, inclús després d'haver cessat en les seues funcions o finalitzat la relació contractual o laboral.

#### **8.7. Ús d'instal·lacions i equipament**

L'EXCEL·LENTÍSSIM AJUNTAMENT DE VILLANUEVA DE CASTELLÓN dotarà els llocs de treball amb l'equipament informàtic i de comunicacions necessari per a l'exercici de les funcions encomanades. Els dits equips no estan destinats a l'ús personal.

L'equipament mencionat en el paràgraf anterior no podrà utilitzar-se per a activitats il·lícites o irregulars, o que afecten negativament el funcionament de l'administració o siguen contràries als interessos d'esta.

La instal·lació o utilització d'elements maquinari o programari aliens a què formen part de la configuració del lloc de treball requeriran d'una autorització prèvia per part de l'òrgan competent en matèria de tecnologies de la informació que corresponga.

Les infraestructures informàtiques i de comunicacions que no formen part dels llocs de treball hauran d'ubicar-se en àrees separades, d'accés restringit i prou



protegides d'acord amb la naturalesa de la informació i els servicis en què intervinguen.

### **8.8. Característiques dels sistemes d'informació**

Els sistemes d'informació proporcionaran la funcionalitat estrictament necessària per a complir els propòsits declarats, i cap més.

L'ús ordinari dels sistemes d'informació ha de ser senzill i segur, de manera que una utilització insegura requereisca d'un acte conscient per part de l'usuari.

Les funcions d'operació, administració, manteniment i registre d'activitat seran les mínimes necessàries, hauran d'estar descrites i documentades i subjectes a controls estrictes.

### **8.9. Protecció de la informació emmagatzemada i en trànsit**

L'EXCEL·LENTÍSSIM AJUNTAMENT DE VILLANUEVA DE CASTELLÓN, a través dels distints agents amb responsabilitats específiques en matèria de seguretat de la informació, establirà les condicions per a la protecció en el tractament de la informació fora dels seus locals i sistemes.

L'EXCEL·LENTÍSSIM AJUNTAMENT DE VILLANUEVA DE CASTELLÓN garantirà, de la mateixa manera que en el paràgraf anterior, la conservació i recuperació de la informació mentres perdure la seua vigència.

La informació en suport no electrònic que haja sigut causa o conseqüència directa de tractament automatitzat d'informació haurà de protegir-se amb el mateix grau de seguretat que esta.

## **9. Obligacions del personal**

Tots els membres de l'EXCEL·LENTÍSSIM AJUNTAMENT DE VILLANUEVA DE CASTELLÓN tenen l'obligació de conèixer i complir esta Política de Seguretat de la Informació i la Normativa de Seguretat desenvolupada a partir d'ella, sent responsabilitat del Comitè de Seguretat disposar els mitjans necessaris perquè la informació arribe als afectats, tenint en compte sempre les disponibilitats pressupostàries de l'EXCEL·LENTÍSSIM AJUNTAMENT DE VILLANUEVA DE CASTELLÓN.

Tots els treballadors de l'EXCEL·LENTÍSSIM AJUNTAMENT DE VILLANUEVA DE CASTELLÓN sota l'abast de l'ENS atendran a una acció de conscienciació en matèria de seguretat TIC, almenys, una vegada cada dos anys. S'establirà un programa d'accions en conscienciació contínua per a atendre tots els membres de l'EXCEL·LENTÍSSIM AJUNTAMENT DE VILLANUEVA DE CASTELLÓN relacionats amb servicis d'Administració Electrònica, en particular als de nova incorporació, tenint en compte sempre les disponibilitats pressupostàries de l'EXCEL·LENTÍSSIM AJUNTAMENT DE VILLANUEVA DE CASTELLÓN. Es realitzarà una acció de conscienciació durant els dos anys següents a l'aprovació d'esta Política de Seguretat i de manera continuada per al personal de nova incorporació.



Si és el cas, si es requerix formació específica per al maneig segur dels sistemes, les persones amb responsabilitat en l'operació o administració de sistemes TIC la rebran en la mesura que la necessiten per a realitzar el seu treball.

## 10. Terceres parts

Quan l'EXCEL·LENTÍSSIM AJUNTAMENT DE VILLANUEVA DE CASTELLÓN preste servicis a altres organismes o manege informació d'altres organismes, se'ls farà partícip d'esta Política de Seguretat de la Informació. Per a això, s'establiran canals per a informe i coordinació dels respectius Comitès de Seguretat de l'ENS i s'establiran procediments d'actuació per a la reacció davant d'incidents de seguretat.

Quan l'EXCEL·LENTÍSSIM AJUNTAMENT DE VILLANUEVA DE CASTELLÓN utilitze servicis de tercers o cedisca informació a tercers, se'ls farà partícip d'esta Política de Seguretat i de la Normativa de Seguretat que implique als dits servicis o informació. Dita tercera part quedarà subjecta a les obligacions establides en la mencionada normativa, havent d'incorporar als plecs i comandes de l'EXCEL·LENTÍSSIM AJUNTAMENT DE VILLANUEVA DE CASTELLÓN. Amb això, el proveïdor haurà de garantir que el seu personal està adequadament format en matèria de seguretat d'acord amb els requeriments de l'EXCEL·LENTÍSSIM AJUNTAMENT DE VILLANUEVA DE CASTELLÓN.

## 11. Entrada en vigor

La present Política de Seguretat de la Informació és efectiva des de l'endemà de la seua data d'aprovació pel Consell de Govern de l'EXCEL·LENTÍSSIM AJUNTAMENT DE VILLANUEVA DE CASTELLÓN i fins que siga reemplaçada per una nova Política.

L'EXCEL·LENTÍSSIM AJUNTAMENT DE VILLANUEVA DE CASTELLÓN disposarà dels mitjans per a publicar, donar a conèixer i facilitar el compliment d'esta política i dels documents que la desenvolupen, així com per a verificar la seua aplicació i efectivitat. Així mateix, habilitarà canals de participació que permeten, als destinataris d'esta política i dels documents complementaris, participar en la seua revisió i millora.

<b>APROVAT:</b>
<b>Ple</b>
<b>Data:</b> <input type="text"/>
<b>Firma:</b>



## Annex A. Glossari de termes

### **Anàlisi de riscos**

Utilització sistemàtica de la informació disponible per a identificar perills i estimar els riscos.

### **Dades de caràcter personal**

Qualsevol informació concernent a persones físiques identificades o identificables. Llei Orgànica 15/1999, de 13 de desembre, de Protecció de Dades de Caràcter Personal.

### **Gestió d'incidents**

Pla d'acció per a atendre a les incidències que es donen. A més de resoldre-les ha d'incorporar mesures d'acompliment que permeten conèixer la qualitat del sistema de protecció i detectar tendències abans que es convertisquen en grans problemes. ENS.

### **Gestió de riscos**

Activitats coordinades per a dirigir i controlar una organització respecte als riscos. ENS.

### **Incident de seguretat**

Succés inesperat o no desitjat amb conseqüències en detriment de la seguretat del sistema d'informació. ENS.

### **Informació**

Cas concret d'un cert tipus d'informació.

### **Política de seguretat**

Conjunt de directrius plasmades en document escrit, que regixen la forma en què una organització gestiona i protegeix la informació i els servicis que consideren crítics. ENS.

### **Principis bàsics de seguretat**

Fonaments que han de regir tota acció orientada a assegurar la informació i els servicis. ENS.

### **Responsable de la informació**

Persona que té la potestat d'establir els requisits d'una informació en matèria de seguretat.

### **Responsable de la seguretat**

El responsable de seguretat determinarà les decisions per a satisfer els requisits de seguretat de la informació i dels servicis.



### **Responsable del servici**

Persona que té la potestat d'establir els requisits d'un servici en matèria de seguretat.

### **Responsable del sistema**

Persona que s'encarrega de l'explotació del sistema d'informació.

### **Servici**

Funció o prestació exercida per alguna entitat oficial destinada a cuidar interessos o satisfer necessitats dels ciutadans.

### **Sistema d'informació**

Conjunt organitzat de recursos perquè la informació es puga arreplegar, emmagatzemar, processar o tractar, mantindre, usar, compartir, distribuir, posar a disposició, presentar o transmetre.

## **Annex B. Abreviatures**

### **CCN**

Centre Criptològic Nacional

### **CERT**

Computer Emergency Reaction Team

### **ENS**

Esquema Nacional de Seguretat

### **STIC**

Seguretat TIC

### **TIC**

Tecnologies de la Informació i les Comunicacions

## **Annex C. Referències**

### **CCN-STIC-402**

Organització i Gestió per a la Seguretat dels Sistemes TIC. Desembre 2006.

### **CCN-STIC-801**

ENS - Responsables i Funcions. 2010.

**Llei 40/2015**, de Règim Jurídic del Sector Públic

**Llei 39/2015**, del Procediment Administratiu Comú de les Administracions Públiques

**Llei 11/2007**

Llei 11/2007, de 22 de juny, d'accés electrònic dels ciutadans als Servicis Públics. BOE de 23 de juny de 2007.

**Llei 15/1999**

Llei Orgànica 15/1999, de 13 de desembre, de protecció de dades de Caràcter Personal. BOE de 14 de desembre de 1999.

**RD 1720/2007**

Reial Decret 1720/2007, de 21 de desembre, pel qual s'aprova el Reglament de desplegament de la llei Orgànica 15/1999, de 13 de desembre, de Protecció de Dades de Caràcter Personal. BOE de 19 de gener de 2008.

**RD 3/2010**

Reial Decret 3/2010, de 8 de gener, pel qual es regula l'Esquema Nacional de Seguretat en l'àmbit de l'Administració Electrònica. BOE de 29 de gener de 2010.