 Ajuntament de Barcelona	<b>CRITERIS DE SEGURETAT DELS SISTEMES D'INFORMACIÓ I PROTECCIÓ DE DADES</b>
<b>Institut Municipal d'Informàtica</b>	<b>GUIA</b>
Codi: SEG_GUIA_INC-01	Versió: 01


## Guia del Procediment de Notificació d'Incidències de Seguretat

**APROVAT**

<i>Component</i>		
<b>Objectiu</b>	Guia del Procediment que estableix com els usuaris han de notificar els incidents de seguretat.	
<b>Abast</b>	Administració Municipal	
<i>Controls</i>		
Codi control	Descripció control	
13.1	Comunicació d'incidents de seguretat	
13.2	Gestió d'incidents i millores	
<i>Responsable:</i>	<i>Revisat per:</i>	<i>Aprovat per:</i>
Responsable Seguretat / Neus Bellavista	Comitè Seguretat IMI	Gerent / Lluís Olivella
<i>Elaborat per:</i>		
Oficina Seguretat TIC / Jose L. Rubiés		
<i>Distribució (Destinatari o perfils d'accés)</i>		
Administració Municipal (informàtica gestionada per l'IMI). És farà una versió especial per publicar a la Intranet Municipal.		

### **RESUM**


Qualsevol persona que pertanyi o treballi per a l'Administració Municipal, que detecti una incidència o anomalia que posi o pugui posar en perill la seguretat dels sistemes d'informació, haurà de comunicar aquesta incidència o anomalia a través dels canals de notificació establerts i d'acord amb els procediments aprovats. Aquest canals i procediments hauran de ser públics i coneguts.

<p>Ajuntament  de Barcelona</p>	<p><b>CRITERIS DE SEGURETAT DELS SISTEMES D'INFORMACIÓ I PROTECCIÓ DE DADES</b></p>
<p><b>Institut Municipal d'Informàtica</b></p>	<p><b>GUIA</b></p>
<p>Guia del Procediment de Notificació d'Incidències de Seguretat</p>	

## ÍNDEX

---

1.	ABAST .....	3
2.	INTRODUCCIÓ.....	3
3.	DEFINICIÓ D'INCIDÈNCIA DE SEGURETAT .....	4
4.	GUIA DEL PROCEDIMENT DE NOTIFICACIÓ D'INCIDÈNCIES DE SEGURETAT .....	5
4.1.	Qui ha de comunicar un incident de seguretat? .....	5
4.2.	Quan notificar un incident de seguretat? .....	5
4.3.	Cóm notificar un incident de seguretat? .....	5
4.4.	Per què s'han de comunicar els incidents de seguretat? .....	6
4.5.	Cóm puc saber si el meu cas és un incident de seguretat?.....	6
5.	REVISIÓ DE LA NORMA.....	7
6.	DOCUMENTS RELACIONATS .....	7
7.	GLOSSARI DE TERMES .....	7

<p>Ajuntament  de Barcelona</p>	<p><b>CRITERIS DE SEGURETAT DELS SISTEMES D'INFORMACIÓ I PROTECCIÓ DE DADES</b></p>
<p><b>Institut Municipal d'Informàtica</b></p>	<p>GUIA</p>
<p><b>Guia del Procediment de Notificació d'Incidències de Seguretat</b></p>	

## 1. ABAST

---

Els Personal Municipal i personal extern al servei de l'Administració Municipal dels Ens Municipals amb informàtica gestionada pel l'IMI.

## 2. INTRODUCCIÓ

---

Les incidències o anomalies de seguretat representen o poden representar un risc, i per tant hauran de ser gestionades amb l'objectiu de protegir els Sistemes d'Informació de l'Administració Municipal.


El Personal Municipal i personal extern al servei de l'Administració Municipal forma part activa en matèria de seguretat i per tant del bon ús de la seguretat dels recursos i actius de l'Administració Municipal. Com a part activa, té l'obligació de notificar els incidents de seguretat que pugui detectar.

Aquesta obligació ha quedat explicitada en les següents normes publicades a la Intranet Municipal i a la gasetta:

- [Instrucció d'ús de sistemes i tecnologies de la informació i comunicació](#) per part del personal al servei de l'Ajuntament de Barcelona, ha estat aprovada per la Gerència de Recursos Humans i Organització i publicada a la Gasetta Municipal del 28/02/2009.

Normes complementàries

- [Norma de Protecció de Dades](#) (NPD) aprovada per la Comissió Tècnica de Seguretat en Protecció de Dades de Caràcter Personal de l'Ajuntament de Barcelona en la seva sessió del 18 de març de 2009 i publicada a la Gasetta Municipal del 30/06/2009. Aquesta Comissió té les seves funcions delegades per l'Alcalde i té com a objectiu aprovar les Polítiques de Protecció de Dades que s'han de seguir dins de l'organització, presidida pel quart Tinent d'Alcalde i la Gerent Adjunta d'e-Administració i Sistemes d'Informació.
- [Norma Tècnica de Seguretat](#) (NTS) aprovada per l'IMI (11/06/2009) i publicada a la Gasetta Municipal del 30/06/2009, on s'estableixen els criteris tècnics de seguretat, és a dir, el conjunt de mecanismes tècnics i organitzatius que permeten garantir la confidencialitat, integritat i disponibilitat dels sistemes d'informació, així com la autenticitat, el no repudi i el compliment legal dels sistemes d'informació i comunicació de l'Ajuntament de Barcelona.

<p>Ajuntament  de Barcelona</p>	<p><b>CRITERIS DE SEGURETAT DELS SISTEMES D'INFORMACIÓ I PROTECCIÓ DE DADES</b></p>
<p>Institut Municipal d'Informàtica</p>	<p>GUIA</p>
<p><b>Guia del Procediment de Notificació d'Incidències de Seguretat</b></p>	

### **3. DEFINICIÓ D'INCIDÈNCIA DE SEGURETAT**

---

Té la consideració d'incidència de seguretat qualsevol anomalia que afecti a la seguretat de les dades o dels sistemes i xarxes que els suporten.

S'ha detectat un incompliment o vulneració de les normes internes en matèria de seguretat informàtica establertes per l'Ajuntament de Barcelona (**Criteris de Seguretat dels Sistemes d'Informació i Protecció de Dades**).


- S'ha detectat una vulneració d'algun dels aspectes bàsics que la seguretat informàtica pretén protegir: la confidencialitat, la integritat i la disponibilitat:

**Confidencialitat** : Accés no autoritzat ja sigui de forma intencional o no intencional a la informació. La pèrdua de la confidencialitat pot ocórrer de moltes maneres, com per exemple amb la publicació intencional d'informació confidencial de l'organització.

**Integritat** : modificacions per usuaris no autoritzats a les dades, informacions o processos; i que les dades i/o informacions siguin consistents tant interna com externament.

**Disponibilitat** : accés fiable i oportú a les dades, informacions o recursos per als usuaris apropiats.

- S'ha detectat una vulneració del compliment legal que sigui d'aplicació. Com per exemple: una vulneració de dades de caràcter personal de conformitat als preceptes legal o reglamentàriament establerts (LOPD 15/99 de 13 de desembre i el seu Reglament de desplegament RD 1720/2007 de 21 de desembre).

<p>Ajuntament  de Barcelona</p>	<p><b>CRITERIS DE SEGURETAT DELS SISTEMES D'INFORMACIÓ I PROTECCIÓ DE DADES</b></p>
<p>Institut Municipal d'Informàtica</p>	<p>GUIA</p>
<p>Guia del Procediment de Notificació d'Incidències de Seguretat</p>	

## **4. GUIA DEL PROCEDIMENT DE NOTIFICACIÓ D'INCIDÈNCIES DE SEGURETAT**

---

### **4.1. Qui ha de comunicar un incident de seguretat?**

Qualsevol persona que pertanyi o treballi per a l'Ajuntament de Barcelona, que detecti una incidència o anomalia que posi o pugui posar en perill la seguretat dels sistemes d'informació, te el deure de comunicar aquesta incidència o anomalia per al seu correcte registre i resolució, a través de línees de comunicació establertes amb aquest propòsit (Servei d'Atenció a l'Usuari).

- Cas que afecti a una persona individualment: l'ha de comunicar la pròpia persona.
- Cas que afecti a un col·lectiu: una persona representativa del col·lectiu (superior jeràrquic, responsable de client, referent d'informàtica del departament).
- Cas que afecti a un procés de negoci (aplicacions, llistats, etc.): la persona de la dependència que se'n faci càrrec habitualment o el seu superior jeràrquic.

### **4.2. Quan notificar un incident de seguretat?**

En el cas dels incidents de seguretat és molt important comunicar-los el més aviat possible per tal d'intentar minimitzar les seves repercussions.


### **4.3. Cóm notificar un incident de seguretat?**

Pels procediments estàndards de comunicació d'incidències de l'IMI indicant que es tracta d'un incident de seguretat.

**Trucant al 78234**

**Correu: IMI\_Entrada\_Incidencies**

Aquesta comunicació es fa a efectes de notificació i registre, els usuaris només hauran d'informar de les dades bàsiques que permetin tipificar la incidència. En el cas que per resoldre la incidència es necessiti informació addicional i/o pels incidents que comportin reportar informació crítica o confidencial, el personal de l'Oficina de Seguretat TIC de l'IMI es posarà en contacte amb la persona que ha notificat la incidència.

<p>Ajuntament  de Barcelona</p>	<p><b>CRITERIS DE SEGURETAT DELS SISTEMES D'INFORMACIÓ I PROTECCIÓ DE DADES</b></p>
<p>Institut Municipal d'Informàtica</p>	<p>GUIA</p>
<p><b>Guia del Procediment de Notificació d'Incidències de Seguretat</b></p>	

Excepcionalment, quan per motius de confidencialitat considereu que els canals estàndards no són els adients, haureu de comunicar l'incident directament al vostre Responsable de Client, qui s'encarregarà de comunicar-ho a l'Oficina de Seguretat TIC de l'IMI.

#### **4.4. Per què s'han de comunicar els incidents de seguretat?**


- És una obligació del personal recollida en les Instruccions internes publicades per la Direcció de RR.HH.
- Cas que l'incident de seguretat afecti a dades de caràcter personal es tracta d'una obligació legal.
- La comunicació dels incidents de seguretat es una bona pràctica reconeguda internacionalment com a mitjà per a millorar la seguretat dels Sistemes d'Informació.

#### **4.5. Cóm puc saber si el meu cas és un incident de seguretat?**

En cas de dubte sempre heu de comunicar l'incident i el personal especialitzat de l'IMI analitzarà si veritablement és un incident de seguretat.

No obstant, en la següent relació es troben la majoria dels incident de seguretat més habituals:

- Relacionats amb les contrasenyes (pèrdua, robatori, utilització de l'accés per part d'un altre usuari)
- Sospita que un tercer està accedint amb el nostre codi d'usuari i contrasenya.
- Esborrat accidental de dades i sol·licitud de recuperació de còpies de seguretat.
- Recepció de llistats amb el precinte de seguretat trencat.
- Pèrdua i/o robatori de llistats.
- Pèrdua i/o robatori de suports amb dades (disquets, cintes, pendrives etc.)
- Pèrdua i/o robatori de dispositius (Portàtils, ordinadors, pda's, telèfons mòbils, etc.)
- Pèrdua i/o robatori de targetes magnètiques, certificats digitals,
- Sospita d'intercepció, modificació, divulgació d'informació no autoritzada
- Pèrdua de dades

	<b>CRITERIS DE SEGURETAT DELS SISTEMES D'INFORMACIÓ I PROTECCIÓ DE DADES</b>
<b>Institut Municipal d'Informàtica</b>	<b>GUIA</b>
<b>Guia del Procediment de Notificació d'Incidències de Seguretat</b>	

- Utilització no autoritzada d'equip, màquina o sistema
- Detecció d'un virus (software maliciós)
- Vulnerabilitat o irregularitats en productes de control d'accés
- Intent d'accés no autoritzat al sistema
- Mal ús dels recursos de màquina, xarxa o servei en general
- etc..

## 5. REVISIÓ DE LA NORMA

---

El Comitè de Seguretat de l'IMI delega en l'Oficina de Seguretat TIC la revisió i actualització d'aquesta Guia.

En tot cas, aquesta guia haurà de ser revisada almenys un cop a l'any.

## 6. DOCUMENTS RELACIONATS


---

Nom del component	Vincle
Norma General	<a href="#">Instrucció d'ús de sistemes i tecnologies de la informació i comunicació</a> per part del personal al servei de l'Ajuntament de Barcelona , ha estat aprovada per la Gerència de Recursos Humans i Organització i publicada a la Gasetta Municipal del 28/02/2009.
Norma Específica	<a href="#">Norma de Protecció de Dades</a> (NPD) aprovada per la Comissió Tècnica de Seguretat en Protecció de Dades de Caràcter Personal de l'Ajuntament de Barcelona en la seva sessió del 18 de març de 2009 i publicada a la Gasetta Municipal del 30/06/2009..
Norma Específica	<a href="#">Norma Tècnica de Seguretat</a> (NTS) aprovada per l'IMI (11/06/2009) i publicada a la Gasetta Municipal del 30/06/2009.
Norma Específica	<a href="#">Incidències</a> de Seguretat Gestionades per l'IMI
Norma Operativa	<a href="#">Control d'incidències</a>
Procediment	<a href="#">Procediment de Comunicació i Gestió d'Incidències</a>

## 7. GLOSSARI DE TERMES

---

Consultar el [Glossari de Termes Global](#)

 <b>Ajuntament de Barcelona</b>	<b>CRITERIS DE SEGURETAT DELS SISTEMES D'INFORMACIÓ I PROTECCIÓ DE DADES</b>
<b>Institut Municipal d'Informàtica</b>	<b>INSTRUCCIÓ GENERAL</b>
<b>Comunicació i Gestió d'Incidències</b>	

<i>Control de versions</i>		
<b>Versió inicial</b>		
01	Elaboració versió inicial	
	Elaborat per:	Data:
	IMI- Oficina de Seguretat TIC / J.L. Rubiés	(04/12/2009)
	Revisat per:	Data:
	IMI – Responsable de Seguretat / Neus Bellavista	(11/12/2009)
	IMI – Comitè de Seguretat	(17/12/2009)
	Aprovat per:	Data:
Gerent de l'IMI / Lluís Olivella	(17/12/2009)	
<b>Versions modificades</b>		
02	Motiu del Canvi:	
	Modificat per:	Data:
	<Àrea>	(dd/mm/aaaa)
	Revisat per:	Data:
	<Àrees>	(dd/mm/aaaa)
	Aprovat per:	Data:
<Àrea>	(dd/mm/aaaa)	
03		