

**Procediment. Gestió i ús de Wildcard**

**Pla Director de Seguretat**



Índex

[1 Control del document 3](#_Toc487013305)

[1.1 Informació General 3](#_Toc487013306)

[1.2 Llista de Distribució 3](#_Toc487013307)

[1.3 Històric de canvis 3](#_Toc487013308)

[2 Introducció 4](#_Toc487013309)

[3 Objecte del Procediment 4](#_Toc487013310)

[4 Abast 4](#_Toc487013311)

[5 Vigència 5](#_Toc487013312)

[6 Revisió i avaluació 5](#_Toc487013313)

[7 Normativa de referència 5](#_Toc487013314)

[8 Rols i Responsabilitats 6](#_Toc487013315)

[9 Documents associats al procediment 6](#_Toc487013316)

[10 Conceptes generals 7](#_Toc487013317)

[10.1 Informació i Informació classificada 7](#_Toc487013318)

[10.2 Matèries classificades. 7](#_Toc487013319)

[10.2.1 Grau Secret 7](#_Toc487013320)

[10.2.2 Grau Reservat 8](#_Toc487013321)

[10.1 Matèries Objecte de Reserva Interna. 8](#_Toc487013322)

[10.1.1 Grau Confidencial 8](#_Toc487013323)

[10.1.2 Difusió limitada 8](#_Toc487013324)

# Control del document

## Informació General

|  |  |
| --- | --- |
| **Títol** | Procediment per a la Gestió i ús de Wildcards |
| **Versió** | 1.0 |
| **Creat per** | Comitè Operatiu |
| **Revisat per** | Responsable de Seguretat |
| **Aprovat per** | Comitè Executiu |
| **Nom del Fitxer** | aoc\_proc\_00\_gestio i us de wildcard v 0.0 |

## Llista de Distribució

|  | Organització |
| --- | --- |
| Personal del Consorci AOC | Intranet |
|  |  |
|  |  |
|  |  |

| Data | Autor | Raó de la modificació |
| --- | --- | --- |
| 31/12/2019 | Esperança Lopez | Creació del document |
| 16/11/2020 | Ivan Caballero | Actualització del document |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

## Històric de canvis

# Introducció

Els procediments associats a la Normativa de Seguretat del Consorci AOC són un conjunt de documents, que estableixen la forma de desenvolupar certs aspectes en matèria de seguretat.

Els procediments desenvolupen aspectes específics de la Normativa. En cas que el procediment pugi ser imprecís o contradictori en els seus termes i no s’indiqui com cal actuar en una certa circumstància caldrà adreçar-se a la Normativa corresponent, que és qui defineix la posició del Consorci AOC en aspectes concrets i serveixen per a indicar com s’ha d’actuar.

Els procediments contribueixen a:

* Facilitar el màxim aprofitament dels recursos i sistemes d’informació en les actuacions del Consorci AOC.
* Assegurar la protecció dels drets dels ciutadans en les seves relacions amb el Consorci AOC i el desenvolupament professionals dels empleats i usuaris que tenen accés als recursos i sistemes d’informació del Consorci AOC.
* Millorar els serveis que les administracions públiques presten als ciutadans, propiciant una gestió eficient i segura dels processos inclosos en els sistemes d’informació amb els que opera.
* Protegir als sistemes d’informació del Consorci AOC i les dades que tracten dels riscos que puguin derivar de l’acció humana, especialment a conductes incorrectes, inadequades o il·legals.

# Objecte del Procediment

L’objecte d’aquest Procediment és indicar com cal gestionar les Wildcards del Consorci AOC i els usos poden tenir.

Aquest procediment s’implantarà atenent al nivell de seguretat de la informació y els serveis prestats y la categoria dels sistemes d’informació del Consorci AOC.

Aquest document d’ús intern del Consorci AOC i per tant no podrà ser divulgat sense autorització del Responsable de Seguretat del Consorci AOC.

# Abast

Aquest Procediment és d’aplicació a tot l’àmbit d’actuació del Consorci AOC, i els continguts són derivats de les directrius de caràcter general definides a la Política de Seguretat de la Informació i de la Normativa de Seguretat del Consorci AOC.

Aquest procediment és d’aplicació i obligat compliment per a tot el personal que de forma permanent o eventual presti els seus serveis al Consorci AOC, i pel personal d’organitzacions externes, sempre i quan siguin usuaris o tinguin accés als sistemes d’informació del Consorci AOC.

# Vigència

Aquest Procediment ha estat aprovat pel Comitè Executiu de Seguretat del Consorci AOC, establint d’aquesta forma les directrius generals per a la classificació i posterior tractament de la informació del Consorci AOC.

Qualsevol modificació posterior entrarà en vigor immediatament després de la seva publicació a la intranet per part del Consorci AOC.

Les versions anteriors que s’hagin pogut distribuir constitueixen esborranys que s’han desenvolupat temporalment i no produeixen cap efecte.

# Revisió i avaluació

La gestió d’aquest Procediment correspon al Comitè Executiu del Consorci AOC.

El Comitè Operatiu del Consorci AOC, revisarà el present Procediment, que es sotmetrà, en cas d’haver modificacions, a l’aprovació del Comitè Executiu del Consorci AOC. El present procediment serà objecte de millora continuada.

La revisió estarà orientada tant a la identificació d’oportunitats de millora en la gestió de la seguretat de la informació, com a l’adaptació als canvis que hagin existit en el marc legal, infraestructura tecnològica, organització general, etc.

El Responsable de Seguretat és la persona encarregada de la custodia i divulgació de la versió aprovada d’aquest document.

# Normativa de referència

Aquest procediment complementa, als seus aspectes específics, a tota la Normativa del Consorci AOC.

# Rols i Responsabilitats

Les responsabilitats definides per les tasques contemplades al procediment són les següents:

| ROLS | RESPONSABILITATS |
| --- | --- |
| Usuaris | * Aplicar el present procediment |
| Responsable de Seguretat | * Totes les especificades a la Política de Seguretat del Consorci AOC. |
| Responsable del sistema | * Totes les especificades a la Política de Seguretat del Consorci AOC |
| Administrador / gestors de serveis, aplicacions,... | * Persones que detecten les necessitats dels diferents serveis, aplicacions, sistemes d’informació del Consorci AOC, són els responsables d’iniciar aquest procediment . |
| Unitat de Sistemes - Tecnologia | * Persones que aporten i posen en marxa la solució tecnològica |
| Unitat de Seguretat | * Realitzar les tasques que s’especifiquen al procediment |

# Documents i Eines associades al procediment

Les eines i documents associats a aquest procediment són:

* Repositori de peticions: JIRA.
* AOC\_PROC\_01\_incidents seguretat

# Conceptes generals

## Que és una Wildcard o Certificat Comodí?

Dins dels diferents camps o elements de seguretat inclosos en un certificat, destaca el nom o identificador de l’entitat (entorn, servidor o aplicació web) a la que està associada.

Per raons de confiança, és fonamental assegurar que els noms i entitats del certificat digital coincideixen i donen cobertura a tots els servidores web que fan ús del certificat, ja sigui:

* Amb una referència directa o única (com www.domini.cat), i una llista amb tots els noms dels servidors web (per exemple, www.domini.cat, portal.domini.cat i seu.domini.cat)
* Mitjançant una Wildcard o certificat digital comodí que agrupi tots els subdominis del domini principal (com \*.dominio.es)

*El certificat wildcard* identifica tots els subdominis associats a un domini determinat, sense necessitat d’adquirir i gestionar múltiples certificats electrònics. Por exemple, el certificat wildcard emès a: **\*.AOC.cat** garanteix la identitat de dominis com: negoci. AOC.cat, organització. AOC.cat , serveis. AOC.cat , direcció. AOC.cat , ...

### Seguretat associada a l’ús de Wildcards

La principal consideració en el moment de fer servir una wildcard, és que només hauria de ser utilitzat en servidors web amb el mateix nivell de seguretat , per tal de minimitzar l’impacte de possibles incidents de seguretat com l’accés a les claus privades vinculades al certificat digital. Per això caldria aplicar el principi de mínim privilegi, intentant reduir la necessitat de compartir el certificat digital i la clau privada entre diferents departaments, sistemes i persones.

Encara que es possible obtenir certificats digitals multi-domini, es a dir, vàlids per a servidors web de diferents dominis, pel mateix motiu (promoure el seu ús en entorns amb el mateix nivell de seguretat i disminuir les necessitats de compartir el Certificat digital i la clau privada), se recomana independitzar els certificats digitals per a cada domini.

D’altra banda, es recomana assegurar-se que el certificat digital inclou el nom del servidor web representat amb el domini.

L’ús de wildcards es habitual en CND’s (Content Delivery Networks) que gestionen el tràfic HTTPS destinat a múltiples servidors web d’una mateixa organització.

Des del punt de vista de seguretat en el cas d’especificar contrasenyes associades a Wildcards (certificats comodí), per simplicitat, HPKP (HTTP Public Key Pinning),s’hauria d’implementar per a la totalitat del domini i no només per a servidors web individuals, Per això caldria fer fer ús de la directiva “includeSubDomains”

## Necessitem una Wildcard?

Entre negoci i Tecnologia caldrà justificar la necessitat d’un certificat WildCard, i que la seva seguretat està reforçada.

Negoci haurà de justificar la necessitat:

1. Dificultat en la gestió de dominis, causat per
   1. Alta volumetria
   2. Manteniment Costós
2. Cost. Quan representa un alta despesa, ja que cal demanar un número alt de certificats.

Tecnologia, justifica el seu estat:

1. Verticalitat, que te a veure amb els servidors afectats. Quants menys servidor tinguin el certificat millor. Idealment hauria d’estar en un únic clúster de frontals.
2. Homogeneïtat de serveis, els serveis que es veuran afectats per l’ús de la wildcard, pel fet de compartir servidor.
3. No compartir altres wildcards. Allà on s’instal·li una wildcard no ha haver una altra.
4. És aconsellable revisar la configuració del frontal per si es pot augmentar la seguretat (seguretat reforçada). Aplicar algunes de les directives per assegurar la seguretat del certificat:
   * Per exemple aplicar HPKP (HTTP Public Key Pinning) amb la directiva de "includeSubDomains"
   * Expect CT (Certificate Transparency)

Si es donen tots els punts de la justificació (alta volumetria, alt cost, pocs servidors, serveis homogenis, etc.) el Responsable de del Sistema de Seguretat podrà aprovar la petició.

Si no es donen tots els punts de la justificació haurà de ser el Responsable de Seguretat qui aprovi la petició.

## Descripció del procediment

| Responsable | Acció |
| --- | --- |
| Cap de servei / Responsable de servei/ ... | * Obrir una petició al JIRA corporatiu, dins del projecte: ’Seguretat’ i component ‘Peticions a Seguretat’ * indicant la necessitat i aportant la justificació basant-se en la plantilla de l’Annex 1. |
| Responsable del sistema | * Valoració de la petició i justificació de la resposta. Si la justificació s’ajusta als supòsits que ja estan pre-aprovats, el responsable del sistema podà aprovar la petició. * Si el responsable del sistema no aprova la petició la escalarà al Responsable de Seguretat. |
| Responsable de Seguretat | * Valorarà la petició tenint en compte les justificacions i els riscos. |
| Cap de servei / Responsable de servei/ ... | * Cas de no conformitat. Desestimar o iniciar de nou el procediment. * Cas de conformitat. Procedir a la comprar del nou domini Wildcard, |
| Tecnologia | * Posada en marxa del nou domini amb les especificacions que es considerin adients. |
| Responsable del sistema | * Introduir la informació al Registre d’events de Seguretat indicant la excepció de fer servir aquest tipus de certificat. |

# Annex 1: Fitxa per d’acceptació de WildCard

La següent fitxa té com a finalitat l’acceptació per sol·licitar un wildcard i la seva documentació.

**Justificació**.

*Motivar quina és la justificació per demanar un certificat WildCard. Veure si s’ajusta als supòsits previstos al procediment: Alta volumetria de dominis, manteniment de certificats cost, despesa de certificats elevada.*

**Mitigació de riscos**

Serveis previstos:

*Indicar quins són els serveis previstos per aquest certificat*

Instal·lació del certificat

*Indicar quins són els sistemes on estarà instal·lat el certificat (identificat en quins frontals)*

Coincidència amb altres WildCards

*Indicar si ens sistemes on estarà instal·lat ja hi ha altres WildCards.*

Revisió de la seguretat del sistemes

*Indicar si s’ha revisat la configuració dels sistemes on estigui instal·lat*