**Procediment. Control i Gestió de vulnerabilitats**

**Pla Director de Seguretat**





Índex

[1 Control del document 3](#_Toc54339236)

[1.1 Informació General 3](#_Toc54339237)

[1.2 Llista de Distribució 3](#_Toc54339238)

[1.3 Històric de canvis 3](#_Toc54339239)

[2 Introducció 4](#_Toc54339240)

[3 Objecte del Procediment 4](#_Toc54339241)

[4 Abast 4](#_Toc54339242)

[5 Vigència 5](#_Toc54339243)

[6 Revisió i avaluació 5](#_Toc54339244)

[7 Normativa de referència 5](#_Toc54339245)

[8 Rols i Responsabilitats 6](#_Toc54339246)

[9 Eines i Documents associats al procediment 6](#_Toc54339247)

[10 Descripció del procediment 7](#_Toc54339248)

[10.1 Identificació de vulnerabilitats 7](#_Toc54339249)

[10.2 Valoració de vulnerabilitats 8](#_Toc54339250)

[10.3 Registre de les vulnerabilitats 8](#_Toc54339251)

[10.4 Correcció de vulnerabilitats 8](#_Toc54339252)

[10.5 Acord de nivell de servei 9](#_Toc54339253)

# Control del document

## Informació General

|  |  |
| --- | --- |
| **Títol** | Procediment de Control i Gestió de Vulnerabilitats |
| **Versió** | 1.0 |
| **Creat per** | Comitè operatiu |
| **Revisat per** | Responsable de Seguretat |
| **Aprovat per** | Comitè Executiu |
| **Nom del Fitxer** | AOC\_PROC\_00\_Control i Gestió de VulnerabilitatsV 2.0.docx |

## Llista de Distribució

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

| Data | Autor | Raó de la modificació |
| --- | --- | --- |
|  | Comitè Operatiu de seguretat | Creació del document |
|  |  |  |

## Històric de canvis

# Introducció

Els procediments associats a la Normativa de Seguretat del Consorci AOC és 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 es indicar com cal procedir en la gestió i control de les vulnerabilitats detectades als sistemes d’informació del Consorci AOC.

Una vulnerabilitat de seguretat de la informació és aquella errada present en el programari, maquinari, entorns físics o procediments, entre altres, que permeten a un atacant guanyar l’accés a un sistema d’informació, un servei Tic o una estació de treball o perjudicar o alterar el seu correcte funcionament i vulnerar les polítiques de seguretat aplicades sobre el mateix.

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 la gestió i control de les vulnerabilitats detectades que afectin als sistemes d’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.

És el Responsable de Seguretat 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 |
| --- | --- |
| 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 |
| Comitè executiu | * Totes les especificades a la Política de Seguretat del Consorci AOC |
| Comitè Operatiu | * Totes les especificades a la Política de Seguretat del Consorci AOC |
| Unitat de Sistemes | * Aplicar el present procediment |
| Unitat de Manteniment Intern | * Aplicar el present procediment |
| Unitat de Projectes | * Aplicar el present procediment |
| Unitat de Seguretat | * Aplicar el present procediment |
| Usuaris del Consorci AOC | * Aplicar el present procediment |

# Eines i Documents associats al procediment

Les eines i documents associats a aquest procediment són:

* Repositori de peticions: JIRA.
* Anàlisis de Vulnerabilitats realitzats trimestralment pel CESICAT
* Anàlisis de Vulnerabilitats realitzats internament pel Consorci AOC
* Guies del CESICAT per a la Gestió de vulnerabilitats
* Registre de vulnerabilitats

# Descripció del procediment

Cada dia es detecten noves vulnerabilitats de seguretat que afecten als diferents actius del Consorci AOC. Molts dels atacs produïts exploten vulnerabilitats per a les quals ja existeix una actualització que les solucionen o per les que es poden establir contramesures.

## Identificació de vulnerabilitats

Identificació de vulnerabilitats de manera proactiva.

Per tal de poder identificar vulnerabilitats proactivament cal:

* Mantenir un inventari d’actius actualitzat, ha de contenir la informació rellevant mínima per a poder gestionar les vulnerabilitats. Entre altres, contindrà dades com la adreça IP i/ó URL, el servei associat, el sistema operatiu, la versió i el grau d’actualització i interdependència amb els altres actius.
* Definir i implantar mecanismes per identificar les vulnerabilitats, des de la Unitat de Seguretat, que coordinarà l’anàlisi de vulnerabilitats externs i interns, acordant les finestres d’execució, la metodologia a seguir.
* Disposar de mecanismes que permetin recollir les vulnerabilitats detectades diàriament, com poden ser la subscripció a butlletins de fabricants o de organismes dedicats a la seguretat.
* Disposar dels anàlisis de vulnerabilitats, que realitza el CESICAT de forma planificada i amb caràcter trimestral que seran accessibles mitjançant el Portal de Seguretat dins d’EACAT.

|  |  |  |
| --- | --- | --- |
| **Tasca** | **Responsable** | **Periodicitat** |
| Mantenir inventari actius d’oficines actualitzat | Unitat de manteniment intern |  |
| Mantenir inventari actius de negoci actualitzat | Unitat de sistemes |  |
| Implantar mecanismes per identificar vulnerabilitats | Unitat de Seguretat |  |
| Executar els anàlisis de vulnerabilitats extern | CESICAT | Trimestral |
| Executar els anàlisis de vulnerabilitats intern | Unitat de sistemes | Mensual |

Identificació de vulnerabilitats de manera reactiva:

Les vulnerabilitats també es podran identificar per qualsevol altre canal (notificació d’un proveïdor o usuari, revisions de codi, tractament d’incidències, etc.) i hauran de tenir el mateix tractament que les identificades de manera proactiva.

Sigui quin sigui el mecanisme pel qual s’ha identificat una vulnerabilitat, la Unitat de Seguretat haurà d’estar informada de la mateixa, per tal de valorar, registrar i fer seguiment del tractament.

## Valoració de vulnerabilitats

A partir de la identificació d’una vulnerabilitat resultat dels anàlisis, cal prioritzat l’aplicació dels canvis que han de corregir la vulnerabilitat de seguretat identificada. Per tal de poder fer aquesta valoració es tenen en compte les variables següents:

* Nivell d’exposició a la xarxa pública de l’actiu / sistema d’informació / estació de treball que presenta la vulnerabilitat.
* Nivell de criticitat pública de l’actiu / sistema d’informació / estació de treball que presenta la vulnerabilitat.
* Nivell de criticitat de la vulnerabilitat.

|  |  |  |
| --- | --- | --- |
| **Tasca** | **Responsable** | **Periodicitat** |
| Valoració de la vulnerabilitat | Unitat de Seguretat |  |

## Registre de les vulnerabilitats

Totes les vulnerabilitats detectades seran registrades indicant la seva descripció, sistema afectat, valoració, estat i el seu tractament.

El registre ha de servir per fer seguiment dels tractament de les vulnerabilitats, evitar que es repeteixin i investigació forense de possibles incidents de seguretat.

El registre haurà d’indicar les vulnerabilitats que després del seu tractament es decideix acceptar sense mitigació per la seva relació cost/benefici.

|  |  |  |
| --- | --- | --- |
| **Tasca** | **Responsable** | **Periodicitat** |
| Registre de la vulnerabilitat | Unitat de Seguretat |  |

## Correcció de vulnerabilitats

Un cop registrada la vulnerabilitat cal procedir a la seva correcció:

* El tractament de les vulnerabilitats es faran via tiquet de JIRA. Qualsevol podrà obrir un tiquet pel tractament d’un vulnerabilitat, però la Unitat de Seguretat haurà d’estar informada per valorar i registrar la vulnerabilitat.
* El responsable de la correcció de la vulnerabilitat podran ser les unitats de Sistemes, de Manteniment Intern o de Projectes.
* La unitat responsable de la correcció haurà de respectar els terminis acordats al punt *10.5 Acord de nivell de servei.* Haurà d’estimar la data en que la vulnerabilitat pot estar corregida per tal que el Responsable de Seguretat valori si el risc és assumible o si cal prioritzar tasques o aplicar mesures mitigatòries del risc.
* La unitat de seguretat o el responsable de la correcció, podran proposar l’aplicació d’altres mesures per mitigar el risc que comporta la vulnerabilitat durant el temps de correcció.
* En el cas de que la vulnerabilitat no es pugui corregir, o que pel seu risc el cost no compensi el benefici, caldrà que el Responsable de Seguretat decideixi si s’accepta la vulnerabilitat. En aquest cas es registrarà dins del Registre de Vulnerabilitats.

|  |  |
| --- | --- |
| **Tasca** | **Responsable** |
| Obrir tiquet al responsable de la correcció | Unitat de Seguretat |
| Aplicar els canvis necessaris per al correcció de la vulnerabilitat. D’acord amb els SLA | Unitats de sistemes, de Manteniment Intern o de Projectes. |
| Acceptar vulnerabilitats | Responsable de Seguretat |
| Proposar mesures de seguretat de cara a minimitzar la possibilitat de que la vulnerabilitat sigui explotada | Unitat de Seguretat i unitat responsable de la correcció |

## Acord de nivell de servei

|  |  |
| --- | --- |
| **Classificació** | **Temps de resposta** |
| Crítiques | 48h |
| Altes | 48h |
| Mitges | 1 setmana |
| Baixes | 1 setmana |

NOTA: es considera **Temps de Resposta** al temps transcorregut des de que s’identifica la vulnerabilitat fins que s’estima la data de resolució de la mateixa. Per tant, inclou les tasques de identificació, valoració, registre i correcció fins que el responsable de la correcció estima la data de correcció.