POLÍTICA DE LA SEGURETAT DE LA INFORMACIÓ

ÀREA DE SOCIETAT DEL CONEIXEMENT

Febrer 2015

POLÍTICA DE SEGURETAT DE LA INFORMACIÓ

ÀREA DE SOCIETAT DEL CONEIXEMENT

CONTROL DEL DOCUMENT

INFORMACIÓ GENERAL

Identificador del document:	4778759483726664 50687084816883648 3 6768 7564 407769788176646672 1367786687	
Entitat:	Ajuntament de la Garriga	
Regidoria:	Societat del Coneixement	
Títol:	Política de la Seguretat de la Informació	
Nivell d'accés:		
Llista de distribució:		
Nom del fitxer i tamany:	Política Seguretat de la Informació.docx	110 Kilobytes
Autor:		

TAULA 1

HISTÒRIC DE REVISIONS

Data de creació:	Dimecres 18 / desembre / 2014 09:43	
Control de versions:	Data última revisió:	dijous, 12 / febrer / 2015 09:59:00
	Usuari:	

TAULA 2

Històric de versions			
Versió	**Data**	**Autor**	**Observacions**
1.0	21/10/2014		Recopilació de fonts, creació de l'estructura de continguts i primer esborrany de continguts.
1.1	18/12/2014		Creació de continguts.
1.2	19/12/2014		Revisió, aportacions finals i maquetació del document a presentar a la Comissió de Seguretat LOPD.
1.3	26/01/2015		Revisió i aportacions de la Comissió de seguretat LOPD de l'Ajuntament de la Garriga.
1.4	04/02/2015		Aportació normativa tècnica gestió documental i arxiu.

TAULA 3

Estat formal			
Elaboració	Revisió/Aprovació,	Revisió/Aprovació,	Aprovació,
04 / 02 / 2015	05 / 02 / 2015	05 / 02 / 2015	09 / 02 / 2015
Tècnic Mitjà Informàtic	Regidor/a Societat del Coneixement	Secretari Comissió protecció de dades de caràcter personal	Junta de Govern Local Punt nº 32

TAULA 4

TAULA DE CONTINGUTS

1. POLÍTICA DE SEGURETAT DE LA INFORMACIÓ

1.1. APROVACIÓ I PUBLICACIÓ

Text aprovat el dia 9 de febrer de 2015 per la Junta de Govern Local de l'Ajuntament de la Garriga.

Aquesta Política de Seguretat de la informació és efectiva des d'aquesta data, anul·lant qualsevol altre existent, i fins que sigui expressament derogada o reemplaçada per una nova.

Aquesta Política de Seguretat es trobarà permanentment disponible de forma pública i enllaçada a la plana del portal de l'Ajuntament de la Garriga:

http://www.lagarriga.cat/el-municipi-per-temes/societat-del-coneixement

1.2. INTRODUCCIÓ

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

L'objectiu de la seguretat de la informació és el de garantir la seva qualitat i la prestació continuada dels serveis, actuant preventivament, supervisant l'activitat diària i reaccionant amb prestesa als incidents.

Els sistemes TIC han d'estar protegits contra amenaces de ràpida evolució amb potencial per incidir en la confidencialitat, integritat, disponibilitat, ús previst i valor de la informació i els serveis. Per defensar-se d'aquestes amenaces, es requereix una estratègia que s'adapti als canvis en les condicions de l'entorn per garantir la prestació contínua dels serveis. Això implica l'aplicació de mesures de seguretat, aprovades per l'Ajuntament de la Garriga, així com realitzar accions de seguiment continu dels nivells de prestació de serveis, anàlisis de vulnerabilitats reportades, i resposta efectiva als incidents per garantir la continuïtat dels serveis prestats.

Els diferents departaments de l'Ajuntament de la Garriga, han de cerciorar-se que la seguretat TIC és una part integral de cada etapa del cicle de vida del servei, des de la seva concepció fins a la seva retirada, passant per les decisions de desenvolupament o adquisició i les activitats d'explotació. Els requisits de seguretat i les necessitats de finançament, han de ser identificats i inclosos en la planificació, en la sol·licitud d'ofertes, i en plecs de licitació.

477875948372666462506870848168836483626768627564624077697881766466726286686513677866 87

Per garantir el compliment de la Política de Seguretat TIC (de la informació), l'Ajuntament de la Garriga ha 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.

1.3. PREVENCIÓ

L'Àrea TIC de l'Ajuntament de la Garriga ha 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 proposa la implementació de mesures de seguretat i controls addicionals, identificats a través d'una avaluació d'amenaces i riscos, segons la metodologia d'anàlisis de riscos MAGERIT v.3 i la norma estàndard ISO/IEC 31000:2010 – Gestió de Riscos.

Les accions, procediments, rols i responsabilitats de seguretat de tot el personal, associat a la prevenció d'incidents que puguin afectar els serveis de l'Ajuntament de la Garriga poden ser consultats a la:

- Declaració d'aplicabilitat de l'Esquema Nacional de Seguretat
- Document de Seguretat per a la protecció de dades de caràcter personal

en possessió de la regidoria de Societat del Coneixement

1.4. 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, han de ser monitoritzats, de manera contínua, per detectar anomalies en els nivells de prestació dels serveis i actuar en conseqüència.

L'Àrea TIC ha establert un sistema de control, recollida i anàlisis de traces, registres i indicadors dels serveis de l'Ajuntament de la Garriga, amb la finalitat de garantir la seva qualitat, segons els estàndards ISO/IEC 31000:2010 – Gestió de Riscos i ISO/IEC 27001 i 27002:2013 – Seguretat Informàtica.

Les accions, procediments, traces, registres, indicadors, rols i responsabilitats de seguretat de tot el personal, associat a la detecció d'incidents que puguin afectar els serveis de l'Ajuntament de la Garriga poden ser consultats al:

- Pla d'Auditories

en possessió de la regidoria de Societat del Coneixement.

1.5. RESPOSTA

Amb la finalitat de garantir una ràpida, eficient i eficaç resolució de les incidències que puguin afectar els serveis de l'Ajuntament de la Garriga, l'Àrea TIC ha establert, segons l'estàndard ISO/IEC 20000:2011 – Gestió de Serveis TI:

- Processos, procediments, mecanismes, rols i responsabilitats de seguretat de tot el personal per respondre eficaçment els incidents de seguretat.
- Un punt de contacte per a la comunicació, registre i gestió d'incidents i peticions de serveis.
- Protocols per l'intercanvi d'informació relacionada amb els incidents (intern, extern, proveïdors, organismes, etc.)

Les accions, procediments, punts i canals de contacte, protocols, rols i responsabilitats de seguretat de tot el personal, associat a la resposta d'incidents que puguin afectar els serveis de l'Ajuntament de la Garriga poden ser consultats al:

- Pla de Continuïtat i Disponibilitat dels Serveis i Sistemes TIC en possessió de la regidoria de Societat del Coneixement.

1.6. RECUPERACIÓ

Per garantir la disponibilitat dels serveis crítics, l'Àrea TIC de l'Ajuntament de la Garriga ha desenvolupat un Pla de Continuïtat dels Serveis i Sistemes TIC, segons l'estàndard ISO/IEC 22301:2013 – Gestió i Continuïtat del negoci.

1.7. ABAST

Aquesta Política és d'aplicació a l'Ajuntament de la Garriga, a:

- tots els sistemes TIC ("Annex – A. Manual de l'Organització i Funcionament de l'Àrea TIC")
- tots els membres de l'organització, sense excepcions
- ciutadans, degudament informats
- tercers col·laboradors amb l'Ajuntament de la Garriga mitjançant una relació contractual

1.8. MISSIÓ

En l'àmbit de les Administracions públiques, la consagració del dret a comunicar-se amb elles a través de mitjans electrònics comporta una obligació correlativa de les mateixes, que té, com a premisses, la promoció de les condicions perquè la llibertat i la igualtat siguin reals i efectives, i la remoció dels obstacles que impedeixin o dificultin la seva plenitud, la qual cosa demanda incorporar les peculiaritats que exigeixen una aplicació segura d'aquestes tecnologies.

Es en aquest context on l'Ajuntament de la Garriga, a través de la Regidoria de Societat del Coneixement, defineix aquesta "Política de Seguretat de la informació" en la utilització de mitjans electrònics que permeti l'adequada protecció de la informació.

477875948372666462506870848168836483626768627564624077697881766466726286686513677866 87

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

L'Ajuntament de la Garriga persegueix fonamentar aquesta confiança en què els sistemes d'informació prestaran els seus serveis i custodiaran la informació d'acord amb les seves especificacions funcionals, sense interrupcions o modificacions fora de control, i sense que la informació pugui arribar al coneixement de persones no autoritzades.

1.9. MARC NORMATIU

L'Ajuntament de la Garriga, defineix, i fa seva, aquesta Política de Seguretat de la informació en compliment de la normativa, que li son d'aplicació:

- Llei 30/1992, de 26 de novembre, de règim jurídic de les administracions públiques i del procediment administratiu comú
- Llei 11/2007, de 22 de juny, d'accés electrònic dels ciutadans als serveis públics
- Reial decret 1671/2009, de 6 de novembre, pel qual es desplega parcialment la Llei 11/2007, de 22 de juny, d'accés electrònic dels ciutadans als serveis públics
- Llei 26/2010, del 3 d'agost, de règim jurídic i de procediment de les administracions públiques de Catalunya.
- Llei 29/2010, del 3 d'agost, de l'ús dels mitjans electrònics al sector públic de Catalunya.
- Llei 56/2007, de 28 de desembre, de mesures d'impuls de la societat de la informació
- Llei 59/2003, de 19 de desembre, de signatura electrònica
- Llei orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal
- 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.
- Llei 34/2002, de 11 de juliol, de Serveis de la Societat de la Informació i de Comerç Electrònic.
- Llei 10/2001, de 13 de juliol, d'arxius i documents
- Reial decret 3/2010, de 8 de gener, pel qual es regula l'Esquema Nacional de Seguretat en l'àmbit de l'Administració electrònica.
- Reial decret 4/2010, de 8 de gener, pel qual es regula l'Esquema Nacional d'Interoperabilitat en l'àmbit de l'Administració electrònica.
- Llei orgànica 1/1992, de 21 de febrer, sobre protecció de la seguretat ciutadana
- Llei 9/2014, de 9 de maig, de telecomunicacions
- Reglaments de creació i Funcionament de la seu electrònica, registre electrònic i de Difusió d'informació de l'administració municipal i Tauler d'edictes de l'Ajuntament de la Garriga (aprovats pel Ple d'aquesta corporació el passat 29 de maig de 2013)
- Llei 19/2013, de 9 de desembre, de transparència, accés a la informació pública i bon govern.
- Llei 19/2014, de de transparència, accés a la informació pública i bon govern.

a més d'aquesta normativa serà d'aplicació la resta de lleis generals de dret administratiu i de Tecnologies de la Informació que puguin aplicar-se (p.ex: ordenança d'administració electrònica, transparència, accés i reutilització de la informació, reglament d'arxiu, etc.) al Servei així com aquells documents amb les condicions d'ús dels diferents serveis que l'Ajuntament de la Garriga determini.

477875948372666462506870848168836483626768627564624077697881766466726286686513677866887

També li seran d'aplicació les normatives i bones pràctiques, que amb l'objectiu d'aconseguir i garantir un millor nivell de servei per al ciutadà, ha decidit aplicar en matèria de:

- Seguretat Informàtica - ISO/IEC 27001 i 27002:2013
- Gestió de Serveis TI - ISO/IEC 20000:2011
- Gestió i Continuïtat del negoci - ISO/IEC 22301:2013
- Gestió de riscos – ISO/IEC 31000:2010
- Gestió, desenvolupament i operacions amb serveis de tecnologia de la informació - ITIL v3
- Control i supervisió de tecnologies de la informació - COBIT v5
- Gestió de documents – ISO/IEC 15489
- Gestió de metadades – ISO/IEC 23081
- Sistemes de gestió per als documents - 30300

en els serveis relacionats amb l'àmbit TIC.

1.10. ORGANITZACIÓ DE SEGURETAT TIC

L'Ajuntament de la Garriga disposa d'un "Organigrama de Seguretat TIC", aprovat per la Junta de Govern Local i en possessió de la regidoria de Societat del Coneixement, on estan identificats i definits els següents ítems:

- Organització de seguretat, en compliment de les lleis, que li son d'aplicació, i de les normes implementades, amb la identificació de rols i càrrecs
- Rols, amb especificació de les missions, funcions i responsabilitats
- Procediments associats (designació, convocatòria, etc.)

1.11. AUDITORIA

El Pla d'Auditories, en possessió de la Regidoria de Societat del Coneixement, de l'Ajuntament de la Garriga identifica:

- Abast
- Objectius
- Planificacions
- Processos i procediments
- Criteris i mètriques
- Rols – responsabilitats
- Informes
- Anàlisis

necessaris per a la realització de les auditories d'obligat compliment:

- Reial decret 3/2010, de 8 de gener, pel qual es regula l'Esquema Nacional de Seguretat en l'àmbit de l'Administració electrònica.
- 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.

477875948372666462506870848168836483626768627564624077697881766466726286686513677866887

i les exigides per les normatives implementades per garantir la qualitat del servei i alimentar el procés de millora continua:

- Seguretat Informàtica - ISO/IEC 27001 i 27002:2013
- Gestió de Serveis TI - ISO/IEC 20000:2011
- Gestió i Continuïtat del negoci - ISO/IEC 22301:2013

1.12. DADES DE CARÀCTER PERSONAL

L'Ajuntament de la Garriga tracta dades de caràcter personal.

El "Document de Seguretat" en possessió de la Regidoria de Societat del Coneixement, inclou l'inventari de fitxers i tractaments amb dades de caràcter personal responsabilitat de l'Ajuntament de la Garriga.

L'Àrea TIC ha definit i implementat les mesures i controls corresponents al nivell de seguretat de les dades de caràcter personal tractades, segons la definició i especificació del "Document de Seguretat" en aplicació del "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".

1.13. GESTIÓ DE RISCOS

L'Àrea TIC disposa d'un "Informe d'Anàlisi de Riscos TIC" actualitzat, on es relacionen els actius informàtics analitzats i els serveis de l'Ajuntament de la Garriga.

Dins d'aquest informe s'inclou:

- Planificació
- Actualització
- Mètriques i sistemes de valoració
- Rols associats
- Anàlisis
- Proposta de millores

A partir d'aquesta informació, s'obté el:

- Pla de Continuïtat i Disponibilitat dels Serveis i Sistemes TIC
- Pla de Millores

47787594837266646250687084816883648362676862756462407769788176646672 628668651367786687

1.14. DESENVOLUPAMENT DE LA POLÍTICA

Aquesta política s'ha de desenvolupar per mitjà de normativa de seguretat que afronti aspectes específics, determini les mesures de seguretat aplicables als sistemes i analitzi els riscos implicats en la prestació dels serveis públics per mitjans electrònics. La normativa de seguretat estarà a disposició de tots els membres de l'organització que necessitin conèixer-la, en particular per aquells que utilitzin, operin o administrin els sistemes d'informació i comunicacions.

Aquesta política estarà en possessió de la regidoria de Societat del Coneixement fent-la extensa a la resta d'àrees que conformen l'Ajuntament de la Garriga a través dels recursos compartits que posen a disposició en aquesta corporació.

1.15. OBLIGACIONS DEL PERSONAL

Tots els afectats:

- membres de l'organització, sense excepcions
- ciutadans, degudament informats
- tercers col·laboradors amb l'Ajuntament de la Garriga mitjançant una relació contractual

tenen l'obligació de complir aquesta Política de Seguretat Àrea TIC, sent responsabilitat del Comitè de Seguretat disposar els mitjans necessaris perquè la informació arribi als afectats.

Tots els membres de l'organització, sense excepcions, assistiran a una sessió de conscienciació en matèria de seguretat TIC, almenys una vegada a l'any.

S'establirà un programa de conscienciació contínua per atendre a tots els membres, en particular als de nova incorporació.

Les persones amb responsabilitat en l'ús, operació o administració de sistemes TIC rebran formació per a la gestió segura dels sistemes en la mesura en què la necessitin per realitzar el seu treball.

La formació serà obligatòria abans d'assumir una responsabilitat, tant si és la seva primera assignació o si es tracta d'un canvi de lloc de treball o de responsabilitats en el mateix.

1.16. TERCERS

A l' "Organigrama de Seguretat TIC" s'especifiquen aquells tercers que assumeixen les responsabilitats d'Encarregats de Tractament per compte de l'Ajuntament de la Garriga.

Els Encarregats de Tractament han estat informats sobre el contingut d'aquesta "Política de Seguretat Àrea TIC" i de on i com obtenir les versions actualitzades de la mateixa

47787594837266646250687084816883648362676862756462407769788176646672 628668651367786687

1.17. FONTS

Per a l'elaboració d'aquesta política s'ha fet ús de la guia:

Model política de seguretat Esquema Nacional de Seguretat

cesicat

477875948372666462506870848168836483626768627564624077697881766466726286686513677866 87

2. ANNEX

2.1. TAULA DE FIGURES

Figures Taules

Figures Il·lustracions

No es troben elements de taula d'il·lustracions

Figures Equacions

No es troben elements de taula d'equacions

47787594837266646250687084816883648362676862756462407769788176646672 628668651367786687