DIGITALIZA

Asunción, 17 de Abril de 2026

*Señores*
**Ministerios del Ambiente y Desarrollo Sostenible**
PRESENTE

***Referencia:***
***"Solución integrada para repositorio de documentos y gestiones institucionales del MADES"***
***– ID N° 459.851-***

A través del presente, hacemos entrega del informe técnico detallado en base al cronograma de trabajos a realizarse en el marco del mantenimiento de la solución integrada para repositorio de documentos y gestiones institucionales del MADES.

A continuación, se detalla los servicios en ejecución e inventario de servidores.

## Inventario de Servidores

| | |
|---|---|
| **Servidor** | VM1 — OpenKM |
| **CPU** | 4 Cores a 2.8 GHz |
| **RAM** | 16 GB |
| **HD** | 1 TB |
| **Distro** | Ubuntu LTS 22.04 |
| **IP** | 10.5.0.139 |

| | |
|---|---|
| **Servidor** | VM2 — APIs |
| **CPU** | 4 Cores a 2.8 GHz |
| **RAM** | 8 GB |
| **HD** | 256 GB |
| **Distro** | Ubuntu LTS 22.04 |
| **IP** | 10.5.0.142 |

| | |
|---|---|
| **Servidor** | VM3 — Base de Datos |
| **CPU** | 4 Cores a 2.8 GHz |
| **RAM** | 8 GB |
| **HD** | 512 GB |
| **Distro** | Ubuntu LTS 22.04 |
| **IP** | 10.5.0.144 |

## Reporte Servidor VM1

### Evidencia de distribución de disco

Lic. Gustavo Silvio López Aranda
Director
Dirección de Sistema Informático
MADES

Denisse Matto
Administradora de Contratos
Dirección Administrativa
MADES

17-04-26

```
Filesystem                         Size  Used Avail Use% Mounted on
tmpfs                              1.6G  1.4M  1.6G   1% /run
/dev/mapper/ubuntu--vg-ubuntu--lv 1006G   24G  940G   3% /
tmpfs                              7.9G     0  7.9G   0% /dev/shm
tmpfs                              5.0M     0  5.0M   0% /run/lock
/dev/sda2                          2.0G  256M  1.6G  14% /boot
tmpfs                              1.6G  4.0K  1.6G   1% /run/user/1000
```

## Versión y actualizaciones pendientes del S.O.

Ubuntu 22.04.5 LTS

```
Welcome to Ubuntu 22.04.5 LTS (GNU/Linux 5.15.0-135-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

 System information as of Thu Apr 16 07:36:47 PM UTC 2026

  System load:  0.81               Processes:             182
  Usage of /:   2.4% of 1005.39GB  Users logged in:       0
  Memory usage: 44%                IPv4 address for ens160: 10.5.0.139
  Swap usage:   0%

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster deployment.

   https://ubuntu.com/engage/secure-kubernetes-at-the-edge

Expanded Security Maintenance for Applications is not enabled.

19 updates can be applied immediately.
8 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

9 additional security updates can be applied with ESM Apps.
Learn more about enabling ESM Apps service at https://ubuntu.com/esm

New release '24.04.4 LTS' available.
Run 'do-release-upgrade' to upgrade to it.
```

## Versión del Servidor Web

Tomcat 9

```
● openkm.service - OpenKM - https://www.openkm.com/
     Loaded: loaded (/etc/systemd/system/openkm.service; enabled; vendor preset: enabled)
     Active: active (running) since Mon 2025-03-31 15:43:20 UTC; 1 year 0 months ago
   Main PID: 923 (java)
      Tasks: 103 (limit: 19055)
     Memory: 9.1G
        CPU: 3d 21h 25min 19.813s
     CGroup: /system.slice/openkm.service
             └─923 /usr/bin/java -Djava.util.logging.config.file=/opt/openkm/tomcat-9.0.99/conf/logging.propertie

Mar 31 15:43:20 digitalizaopenkm systemd[1]: Starting OpenKM - https://www.openkm.com/...
Mar 31 15:43:20 digitalizaopenkm bash[819]: Existing PID file found during start.
Mar 31 15:43:20 digitalizaopenkm bash[819]: Removing/clearing stale PID file.
Mar 31 15:43:20 digitalizaopenkm bash[819]: Tomcat started.
Mar 31 15:43:20 digitalizaopenkm systemd[1]: Started OpenKM - https://www.openkm.com/.
lines 1-15/15 (END)
```

## Configuraciones SSL, red y proxy

El tráfico SSL saliente y entrante es administrado por el administrador local a través de ProxyPass SSL.

## Verificación de Repositorio

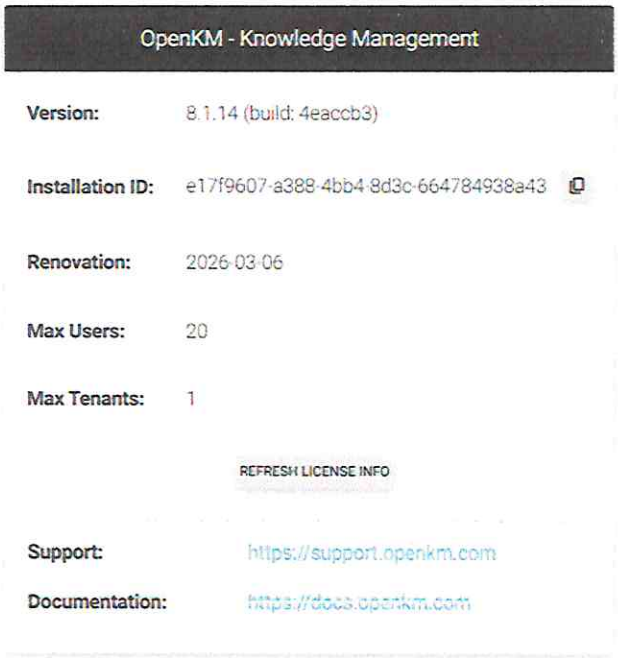
- Validación de los Nodos del sistema (registros, carpetas y documentos): Validado
- Verificación de nodos huérfanos — reindexados: Verificado
- Verificación de Índices: Verificado
- Verificación de Checksums: Verificado

*No se observan problemas. Se adjunta archivo log para verificación.*

Lic. Gustavo Silvio López Aranda
Director
Dirección de Sistema Informático
MADES

## Actualización

Versión inicial de OpenKM: 8.1.14




# Reporte Servidor VM2

## Evidencia de distribución de disco

```
Filesystem                         Size  Used Avail Use% Mounted on
tmpfs                              794M  2.1M  792M   1% /run
/dev/mapper/ubuntu--vg-ubuntu--lv   44G   19G   24G  45% /
tmpfs                              3.9G     0  3.9G   0% /dev/shm
tmpfs                              5.0M     0  5.0M   0% /run/lock
/dev/sda2                          1.7G  256M  1.4G  16% /boot
tmpfs                              794M  4.0K  794M   1% /run/user/1000
overlay                             44G   19G   24G  45% /var/lib/docker/overlay2/
overlay                             44G   19G   24G  45% /var/lib/docker/overlay2/
overlay                             44G   19G   24G  45% /var/lib/docker/overlay2/
overlay                             44G   19G   24G  45% /var/lib/docker/overlay2/
overlay                             44G   19G   24G  45% /var/lib/docker/overlay2/
overlay                             44G   19G   24G  45% /var/lib/docker/overlay2/
overlay                             44G   19G   24G  45% /var/lib/docker/overlay2/
```

## Versión y actualizaciones pendientes del S.O.

Ubuntu 22.04.5 LTS

MINISTERIO DEL AMBIENTE Y DESARROLLO SOSTENIBLE
Dirección de Sistemas
Lic. Gustavo Silvio Lopez Aranda
Director
Dirección de Sistema Informático
MADES

```
Welcome to Ubuntu 22.04.5 LTS (GNU/Linux 5.15.0-134-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

 System information as of Thu Apr 16 04:52:01 PM -03 2026

  System load:  2.31               Processes:               289
  Usage of /:   43.0% of 43.44GB   Users logged in:         1
  Memory usage: 17%                IPv4 address for ens160: 10.5.0.142
  Swap usage:   0%

  => There is 1 zombie process.

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster deployment.

   https://ubuntu.com/engage/secure-kubernetes-at-the-edge

Expanded Security Maintenance for Applications is not enabled.

8 updates can be applied immediately.
8 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

1 additional security update can be applied with ESM Apps.
Learn more about enabling ESM Apps service at https://ubuntu.com/esm

New release '24.04.4 LTS' available.
Run 'do-release-upgrade' to upgrade to it.
```

## Versión del Servidor Web

nginx

```
● nginx.service - A high performance web server and a reverse proxy server
     Loaded: loaded (/lib/systemd/system/nginx.service; enabled; vendor preset: enabled)
     Active: active (running) since Thu 2026-04-16 16:51:27 -03; 1min 38s ago
       Docs: man:nginx(8)
    Process: 1427354 ExecStartPre=/usr/sbin/nginx -t -q -g daemon on; master_process on; (code=exited, status=0/SUCCESS)
    Process: 1427392 ExecStart=/usr/sbin/nginx -g daemon on; master_process on; (code=exited, status=0/SUCCESS)
   Main PID: 1427393 (nginx)
      Tasks: 5 (limit: 9393)
     Memory: 6.5M
        CPU: 42ms
     CGroup: /system.slice/nginx.service
             ├─1427393 "nginx: master process /usr/sbin/nginx -g daemon on; master_process on;"
             ├─1427394 "nginx: worker process" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" ""
             ├─1427395 "nginx: worker process" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" ""
             ├─1427396 "nginx: worker process" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" ""
             └─1427397 "nginx: worker process" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" ""

Apr 16 16:51:27 ita systemd[1]: Starting A high performance web server and a reverse proxy server...
Apr 16 16:51:27 ita systemd[1]: Started A high performance web server and a reverse proxy server.
```

## Servicios Expuestos

```
IMAGE
        NAMES
grafana/loki:latest
0/tcp   loki-main
gitl.digitaliza.com.py:5050/mades/generador_expedientes:main
        api-main
prom/prometheus
        prometheus-main
7173367b6f48
        api-stage
```

```
PORTS

0.0.0.0:3100->3100/tcp,

0.0.0.0:3000->3000/tcp

0.0.0.0:9090->9090/tcp

3000/tcp, 0.0.0.0:3001->
```

## Verificación de los Servicios

Se realizaron llamadas a todos los servicios expuestos con respuestas satisfactorias y esperadas.

Lic. Gustavo Silvio López Aranda
Director
Dirección de Sistema Informático
MADES

```
## Login

### CURL

```curl

curl --location 'http://ita.mades.gov.py:3443/usuarios/login' \
--header 'Content-Type: application/json' \
--data '{
    "usuario": "mades",
    "password": "BiDxyYnVivsbgt1I"
}'

```

### RESPONSE

```json
{
    "mensaje": "Usuario Logueado",
    "token": "eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXV....."
}
```

## Crear Expediente

### CURL

```curl
curl --location 'http://ita.mades.gov.py:3443/expedientes' \
--header 'Authorization: â€¢â€¢â€¢â€¢â€¢â€¢â€¢â€¢â€¢â€¢' \
--form 'fecha="2025-03-21"' \
--form 'nroResolucion="Nro Resolucion Prueba"' \
--form 'nroControl="00123456789012345678901"' \
--form 'proyecto="Proyecto prueba"' \
--form 'propiedad="Propiedad Prueba"' \
--form 'finca="Finca Prueba"' \
--form 'padron="Padron Prueba"' \
--form 'distrito="Distrito Prueba"' \
--form 'departamento="Departamento Prueba"' \
--form 'expNro="Exp Nro Prueba"' \
--form 'resolucion="Resolucion Prueba"' \
--form 'documento=@"/media/guillermo/Storage/Stuff/expediente_88-2024.docx"'
```

### RESPONSE

```json
{
    "mensaje": "Datos recibidos con exito",
    "data": {
        "uuid": "6260aae5-4075-4c47-afdc-1e74aceb29e5"
    }
}
```

## Obtener Expediente

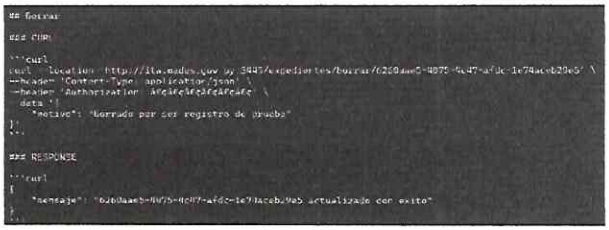
### CURL

```curl
curl --location 'http://ita.mades.gov.py:3443/expedientes/6260aae5-4075-4c47-afdc-1e74aceb29e5' \
--header 'Authorization: â€¢â€¢â€¢â€¢â€¢â€¢â€¢â€¢â€¢â€¢'
```

### RESPONSE

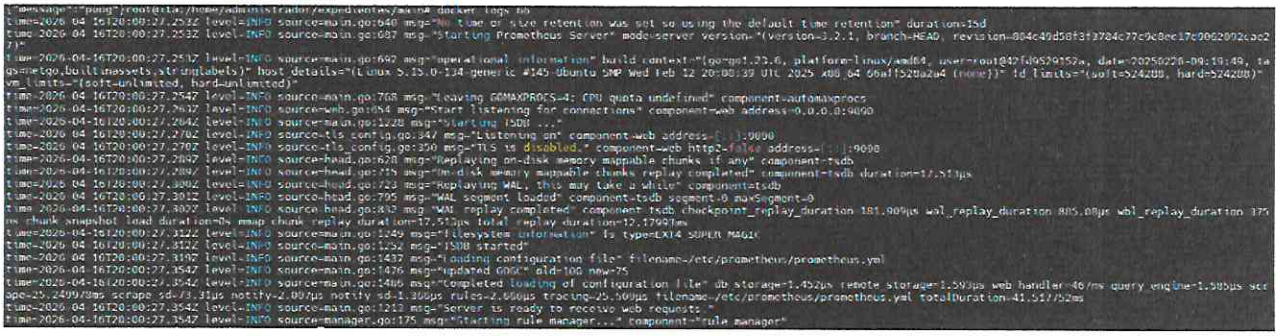
```json
{
    "mensaje": "pdf Generado con exito",
    "data": {
        "id": "6260aae5-4075-4c47-afdc-1e74aceb29e5",
        "fecha": "2025-03-21",
        "nroResolucion": "Nro Resolucion Prueba",
        "proyecto": "Proyecto prueba",
        "propiedad": "Propiedad Prueba",
        "finca": "Finca Prueba",
        "padron": "Padron Prueba",
        "distrito": "Distrito Prueba",
        "departamento": "Departamento Prueba",
        "expNro": "Exp Nro Prueba",
        "consultor": "Consultor Prueba",
```

MINISTERIO DEL AMBIENTE Y DESARROLLO SOSTENIBLE
Dirección de Sistema Informático
Lic. Gustavo Silvio López Aranda
Director
Dirección de Sistema Informático
MADES
```



## Servicio de Monitoreo

Los servicios de Grafana y Loki de monitoreo y recolección de logs están en correcto funcionamiento.



## Servicios Actualizados

Se procedió a realizar mejoras en los servicios. Los detalles se encuentran en el Anexo I de este documento.

Lic. Gustavo Silvio López Aranda
Director
Dirección de Sistema Informático
MADES

DIGITALIZA

# Reporte Servidor VM3

## Evidencia de distribución de disco

```
Filesystem                         Size  Used Avail Use% Mounted on
tmpfs                              794M  1.6M  793M   1% /run
/dev/mapper/ubuntu--vg-ubuntu--lv   98G  9.7G   84G  11% /
tmpfs                              3.9G  1.1M  3.9G   1% /dev/shm
tmpfs                              5.0M     0  5.0M   0% /run/lock
/dev/sda2                          2.0G  259M  1.6G  15% /boot
tmpfs                              794M  4.0K  794M   1% /run/user/1000
```

## Versión y actualizaciones pendientes del S.O.

Ubuntu 22.04.5 LTS

```
Welcome to Ubuntu 22.04.5 LTS (GNU/Linux 5.15.0-133-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

 System information as of Thu Apr 16 08:27:49 PM UTC 2026

  System load:  0.09              Processes:             206
  Usage of /:   9.8% of 97.87GB   Users logged in:       2
  Memory usage: 13%               IPv4 address for ens160: 10.5.0.144
  Swap usage:   0%

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster deployment.

   https://ubuntu.com/engage/secure-kubernetes-at-the-edge

Expanded Security Maintenance for Applications is not enabled.

12 updates can be applied immediately.
8 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status
```

## Servicios Corriendo

PostgreSQL

```
● postgresql.service - PostgreSQL RDBMS
     Loaded: loaded (/lib/systemd/system/postgresql.service; enabled; vendor preset: enabled)
     Active: active (exited) since Thu 2025-02-27 17:45:56 UTC; 1 year 1 month ago
   Main PID: 36924 (code=exited, status=0/SUCCESS)
        CPU: 3ms

Feb 27 17:45:56 srvbddigitaliza systemd[1]: Starting PostgreSQL RDBMS...
Feb 27 17:45:56 srvbddigitaliza systemd[1]: Finished PostgreSQL RDBMS.
```

## Informes Detallados del Estado de la Base de Datos

### Estado de Expedientes del día 15 de Abril 2026

MINISTERIO DEL AMBIENTE Y DESARROLLO SOSTENIBLE
Dirección de Sistema Informático
Lic. Gustavo Silvio Lopez Arafua
Director
Dirección de Sistema Informático
MADES

```
expedientes_main=# SELECT
  e.id_estado,
  est.nombre AS estado,
  COUNT(*) AS cantidad
FROM
  tbl_expedientes e
JOIN
  tbl_estado_expediente est ON e.id_estado = est.id
WHERE
  DATE(e.fecha_creacion AT TIME ZONE 'America/Asuncion') = CURRENT_DATE -1
GROUP BY
  e.id_estado, est.nombre
ORDER BY
  cantidad DESC;
 id_estado |       estado       | cantidad
-----------+--------------------+----------
         4 | Expediente Firmado |       70
(1 row)
```

### Estado de Expedientes — últimos 7 días

```
expedientes_main=# SELECT
  DATE(e.fecha_creacion AT TIME ZONE 'America/Asuncion') AS fecha,
  est.nombre AS estado,
  COUNT(*) AS cantidad
FROM
  tbl_expedientes e
JOIN
  tbl_estado_expediente est ON e.id_estado = est.id
WHERE
  e.fecha_creacion >= CURRENT_DATE - INTERVAL '7 days'
GROUP BY
  DATE(e.fecha_creacion AT TIME ZONE 'America/Asuncion'),
  est.nombre
ORDER BY
  fecha DESC, cantidad DESC;
   fecha    |       estado       | cantidad
------------+--------------------+----------
 2026-04-16 | Recibido           |       60
 2026-04-16 | Expediente Firmado |        7
 2026-04-15 | Expediente Firmado |       70
 2026-04-14 | Expediente Firmado |       12
 2026-04-13 | Expediente Firmado |       41
 2026-04-10 | Expediente Firmado |       65
 2026-04-10 | Expediente Borrado |        1
 2026-04-09 | Expediente Firmado |       58
 2026-04-09 | Expediente Borrado |        1
 2026-04-09 | Recibido           |        1
(10 rows)
```

### Estado de Expedientes acumulados por mes

```
expedientes_main=# SELECT
  est.nombre AS estado,
  COUNT(*) AS cantidad
FROM
  tbl_expedientes e
JOIN
  tbl_estado_expediente est ON e.id_estado = est.id
WHERE
  DATE_TRUNC('month', e.fecha_creacion AT TIME ZONE 'America/Asuncion') = DATE_TRUNC('month', CURRENT_DATE)
GROUP BY
  est.nombre
ORDER BY
  cantidad DESC;
       estado       | cantidad
--------------------+----------
 Expediente Firmado |      419
 Recibido           |       61
 Expediente Borrado |        5
(3 rows)
```

## Conclusión

- Se observaron actualizaciones pendientes en las 3 máquinas virtuales, las cuales fueron aplicadas.
- Los servidores se encuentran en correcto funcionamiento y son monitoreados 24/7 por el sistema de alertas y logs.

Lic. Gustavo Silvio Lopez Aranda
Director
Dirección de Sistema Informático
MADES

- Se prevé un mantenimiento continuo de actualizaciones y nuevas funcionalidades de acuerdo con lo solicitado por la convocante.

Sin otro particular, nos despedimos atentamente.

Lic. Gustavo Silvio López Aranda
Director
Dirección de Sistema Informático
MADES

**Armando Insfran**
Digitaliza S.A.

Lic. Gustavo Silvio López Aranda
Director
Dirección de Sistema Informático
MADES

DIGITALIZA

# ANEXO I

## Reporte de Mejoras de Seguridad y Optimización

*Generador de Expedientes — MADES*

| | |
|---|---|
| **Proyecto** | Generador de Expedientes (MADES) |
| **Período analizado** | 10 de septiembre de 2025 — 16 de abril de 2026 |
| **Fecha de emisión** | 16 de abril de 2026 |
| **Fuente de datos** | Historial de commits del repositorio Git del proyecto |
| **Alcance** | Mejoras implementadas en materia de seguridad y optimización |

## 1. Introducción

El presente documento constituye un relevamiento objetivo de las mejoras incorporadas al sistema Generador de Expedientes durante el período comprendido entre el 10 de septiembre de 2025 y el 16 de abril de 2026.

El informe se ha estructurado en dos categorías principales:

- Mejoras de seguridad: cambios cuyo objetivo primario es reducir riesgos de confidencialidad, integridad o autenticación.
- Mejoras de optimización: cambios cuyo objetivo primario es mejorar el rendimiento, la eficiencia de recursos o la confiabilidad operativa del sistema.

En el período analizado se registraron 28 mejoras en total, de los cuales 5 corresponden a mejoras de seguridad y 5 a mejoras de optimización consolidadas.

## 2. Mejoras de Seguridad

### 2.1. Mitigación de ataque a la cadena de suministro en dependencia axios

**Fecha:** 31 de marzo de 2026

**Archivos modificados:** package.json

**Descripción técnica**

Se fijó la versión de la dependencia axios a la versión 1.8.4, reemplazando el rango semántico anterior (^1.7.9). Este cambio responde a un ataque a la cadena de suministro detectado el 30 de marzo de 2026, mediante el cual la versión 1.14.1 de axios incorporó una dependencia maliciosa identificada como plain-crypto-js.

**Impacto sobre la seguridad**

La fijación de la versión impide que actualizaciones automáticas del ecosistema Node.js instalen versiones comprometidas de la biblioteca cliente HTTP utilizada por el sistema.

### 2.2. Validación previa de credenciales de token contra API externa

**Fecha:** 30 de enero de 2026

**Archivos modificados:** src/controllers/expedienteController.js, src/utils/firmador.js

**Descripción técnica**

Lic. Gustavo Silvio López Aranda
Director
Dirección de Sistema Informático
MADES

Se incorporó la función verifyCredentials() en el módulo src/utils/firmador.js, la cual realiza una validación de las credenciales (usuario, contraseña y PIN) contra un servicio externo de verificación (parámetro de entorno VERIFY_PIN_URL) antes de enviar el trabajo de firma al Módulo de Seguridad por Hardware (HSM). La lógica de control incorpora el manejo diferenciado de los estados de error: "Token not found", "Pin invalid", "Invalid credentials" y "Authentication refused".

**Impacto sobre la seguridad**

El sistema verifica la validez de las credenciales antes de comprometer recursos del HSM, reduciendo la exposición de credenciales inválidas ante el servicio de firma y permitiendo una diferenciación precisa de los fallos de autenticación.

### 2.3. Detección de errores de autenticación en cuerpo de respuesta

**Fecha:** 29 de enero de 2026

**Archivos modificados:** src/utils/firmador.js

**Descripción técnica**

Se añadió validación del cuerpo crudo (raw body) de las respuestas de la API de firma para identificar mensajes de error embebidos aun cuando la respuesta HTTP presente un código de estado 200. Se detectan los patrones: "Invalid credentials", "Authentication refused", "Token not found", "insufficient credits" y "No tiene créditos".

**Impacto sobre la seguridad**

Se previene que fallos de autenticación sean interpretados erróneamente como operaciones exitosas en escenarios donde el servicio externo retorna códigos de respuesta no conformes con el estándar.

### 2.4. Eliminación del registro de sentencias SQL en logs

**Fecha:** 22 de diciembre de 2025

**Archivos modificados:** config/database.js

**Descripción técnica**

Se modificó la configuración de Sequelize para desactivar el registro (logging) de las sentencias SQL y sus parámetros. El parámetro logQueryParameters: true fue reemplazado por logging: false tanto en el entorno de producción como en el entorno de pruebas.

**Impacto sobre la seguridad**

Se mitiga el riesgo de divulgación de información sensible (information disclosure) a través de los registros del sistema, impidiendo que parámetros de consultas —potencialmente portadores de datos personales o credenciales— queden expuestos en archivos de log.

### 2.5. Verificación del certificado SSL en endpoints de la API CONFIRMA

**Fecha:** 17 de septiembre de 2025

**Archivos modificados:** src/utils/firmador.js

**Descripción técnica**

Se incorporó la configuración de un agente HTTPS con verificación explícita de certificados en las tres funciones que consumen la API CONFIRMA: signWithNewAPI(), login() y sign(). La verificación se controla mediante la variable de entorno NODE_TLS_REJECT_UNAUTHORIZED. El comportamiento por defecto rechaza conexiones con certificados no autorizados, manteniendo la seguridad en producción.

**Impacto sobre la seguridad**

Lic. Gustavo Silvio Lopez Aranda
Director
Dirección de Sistema Informático
MADES

Se reduce el riesgo de ataques de tipo Man-in-the-Middle (MITM) sobre las comunicaciones HTTPS con los servicios de firma y de sellado de tiempo (signbox.confirma.com.py, timestamp.confirma.com.py). Este cambio se encuentra respaldado por el documento técnico de seguridad TLS incorporado al repositorio en diciembre de 2025.

## 3. Mejoras de Optimización

### 3.1. Refactorización a operaciones en memoria de la función signWithNewAPI

**Fecha:** 18 de septiembre de 2025

**Archivos modificados:** src/utils/firmador.js

**Descripción técnica**

Se eliminaron todas las operaciones de entrada/salida sobre el sistema de archivos (fs.createWriteStream, fs.readFileSync, fs.unlinkSync) dentro del flujo de firma. El procesamiento del PDF se reemplazó por una conversión directa de stream a buffer en memoria, incluyendo validación del tamaño del buffer.

**Impacto sobre el rendimiento**

- Se suprimen múltiples operaciones de disco por cada solicitud de firma.
- Se eliminan condiciones de carrera asociadas a la sincronización del sistema de archivos.
- Se reduce la contención de disco bajo procesamiento concurrente.

### 3.2. Transmisión directa del PDF mediante stream en la nueva API de firma

**Fecha:** 28 de noviembre de 2025

**Archivos modificados:** src/utils/firmador.js

**Descripción técnica**

Se reemplazó el patrón previo de acumulación de chunks en memoria (Buffer.concat) por la transmisión directa del stream del archivo al FormData, eliminando la etapa intermedia de bufferizado completo del PDF.

**Impacto sobre el rendimiento**

- Se elimina el uso de memoria proporcional al tamaño del archivo para archivos de gran tamaño.
- Se resuelve una condición de carrera en la cual el stream de respuesta de axios podía perder datos antes de la vinculación de los detectores de eventos, causando envíos de archivo vacíos.

### 3.3. Refactorización del sistema de callback para procesamiento en memoria

**Fecha:** 17 de septiembre de 2025

**Archivos modificados:** src/controllers/callbackController.js, src/controllers/expedienteController.js, src/utils/firmador.js, src/utils/okm.js

**Descripción técnica**

Se eliminó el uso de fs.createWriteStream y fs.readFileSync en el controlador de callbacks. La recepción del archivo PDF se realiza mediante la recolección de chunks en un arreglo en memoria, consolidados posteriormente mediante Buffer.concat. Se estandarizó el formato de nombre de archivo manteniendo compatibilidad retroactiva.

**Impacto sobre el rendimiento**

- Se eliminan operaciones de E/S sobre disco en cada callback recibido.

Lic. Gustavo Silvio López Aranda
Director
Dirección de Sistema Informático
MADES

- Se reduce la contención del sistema de archivos bajo concurrencia.

### 3.4. Corrección del manejo de streams en la carga de archivos a OpenKM

**Fecha:** 18 de septiembre de 2025

**Archivos modificados:** src/utils/okm.js

**Descripción técnica**

Se reemplazó el patrón PassThrough por Readable en la construcción del stream utilizado para la carga de archivos a OpenKM a través de FormData. Se incorporó el parámetro filename en la llamada FormData.append() para asegurar los metadatos correctos del multipart.

**Impacto sobre el rendimiento y confiabilidad**

- Se resuelve el error dataSize:0 que generaba cargas de archivos vacíos a OpenKM.
- Se previene la excepción NullPointerException del lado del servidor OpenKM.

### 3.5. Eliminación de valores por defecto para puertos de escucha

**Fecha:** 18 de septiembre de 2025

**Archivos modificados:** app.js, index.js

**Descripción técnica**

Se eliminaron los valores por defecto embebidos (puertos 3000 y 3001) en la configuración del puerto de escucha del servicio. La variable PORT fue reemplazada por API_PORT, obligando a la configuración explícita mediante variables de entorno.

**Impacto sobre la operación**

- Se asegura la consistencia de la configuración entre los entornos de stage y producción.
- Se previene la asignación automática de puertos en ausencia de configuración explícita, evitando conflictos de despliegue.

## 4. Mejoras de Refinamiento Técnico

Durante el mes de septiembre de 2025 se registraron múltiples mejoras iterativas orientados a la depuración y refinamiento de las optimizaciones descritas en los puntos 3.1, 3.3 y 3.4. Se listan por completitud documental:

| Fecha | Descripción |
|---|---|
| 17/09/2025 | Corrección del parámetro filename faltante en FormData. |
| 17/09/2025 | Corrección de metadatos de stream en FormData mediante conversión a buffer. |
| 17/09/2025 | Implementación inicial de E/S en sistema de archivos para carga de archivos. |
| 17/09/2025 | Ajuste de ruta de archivo temporal para el mapeo de volumen de Docker. |
| 17/09/2025 | Manejo robusto de FormData con seguridad asíncrona. |
| 18/09/2025 | Corrección de bloques catch duplicados en signWithNewAPI. |
| 18/09/2025 | Implementación inicial con PassThrough stream (reemplazado posteriormente por Readable). |
| 18/09/2025 | Corrección de fallos de carga en el webhook de OpenKM. |

Lic. Gustavo Silvio López Arias
Director
Dirección de Sistema Informático
MADES

## 5. Mejoras de Soporte y Documentación

| Fecha | Descripción |
|---|---|
| 22/12/2025 | Incorporación del documento de seguridad TLS con la arquitectura de despliegue (proxy inverso nginx, certificados TLS de Cloudflare, mapeo de puertos por entorno). |
| 22/12/2025 | Corrección del nivel de log de error a info para la operación exitosa okmCreateRecord: OK, reduciendo falsos positivos en el monitoreo. |
| 16/09/2025 | Implementación de integración alternativa con la API signbox — base sobre la cual se realizaron las optimizaciones posteriores. |

## 6. Resumen Ejecutivo

| Categoría | Commits | Archivos principales afectados |
|---|---|---|
| Mejoras de seguridad | 5 | package.json, config/database.js, src/utils/firmador.js, src/controllers/expedienteController.js |
| Mejoras de optimización | 5 | src/utils/firmador.js, src/utils/okm.js, src/controllers/callbackController.js, app.js, index.js |

### Áreas de impacto observadas:

- Cadena de suministro de dependencias: fijación de versión de axios ante incidente de compromiso.
- Autenticación y validación de credenciales: verificación previa y detección robusta de fallos.
- Confidencialidad de datos: eliminación de registro de parámetros SQL.
- Confidencialidad e integridad en tránsito: verificación explícita de certificados TLS.
- Eficiencia operativa: eliminación de E/S en disco en el flujo de firma y procesamiento de callbacks.
- Confiabilidad de cargas de archivos: manejo correcto de streams hacia OpenKM.
- Consistencia de despliegue: eliminación de valores por defecto en la configuración de puertos.

## 7. Metodología y Alcance

Este reporte se elaboró mediante la inspección directa del historial de mejoras del repositorio generador_expedientes, utilizando el rango temporal --since="2025-09-10" --until="2026-04-17". Cada mejora citada fue verificada mediante la inspección de su diff y estadísticas de archivos. Los impactos declarados corresponden a lo observado en el código modificado; no se han inferido consecuencias no evidenciadas por el cambio técnico registrado.

### Limitaciones del reporte:

- El reporte cubre únicamente cambios registrados en el sistema de control de versiones durante el período especificado.

Lic. Gustavo Silvio López Aranda
Director
Dirección de Sistema Informático
MADES

- No contempla cambios de configuración realizados directamente en los entornos de despliegue fuera del repositorio (nginx, Cloudflare, variables de entorno de contenedores).
- No contempla auditorías externas ni revisiones de código no integradas al repositorio.

*Documento emitido con fines de documentación institucional.*

MINISTERIO DEL AMBIENTE Y DESARROLLO SOSTENIBLE
Dirección de Sistema Informático

Lic. Gustavo Silvio López Aranda
Director
Dirección de Sistema Informático
MADES