

# Auditoria del Servei de Certificació Digital. Qüestionari per als Ens subscriptors



## GESTIÓ DOCUMENTAL I ARXIU

1.1.1 Disposeu d'una metodologia d'arxiu i traçabilitat per la tramitació dels expedients diferent a la que proposa el Consorci AOC?

1.2.1 Es realitza una digitalització de la documentació?

1.3.1 Existeix un procediment de transferència d'expedients a l'arxiu central que defineix la periodicitat, el responsable i el mode d'enviament en cas que hagi de ser traslladat?

1.4.1 Els controls de seguretat física de l'arxiu són adequats? (No deixar cap document fora del seu expedient; Tancar amb clau l'arxivador i/o armari; Permetre l'accés a l'arxiu o al mobiliari d'arxiu només al personal autoritzat, etc.)

## OPERATIVA

Evidències dels CERTIFICATS seleccionats

2.1.1 Disposeu d'una fitxa ens subscriptor actualitzada a la situació actual i que d'aquesta manera garanteixi el compliment i hagi estat enviada en els darrers 2 anys?

2.2.1 Totes les persones que tenen algun rol en la sol·licitud i revocació de certificats tenen suficients coneixements sobre els procediments a seguir?

## SEGURETAT

### Seguretat física

3.1.1 Es realitza una revisió regular de les llistes d'accés per a assegurar-se que només persones autoritzades tinguin accés?

3.1.2 Hi ha sistemes de càmeres de seguretat instal·lats i operatius per a monitorar àrees clau?

3.1.3 Existeix personal de seguretat o guàrdies per a supervisar físicament les instal·lacions?

3.1.4 S'implementen mesures de seguretat física per a protegir dispositius d'emmagatzematge d'informació, com a servidors i unitats de suport?

3.1.5 Existeix un inventari actualitzat de tots els equips i actius relacionats amb la seguretat física?

### **Seguretat lògica**

3.2.1 Es revisen i actualitzen regularment les polítiques de seguretat lògica?

3.2.2 Se segueix un procés formal per a assignar i revocar privilegis d'accés?

3.2.3 S'implementen eines de monitoratge de seguretat per a detectar activitats inusuals?

3.2.4. Existeixen procediments per a respondre a esdeveniments de seguretat i possibles intrusions?

3.2.5 Es té un procés establert per a gestionar i aplicar pegats de seguretat?

3.2.6 Es realitza un seguiment de les vulnerabilitats conegudes i es prenen mesures per a mitigar-les?

3.2.7 Se segueixen pràctiques segures durant el desenvolupament de programari?

3.2.8 Es realitzen proves de seguretat i anàlisi de vulnerabilitats en les aplicacions desenvolupades internament?

3.2.9 Es realitza un seguiment post-incident per a aprendre i millorar les mesures de seguretat?

### **Seguretat de personal**

3.3.1 Existeix un procediment clar per a la notificació de pèrdua o robatori de dispositius que puguin contenir informació confidencial?

3.3.2 Es revisen regularment els permisos d'accés a mesura que canvien les responsabilitats laborals?

3.3.3 Es té un procés clar i segur al final de l'ocupació per a retirar els accessos i privilegis?

3.3.4 Es formen als empleats sobre les seves responsabilitats de seguretat en abandonar l'organització?

#### **Seguretat de l'arxiu**

3.4.1 Existeixen polítiques clares sobre el maneig d'arxius confidencials?

3.4.2 S'han realitzat proves de recuperació per a assegurar-se que els arxius poden restaurar-se eficaçment?

3.4.3 Existeixen nivells d'autorització clarament definits per a limitar l'accés segons els rols i les responsabilitats?