



Farmacéuticos

Consejo General de Colegios Farmacéuticos de España



nodofarma
verificación

Guía para la Oficina de Farmacia en el cumplimiento de la normativa antifalsificación

Septiembre 2024 (v1)



Tabla de contenido

1. Marco legal	3
2. Generalidades	4
3. Objetivos del documento	5
4. Instrucciones generales en el cumplimiento de la normativa antifalsificación por la OF	6
4.1 Comprobación de la integridad del dispositivo contra manipulaciones	6
4.2 Comprobación de la autenticidad del identificador único	7
5. Fin del periodo estabilización del sistema	9
6. Instrucciones para la gestión de alertas. Notificación de sospechas de falsificados	10
6.1 Sistema Gestión Alertas (en desarrollo)	10
6.2 Recomendaciones para las OF mientras no exista un Sistema de Gestión de Alertas	10
6.3 Instrucciones ante la sospecha de medicamento falsificado	16
7. Herramientas de ayuda	17
7.1 Web de contingencia	17
7.2 Documentos relacionados	19
7.3 Listado de puntos de contacto de autoridades y otros agentes	19
7.4 Listado de Alertas SEVeM más comunes	20
7.5 Listado de errores técnicos detectados en Nodofarma Verificación (códigos de error NFV)	23

Guía para la Oficina de Farmacia en el cumplimiento de la normativa antifalsificación

1. Marco legal

Los dispositivos de seguridad de los envases de medicamentos de uso humano se regulan, a nivel europeo, en el [Reglamento Delegado \(UE\) 2016/161 de la Comisión, aplicable desde el 9 de febrero de 2019](#), que complementa la Directiva antifalsificación adoptada en 2011, donde se establece que los medicamentos afectados por esta norma deben incorporar en sus envases dos dispositivos de seguridad: un dispositivo contra manipulaciones¹ y un identificador único². El objetivo de esta normativa antifalsificación es el de impedir la entrada de medicamentos falsificados en la cadena legal de suministro. La normativa entró en vigor el 9 de febrero de 2019.

Los dispositivos de seguridad son de dos tipos:

- › Un código **datamatrix** que identifica individualmente el envase (IU, **identificador único**) y permite verificar su autenticidad mediante consulta al repositorio nacional de SEVeM. La información incluida en este código bidimensional (bidi) también vendrá impresa en formato legible para las personas, es decir:
 - › Código de Producto (PC)
 - › Número de Serie, único por envase (SN)
 - › Lote
 - › Fecha de Caducidad

- › Un **dispositivo contra manipulaciones** (DCM), que permitirá verificar si el envase ha sido objeto de manipulación.

En el caso de las oficinas de farmacia (en adelante, las “**OF**”) la normativa antifalsificación establece la obligación de verificar en el momento de la dispensación los dispositivos de seguridad (identificador único y dispositivo contra manipulaciones) de los envases de los medicamentos de uso humano que, de acuerdo con dicha normativa, tienen la obligación de llevarlos; desactivando el identificador único en el momento de la dispensación.

¹ «dispositivo contra las manipulaciones»: dispositivo de seguridad que permite verificar si el envase de un medicamento ha sido manipulado (art. 3.1.b).

² «identificador único»: dispositivo de seguridad que permite verificar la autenticidad y la identificación de cada envase de un medicamento (art. 3.1.a).

Si en la verificación de los dispositivos de seguridad de un envase surge la sospecha de que éste ha sido manipulado, o se pone de manifiesto que el medicamento puede no ser auténtico, las farmacias no lo dispensarán e informarán de ello a las autoridades competentes, conforme a lo dispuesto en el artículo 30 del citado Reglamento.

El Reglamento Delegado establece los casos en los que estos dispositivos de seguridad deben ser verificados, y cuándo debe realizarse la desactivación del identificador único tras la comprobación de su autenticidad en el sistema de repositorios. Para que los envases puedan ser verificados, los identificadores únicos son cargados en un sistema de repositorios. La propia normativa también establece los agentes que deben gestionar estos repositorios. En España lo hace la entidad SEVeM, como explicaremos más adelante. Además, los sistemas de repositorios nacionales están a su vez conectados entre ellos en una plataforma gestionada por el organismo europeo de verificación de medicamentos (EMVO, por sus siglas en inglés).

Asimismo, establece que los laboratorios farmacéuticos fabricantes, entidades de distribución, y los servicios y oficinas de farmacia que dispensen medicamentos al público tienen la obligación de informar inmediatamente a las autoridades competentes cuando consideren que el envase de un medicamento ha sido manipulado o cuando la verificación de los dispositivos de seguridad ponga de manifiesto que el medicamento puede no ser auténtico.

A nivel nacional, el [Real Decreto 717/2019, de 5 de diciembre, por el que se modifica el Real Decreto 1345/2007, de 11 de octubre, por el que se regula el procedimiento de autorización, registro y condiciones de dispensación de los medicamentos de uso humano fabricados industrialmente](#), establece para cada agente (laboratorios, entidades de distribución y servicios y oficinas de farmacia), las autoridades nacionales competentes aplicables en cada caso para la notificación de dichas sospechas de falsificación (art. 82). En el caso de la OF, autoridad competente será la de la Comunidad Autónoma donde esté ubicada ésta.

2. Generalidades

En base a la normativa europea, se creó el sistema español de verificación de medicamentos gestionado por la **entidad jurídica SEVeM**. Sus socios fundadores son: la Asociación Nacional Empresarial de la Industria Farmacéutica (FARMAINDUSTRIA), la Asociación Española de Medicamentos Genéricos (AESEG), la Federación de Distribuidores Farmacéuticos (FEDIFAR) y el Consejo General de Colegios Oficiales de Farmacéuticos (CGCOF).

SEVeM es el responsable de gestionar el repositorio nacional donde están cargados todos los identificadores únicos, registrando las operaciones efectuadas por los diversos agentes que interactúan con el repositorio (ya sea para cargar códigos de medicamentos, como es el caso de laboratorios, o de verificar que el código es correcto y está activo, como es el caso de las OF).

En base a un Convenio firmado entre SEVeM y el CGCOF, las OF se conectan al repositorio nacional a través de **Nodofarma Verificación** (en adelante, “**NFV**”), herramienta gestionada por el CGCOF. La adhesión de todos los Colegios a NFV, permitió que todas las farmacias de España pudieran efectuar todas las operaciones que tienen encomendadas a la luz de la normativa europea (verificación, desactivación o reversión del estado) en el plazo indicado.

3. Objetivos del documento

La presente guía pretende orientar a las OF sobre las principales operativas a llevar a cabo relacionadas con la verificación de medicamentos, así como resolver las dudas que pudieran surgir en relación con el uso del sistema; garantizando su adecuado funcionamiento y el cumplimiento de la normativa antifalsificación.

El documento recoge instrucciones sobre cómo verificar, dispensar o reintroducir un envase de un medicamento en el repositorio nacional. Así como las obligaciones aplicables a las OF una vez finalizado el periodo de estabilización en España, el 30 de septiembre de 2024.

Igualmente recoge recomendaciones para gestionar las alertas generadas desde la OF, mientras se trabaja entre los agentes implicados en la implantación de una herramienta específica para su gestión.

Por último, se incluyen las instrucciones a seguir por las OF ante la sospecha de que un envase sea un medicamento falsificado y la correspondiente notificación a las autoridades competentes.

Se trata de un documento general de uso común y generalizado, aplicable a todos los territorios y sistemas de gestión de las OF, sin perjuicio de las particularidades que, en su caso, pudieran existir en cada uno de ellos.

La información de este documento se podrá ir actualizando según se vayan estableciendo procedimientos más específicos en colaboración con las autoridades sanitarias y los agentes implicados en el SEVeM.

4. Instrucciones generales en el cumplimiento de la normativa antifalsificación por la OF

La legislación establece que las OF están obligadas a verificar en el momento de la dispensación los dispositivos de seguridad (identificador único y dispositivo contra manipulaciones) de los envases de aquellos medicamentos de uso humano que tienen la obligación de llevarlos.

4.1 Comprobación de la integridad del dispositivo contra manipulaciones

En la farmacia se comprobará que el **dispositivo contra manipulaciones** (DCM) del envase no ha sido quebrantado, y por tanto que no ha sido objeto de manipulación.

En caso de que se sospeche que el envase ha sido manipulado y, por tanto, es **sospechoso de ser un medicamento falsificado**, se ha de notificar a las autoridades competentes de la Comunidad Autónoma correspondiente, que, en caso necesario, lo pondrán en conocimiento de la Agencia Española de Medicamentos y Productos Sanitarios (AEMPS).

Para permitir una evaluación del caso y la pertinente toma de decisiones por la autoridad, la notificación ha de contener la mayor cantidad de información posible y disponible:

- › Identificación y contacto de la farmacia
- › Nombre del medicamento
- › Titular de autorización de comercialización
- › Proveedor y fecha de recepción (si se dispone de esta información)
- › Código de producto (PC)
- › Número de serie (SN)
- › Número de lote
- › Fecha de caducidad
- › Fotografías del envase sospechoso

Asimismo, deberá incluirse cualquier otra información adicional de la que disponga en relación al envase objeto de la sospecha.

Para facilitar esta notificación, la AEMPS publica en su página web un listado de puntos de contacto de las autoridades sanitarias competentes para la notificación de sospechas de falsificaciones de medicamentos (Ver apartado 7. *Herramientas de ayuda*).

4.2 Comprobación de la autenticidad del identificador único

Las siguientes son unas instrucciones generales para las OF sobre cómo verificar, dispensar o reintroducir un envase de un medicamento en el repositorio nacional, pudiendo en cada caso realizarse automáticamente desde el programa de gestión (escáner), manualmente, o desde la web de contingencia desplegada por el CGCOF, según las diferentes situaciones que se presenten.

4.2.1 Verificación del IU

La verificación del IU de un envase supone consultar su estado en el repositorio nacional, y comprobar que se encuentre cargado correctamente y activo. Esta comprobación se puede realizar en cualquier momento, siendo obligatoria en el proceso de dispensación.

Sería recomendable llevarla cabo en la **recepción del pedido**, de forma que, en caso de existir algún problema, se pueda detectar con tiempo suficiente para tomar las acciones oportunas (evitando que sea en el momento de dispensar).

4.2.2 Desactivación del IU

En el momento de la dispensación de un medicamento, una vez comprobada la integridad del DCM (ver apartado 4.1 *Comprobación de la integridad del dispositivo contra manipulaciones*), la farmacia verificará, escaneando el código bidi, que el IU está activo en el repositorio (es decir, que no se encuentra desactivado) y, por tanto, que ese envase puede ser dispensado.

En el momento de la dispensación se procederá a desactivar el código, con lo que el estado en el repositorio para ese envase pasará a ser “inactivo”, no pudiéndose volver a dispensar de nuevo por haber quedado desactivado.

Si finalmente la dispensación no se hace efectiva y, por error, ese mismo datamatrix se escaneará de nuevo en la misma farmacia para una dispensación posterior, se generaría una alerta en el sistema, pues se consideraría un indicio de ser un potencial falsificado.

4.2.3 Reintroducción en el sistema (reversión del estado a activo)

Como se ha explicado, es posible que se den casos en los que la OF completa el proceso de verificación/desactivación del IU, pero luego se necesite anular la dispensación porque finalmente ésta no se produce (el paciente no se lleva ese envase, por ejemplo). Entonces es necesario que la farmacia reintroduzca ese envase en el repositorio nacional para poder dispensarlo en el futuro. Los requisitos para esta actuación están estipulados en el art. 13 del Reglamento.

Si no han pasado más de 10 días desde la desactivación (y siempre que el medicamento no fuese retirado de la farmacia por el paciente) se podrá revertir el estado a activo.

Si han transcurrido más de 10 días desde la desactivación no se podrá revertir.

Asimismo, para esta reversión, el envase del medicamento no podrá figurar en el repositorio como *recuperado*, *retirado*, *destinado a su destrucción* o *robado*.

Cabe destacar que los distribuidores nunca aceptarán la devolución de un medicamento desactivado en el repositorio nacional. Por ello, es importante que las OF recuerden que tras una dispensación errónea siempre hay que reintroducir el IU en el repositorio dentro del plazo establecido (no más de 10 días).

Además, y como se ha expuesto, en ningún caso podrá ser reactivado un medicamento que haya sido efectivamente dispensado.

Tampoco podrá revertir el estado de un medicamento de inactivo a activo una farmacia distinta a la que generó la desactivación.

5. Fin del periodo estabilización del sistema

Durante la fase de puesta en marcha del sistema de verificación surgieron numerosas alertas no relacionadas con sospechas de medicamentos falsificados. Teniendo en cuenta que en España nunca se han detectado medicamentos falsificados dentro del canal legal del medicamento (según indica la AEMPS), y para atender a la necesidad de garantizar la continuidad del suministro de los medicamentos, se aceptó por las autoridades la dispensación de medicamentos que tras la verificación del identificador único generasen una alerta en el sistema, siempre que:

- › La alerta fuera generada por errores técnicos, procedimentales o humanos causados fundamentalmente por problemas en la carga de códigos de IU en el repositorio, errores en la codificación del datamatrix, por la existencia previa en el mercado de envases con códigos incompletos o no conformes con el Reglamento Delegado, así como por el desconocimiento de los usuarios en el manejo del sistema, y
- › El IU no estuviera desactivado, y se hubiera comprobado la integridad del dispositivo contra manipulaciones del envase, así como la legalidad del proveedor del medicamento que generó la alerta.

Después del trabajo realizado a lo largo de estos años en el marco de SEVeM y tras los avances técnicos implementados para una mejor funcionalidad del sistema, se ha logrado reducir significativamente el número de alertas generadas, motivo por el que la AEMPS considera que se ha alcanzado la estabilización del sistema en España.

Por ello, a partir del 30 de septiembre de 2024, tal y como [anunció la propia AEMPS](#) el 1 de julio, se pone fin al periodo de estabilización en nuestro país.

El fin de este periodo de estabilización supondrá que a partir de dicha fecha dejarán de permitirse las excepciones expuestas en los párrafos anteriores lo que implica que no se podrá suministrar ni dispensar ningún medicamento para el que no se obtenga una operación de verificación/desactivación satisfactoria y genere una alerta que no pueda ser descartada como sospecha de falsificación.

6. Instrucciones para la gestión de alertas. Notificación de sospechas de falsificados

6.1 Sistema Gestión Alertas (en desarrollo)

Actualmente se está trabajando desde SEVeM (entidad gestora), en coordinación con todos los agentes implicados, en una herramienta específica y automatizada para la gestión de las alertas dentro del sistema que permita a todos los usuarios, incluidas las OF, resolver posibles alertas técnicas o dar pie al inicio de una investigación en el caso de que surja una sospecha de un potencial medicamento falsificado. Sin embargo, hasta que no se disponga de dicha herramienta, y de forma transitoria, SEVeM seguirá gestionando las alertas de manera agrupada y siguiendo criterios de priorización por tipo de alerta y número, además de aquellas que pudieran surgir por fallos técnicos.

Por su parte, los laboratorios farmacéuticos titulares de los medicamentos cargados en el repositorio (“Titulares de Autorización de Comercialización” o “TAC”) deberán investigar las alertas generadas por sus medicamentos para descartar cualquier posible error por su causa, para una pronta detección y subsanación del error.

En el caso de las OF, por el momento, se deberán seguir las recomendaciones que a continuación se detallan.

6.2 Recomendaciones para las OF mientras no exista un Sistema de Gestión de Alertas

6.2.1 Recomendaciones generales:

A continuación, se recogen unas instrucciones sobre cómo deben proceder las OF mientras no se disponga de una herramienta específica para la gestión de las alertas.

Estas instrucciones se podrán ir actualizando según evolucione el Sistema de Gestión de Alertas y se detallen procedimientos más específicos en el ámbito de SEVeM.

6.2.1.1. Verificar en la recepción del pedido

A pesar de que no existe la obligación legal de verificar en ese momento, se recomienda proceder a la **verificación del IU en el momento de la recepción del pedido**.

Esta práctica facilitará la detección de posibles errores antes de llevar a cabo la dispensación. De esta manera, si se generara alguna alerta en ese momento de recepción del pedido, se detectaría con antelación suficiente como para poder investigar o solucionar el posible error que podría ocasionarse en la dispensación de ese envase, evitando inconvenientes a los pacientes.

6.2.1.2. Conocimiento del programa de gestión y otras herramientas

Los programas de gestión utilizados en las OF tienen implementadas funcionalidades relacionadas con la verificación de medicamentos, homologadas por la organización farmacéutica colegial en el marco del SEVeM, que pueden variar de unos a otros. Es más que recomendable que cada OF conozca en profundidad dichas funcionalidades, para trabajar de una forma adecuada y con herramientas de ayuda que les agilicen el trabajo. Si se considera que el conocimiento es limitado, se recomienda solicitar soporte a la empresa proveedora del programa de gestión homologado.

También es necesario tener actualizado el programa de gestión con la última versión disponible.

Asimismo, el CGCOF pone a disposición de las OF herramientas que considera pueden ayudar en el análisis de las alertas que está generando, para hacer seguimiento y comprender el origen de éstas. (Ver apartado 7. *Herramientas de ayuda*)

6.2.1.3. Cómo proceder ante una alerta

Si se genera una alerta tras una verificación o desactivación del datamatrix, ésta origina un aviso que se transmite a SEVeM (la entidad gestora del repositorio nacional), al laboratorio o TAC y a la propia OF. Las autoridades competentes (de las Comunidades Autónomas y AEMPS) podrán tener acceso a las alertas también, cuando así lo requieran.

En función de la alerta, se ha de investigar el posible origen y valorar si dicha alerta hace sospechar que se podría tratar de un medicamento falsificado, o si, por el contrario, se trata de un error técnico o de procedimiento.

Una vez analizado el motivo de la alerta, **si se puede descartar justificadamente una sospecha de falsificación y, hasta que se cuente con el Sistema de Gestión de Alertas automatizado, se procederá a dispensar.**

Será necesario dejar documentada la **justificación** por la que no se sospecha de un medicamento falsificado sino de un error técnico o de procedimiento, en caso de requerirse por las autoridades competentes conocer la causa por la que se cerró la alerta generada por el usuario y se dispensó el envase.

Mientras se desarrolla el Sistema de Gestión de Alertas, el registro de la justificación de la dispensación asociada a cada alerta podrá ser diferente en cada farmacia. Se recomienda un registro electrónico (email, fichero Excel, ...) de, como mínimo, la siguiente información: alertID, código de alerta generada, fecha, nombre del medicamento, PC, SN, lote del envase y motivo por el que se descarta la sospecha de falsificación.

Por último, es recomendable tener presente la severidad de la alerta, pues existe una graduación según la probabilidad de que se esté detectando un medicamento falsificado. Las alertas están clasificadas en niveles, siendo las de **nivel 1-4** las relacionadas con la operativa de la farmacia. Las de **nivel 5** son aquellas que pueden estar identificando un potencial falsificado y, en consecuencia, para las que es necesario tener mayor precaución. (Ver listado de alertas con su clasificación en el apartado 7. *Herramientas de ayuda*).

6.2.2 Propuestas de actuación para evitar los tipos de alertas más frecuentes:

Hasta el momento, se han podido identificar como más frecuentes los siguientes tipos de alertas y posibles causas asociadas. A continuación, se detallan propuestas para tratar de evitarlas.

En cualquier caso, si no se consigue evitar la alerta, habría que proceder según lo recogido en la sección 6.2.1.3. *Cómo proceder ante una alerta*.

ALERTAS POR DOBLE ACCIÓN:

I. PROBLEMAS DE OPERATIVA EN UNA MISMA OF

Cuando una OF realiza la dispensación de un mismo envase en un plazo de 24 horas, las 3 primeras veces devuelve una alerta de nivel 1-4 (NMVS_NC_PCK_23). A partir del cuarto intento o pasadas las 24 horas, la alerta generada es de nivel 5 (NMVS_NC_PCK_19).

Las posibles causas identificadas hasta el momento son:

- › El farmacéutico comete un error humano y lee el mismo datamatrix.
- › En algunos programas de gestión, al dispensar varios envases del mismo medicamento se lee solo un código datamatrix de uno de los envases.
- › El farmacéutico, ante la duda de si una lectura ha sido correcta, repite el escaneo de un IU ya desactivado.

Recomendaciones:

Conocer el funcionamiento del sistema y del programa de gestión (ver también sección *Desactivación del IU en el apartado 4.2 Comprobación de la autenticidad del identificador único*) y evitar las posibles operativas que se sabe que generan estas alertas.

II. PROBLEMAS DE OPERATIVA EN DIFERENTES OF

Aunque es muy poco común, se ha reportado algún caso excepcional en el que una OF dispensa el producto y otra intenta realizar una dispensación sobre ese mismo envase, generando una alerta de nivel 5 (NMVS_NC_PCK_19).

Recomendaciones:

Cumplir la normativa y nunca intercambiar medicamentos entre farmacias.

III. PROBLEMAS EN LA GESTIÓN DE “BULKS” CAUSADOS POR EL PROGRAMA DE GESTIÓN

Algunos programas de gestión de las OF no tratan correctamente los “bulk” (envío por lotes de las transacciones cuando se ha perdido la conectividad y la farmacia vuelve a conectarse). Es decir, el programa envía a través de NFV varias veces los mismos envases a dispensar y se generan alertas. Las alertas generadas pueden ser de nivel 1-4 (NMVS_NC_PCK_23), o de nivel 5 (NMVS_NC_PCK_19).

Recomendaciones:

El farmacéutico no suele tener conocimiento del problema en estos casos, pero sabiendo que puede existir, se recomienda revisar el listado de bulks de su OF y consultar a su proveedor de software si se considera que las alertas pueden tener este origen.

IV. PROBLEMAS CAUSADOS POR ROBOTS

Es posible que algunos robots o su relación con el programa de gestión de la farmacia puedan provocar involuntariamente casos de doble acción. Parece ser que en algunos casos se desactiva el IU cuando se extrae el envase del robot y luego se repite la operación cuando efectivamente se produce la dispensación al paciente, generándose alertas de nivel 1-4 (NMVS_NC_PCK_23).

Recomendaciones:

Si se dispone de robot, conocer la operativa de éste y su relación con el programa de gestión, de forma que se descarte que involuntariamente se esté realizando dos veces la dispensación en esos casos.

Por otro lado, si se va a reintroducir en el robot un envase que finalmente no ha sido dispensado, antes será necesario revertir en el repositorio el estado de éste a activo (ver sección 4.2.3 *Reintroducción en el sistema* y más adelante *viii. Problemas por intentos de reintroducción no posible*).

ALERTAS POR PROBLEMAS DE ESCÁNER O FALTA DE INFORMACIÓN DEL LABORATORIO

V. PROBLEMAS DE CONFIGURACIÓN DEL ESCÁNER DE LA FARMACIA

Aunque se ha trabajado intensamente por todos los implicados en evitar los problemas más comunes de configuración de escáner, continúan apareciendo configuraciones incorrectas, aunque en menor medida.

Suelen originar alertas relacionadas con la lectura incorrecta del número de serie o lote codificados en el datamatrix (NMVS_FE_LOT_03, NMVS_NC_PC_02, NMVS_FE_LOT_13), o la fecha de caducidad (NMVS_FE_LOT_12) o el código de producto (PC) (NMVS_NC_PC_01).

Recomendaciones:

Los programas de gestión han incluido un módulo de verificación que permite al farmacéutico revisar si su escáner tiene problemas de configuración. Es recomendable consultar al proveedor del programa en caso de duda.

Adicionalmente se recomienda introducir los datos de forma manual (evitando hacer más de 3 intentos para que no se genere otra alerta de nivel 5) para comprobar si es un fallo originado en el escaneo.

VI. PROBLEMAS DE LECTURA CAUSADOS POR EL PROGRAMA DE GESTIÓN

En ciertos casos el software de gestión comete errores en la lectura del envase, modificando los valores leídos o concatenando varios valores en un solo campo. Suelen originar alertas similares al caso anterior (NMVS_FE_LOT_03, NMVS_NC_PC_02, NMVS_FE_LOT_13, NMVS_FE_LOT_12, NMVS_NC_PC_01, NMVS_NC_PC_17).

Recomendaciones:

Contactar con el proveedor del programa de gestión.

VII. FALTA DE INFORMACIÓN DEL ENVASE EN EL REPOSITORIO

Los laboratorios o TAC están obligados a cargar en el repositorio los datos del envase, sin embargo, en ocasiones muy poco frecuentes, este proceso no se cumple o falla, lo que provoca alertas en las OF. En estos casos los TAC tienen 24 horas laborables para hacer las comprobaciones necesarias y cargar la información correcta en el repositorio.

Suelen generarse las alertas relacionadas con el lote y número de serie (SN) codificado en el IU (NMVS_FE_LOT_03, NMVS_NC_PC_02) o la fecha de caducidad del envase (NMVS_FE_LOT_12).

Recomendaciones:

Si al introducir los datos de forma manual (evitando cometer más de 3 intentos erróneos para que no se genere otra alerta de nivel 5) sigue saltando la alerta de nivel 1-4, es posible que la causa deba ser resuelta por el TAC. Se recomienda dejar el envase en cuarentena, pudiéndose reintentar la verificación transcurrido el plazo del que dispone el TAC para su resolución (24 horas laborables). Si el TAC ha resuelto el problema, ya no debería generarse la alerta.

OTROS TIPOS DE ALERTAS:

VIII. PROBLEMAS POR INTENTOS DE REINTRODUCCIÓN NO POSIBLE

Se trata de problemas originados por operativas mencionadas anteriormente, en las que se intenta reintroducir en el repositorio nacional un envase fuera de plazo (más de 10 días desde la desactivación) o por una farmacia diferente a la que lo desactivó (códigos de alerta de nivel 1-4 NMVS_NC_PCK_20 y NMVS_NC_PCK_21, respectivamente).

Recomendaciones:

Si en una tentativa de dispensación finalmente el paciente decide no retirar el envase, es necesario reintroducirlo en el sistema lo antes posible, sin sobrepasar los 10 días (ver sección anterior *4.2.3 Reintroducción en el sistema*). Si se intenta la reintroducción pasados 10 días se generará la alerta NMVS_NC_PCK_20.

IX. PROBLEMAS EN LA INTRODUCCIÓN MANUAL

En las operaciones manuales es posible que se den errores de escritura por parte del farmacéutico.

Recomendaciones:

Asegurarse de la correcta introducción de los datos, evitando sobrepasar los 3 intentos.

6.3 Instrucciones ante la sospecha de medicamento falsificado

Si tras la verificación y/o desactivación del datamatrix (IU) de un envase en la OF se genera una alerta en el sistema, y se realizan las comprobaciones necesarias que permiten descartar que el error se ha originado por mal funcionamiento del sistema u otros errores originados por la propia farmacia o el laboratorio titular, **no se podrá descartar la sospecha de que el envase podría ser falsificado**. En tal caso, no se dispensará el envase y se han de seguir las [instrucciones publicadas por la AEMPS para su notificación](#) a las autoridades competentes.

Dichas instrucciones han sido elaboradas por la AEMPS en colaboración con las autoridades competentes de las Comunidades Autónomas (CCAA), la entidad gestora del repositorio nacional (SEVeM) y los agentes representados en ella, entre los que se encuentra el CGCOF.

Las instrucciones definen los pasos a seguir una vez sea confirmada la sospecha, así como la información que debe contener la notificación que será necesaria realizar a la autoridad sanitaria competente de la Comunidad Autónoma (CA) donde esté ubicada la OF, y que consistirá, al menos, en la siguiente:

- › Identificación y contacto de la OF
- › Nombre del medicamento
- › Titular de autorización de comercialización
- › Proveedor y fecha de recepción (si se dispone de esta información)
- › Código de producto (PC)
- › Número de serie (SN)
- › Número de lote
- › Fecha de caducidad

Asimismo, deberá incluirse cualquier otra información adicional de la que disponga en relación al envase objeto de la alerta.

Se puede consultar el listado de contactos de las autoridades competentes en el apartado *7. Herramientas de ayuda*.

Envases sospechosos:

Los envases sospechosos de falsificación o manipulación permanecerán depositados y custodiados en la OF, separados de las existencias dispensables y a disposición de la autoridad sanitaria competente de la CA. En caso de problema al respecto, se deberá consultar con ésta.

Cuando se considerase necesaria la comprobación física de los envases sospechosos (o si dicha comprobación es solicitada por el TAC), la OF será informada por la CA. Ésta gestionará su remisión a la AEMPS para la realización de la comparecencia de confirmación de la autenticidad del envase con el laboratorio o TAC.

7. Herramientas de ayuda

7.1 Web de contingencia

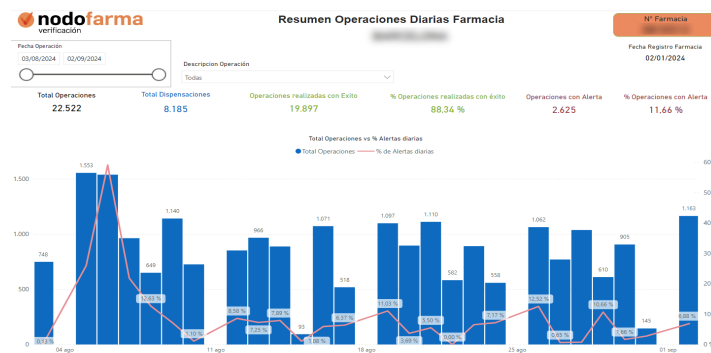
La **web de contingencia** se facilita para que las OF puedan realizar comprobaciones, verificaciones y desactivaciones de IU si su programa de gestión no está disponible para realizar estas operaciones.

Cuadro de mando:

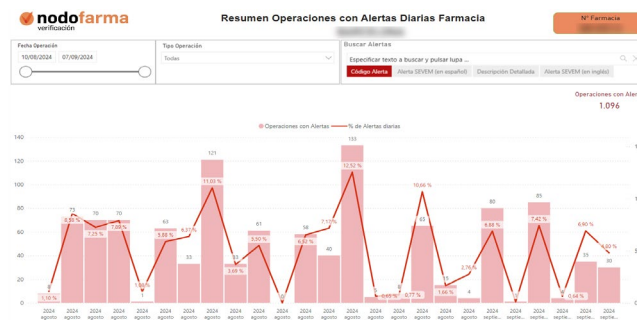
Desde esa misma web se puede acceder a unos **INFORMES** para consultar información de operaciones y alertas generadas en los últimos 30 días en la propia OF.

A modo de resumen, actualmente existen 3 informes:

RESUMEN DE OPERACIONES:



RESUMEN DE OPERACIONES CON ALERTAS:



MATRIZ DE ALERTAS DIARIAS:

nodofarma Matriz de Alertas diarias N° Farmacia

Fecha Operación: 10/08/2024 - 07/09/2024

Tipo Operación: Todas

Buscar Alertas: Especificar texto a buscar y pulsar lupa...

Código Alerta: Alerta SEVeM (en español) Descripción Detallada Alerta SEVeM (en inglés)

Año	2024																												Total
Mes	agosto														septiembre														
Descripción Operación	10	12	13	14	15	16	17	19	20	21	23	24	26	27	28	29	30	31	2	3	4	5	6	7					
Dispensación	8	73	70	70	1	63	33	121	33	61	58	40	133	5	8	65	15	4	80	1	85	4	35	29	1.095				
NMVS_NC_PCK_19	1	1	2		2	2	15	1	2				1	4	8	2	3	3	1	8		3	1	60					
NMVS_NC_PCK_23	8	72	69	68	1	61	31	106	33	60	56	40	132	1		63	12	4	77		77	4	32	28	1.035				
Verificación																									1				
NMVS_FE_LOT_13																									1				
Total	8	73	70	70	1	63	33	121	33	61	58	40	133	5	8	65	15	4	80	1	85	4	35	30	1.096				

LISTADO DE ALERTAS:

Se facilita el listado completo, no solo de aquellas alertas más comunes (incluidas en la siguiente sección 7.4 *Listado de Alertas SEVeM más comunes*).

nodofarma Listado Alertas Farmacia N° Farmacia

Fecha Operación: 10/08/2024 - 07/09/2024

Tipo Operación: Todas

Buscar Alertas: Especificar texto a buscar y pulsar lupa...

Código Alerta: Alerta SEVeM (en español) Descripción Detallada Alerta SEVeM (en inglés)

Primera Fecha Operación	Última Fecha Operación	Código Alerta	Alerta SEVeM (en español)	Total Alertas	Descripción Detallada
10/08/2024	07/09/2024	NMVS_NC_PCK_23	Se ha producido un escaneo por duplicado en un corto intervalo de tiempo (sin haberse sobrepasado el número máximo de intentos).	1.035	Error que se genera cuando un usuario intenta desactivar nuevo el mismo código que ya había desactivado previamente ese mismo usuario y no se han sobrepasado los límites temporales establecidos entre acciones repetidas ni el número de intentos.
12/08/2024	07/09/2024	NMVS_NC_PCK_19	Se está intentando desactivar un envase que ya había sido desactivado.	60	Desactivación de un código que ya había sido desactivado ese mismo motivo. Ejemplo: Dispensar un código que ya en estado supplied. Nota: si es el mismo usuario el que realiza las dos desactivaciones (la inicial con éxito y la repetición), generalmente recibirá previamente el aviso NMVS_NC_P antes de generar la alerta nivel 5
07/09/2024	07/09/2024	NMVS_FE_LOT_13	El número de serie existe en el Repositorio Nacional, pero la información del lote es incorrecta.	1	El número de serie existe en el Repositorio Nacional para código de producto, pero la información del lote es incorrecta.

!!! IMPORTANTE !!!
A medida que se vaya avanzando con los análisis y feedback que se envíen desde las Farmacias a los CGP, se irá ampliando la información sobre las causas más frecuentes de las alertas. Muchas gracias a todos por vuestra colaboración.

Los **programas de gestión** también dispondrán de un cuadro de mando similar a este, diseñado por el proveedor del programa (por lo que podría haber algunas variaciones entre los informes facilitados por la web de contingencia y por el programa).

7.2 Documentos relacionados

[INSTRUCCIONES PARA FARMACIAS PARA NOTIFICAR SOSPECHAS DE MEDICAMENTOS FALSIFICADOS EN RELACIÓN CON LA VERIFICACIÓN DE LA AUTENTICIDAD DEL IDENTIFICADOR ÚNICO](#) (publicadas en la web de la AEMPS).

7.3 Listado de puntos de contacto de autoridades y otros agentes

Autoridades competentes

La AEMPS mantiene actualizado en su web un listado de aquellos [contactos de la autoridad competente](#) que debe ser informada en cada caso ante la sospecha de un medicamento falsificado, incluidas aquellas de las diferentes CCAA.

Laboratorios farmacéuticos

En la web de la AEMPS se facilita la lista de correos electrónicos de [contacto de los Titulares de Autorización de Comercialización o Representantes Locales en España](#).

7.4 Listado de Alertas SEVeM más comunes

CÓDIGO	ALERTA SEVeM (inglés)	ALERTA SEVeM (en español)	NIVEL	DESCRIPCIÓN DETALLADA
NMVS_FE_LOT_03	Failed to find a batch for the given data.	El lote y el número de serie enviados no existen en el repositorio nacional	Errores nivel 5	El lote y el número de serie enviados en la petición no existen en el repositorio nacional.
NMVS_FE_LOT_12	Expiry date does not match the date held in the NMVS.	La fecha de caducidad no coincide con la del repositorio nacional	Errores nivel 5	La fecha de caducidad enviada en la petición no coincide con la fecha de caducidad del lote cargado en el repositorio nacional.
NMVS_FE_LOT_13	The batch ID does not match the serial number in the NMVS.	El número de serie existe en el repositorio nacional, pero la información del lote es incorrecta.	Errores nivel 5	El número de serie existe en el repositorio nacional para dicho código de producto, pero la información del lote es incorrecta.
NMVS_NC_PC_02	Unknown serial number.	Número de serie no existe o no coincide con el del repositorio nacional.	Errores nivel 5	El número de serie enviado en la petición no existe en el repositorio nacional.
NMVS_NC_PC_01	Unknown product code.	Código de producto desconocido	Errores alto riesgo de potenciales falsificados	El código de producto enviado en la petición no existe en el sistema.
NMVS_NC_PC_17	The NHRN is not found in the NMVS product masterdata for the given productcode.	Código Nacional y Código de producto no coinciden con los datos registrados en el repositorio nacional	Errores con alto riesgo de ser potenciales falsificados	La relación de código nacional y código de producto enviado en la petición no coincide con la información cargada en el repositorio nacional de SEVeM para ese producto.
NMVS_NC_PC_06	Product code not available in the system (no alert).	Código de producto desconocido (al introducir el código de manera manual).	Errores nivel 1-4	Error al introducir el código de producto al realizar una operación manual.
NMVS_NC_PC_14	The serial number is not known (no alert).	Número de serie desconocido (al introducir el número de manera manual).	Errores nivel 1-4	Error al introducir el número de serie al realizar una operación manual.



NMVS_NC_PCK_23	Re-setting of the property via double scan is registered.	Se ha producido un escaneo por duplicado en un corto intervalo de tiempo (sin haberse sobrepasado el número máximo de intentos).	Errores con alto riesgo de ser potenciales falsificados	Error que se genera cuando un usuario intenta desactivar de nuevo el mismo código que ya había desactivado previamente ese mismo usuario y no se han sobrepasado los límites temporales establecidos entre acciones repetidas ni el número de intentos.
NMVS_NC_PCK_19	Property is already set on pack.	Se está intentando desactivar un envase que ya había sido desactivado.	Errores nivel 5	Desactivación de un código que ya había sido desactivado por ese mismo motivo. Ejemplo: Dispensar un código que ya estaba en estado "dispensado". Nota: si es el mismo usuario el que realiza las dos desactivaciones (la inicial con éxito y la repetición), generalmente recibirá previamente el aviso NMVS_NC_PCK_23 antes de generar la alerta de nivel 5
NMVS_NC_PCK_22	Pack is already inactive.	El envase ya se encuentra inactivo. Se está intentando desactivar un envase que ya había sido desactivado indicando un motivo diferente.	Errores nivel 5	Desactivación de un código que ya había sido desactivado por un motivo diferente. Ejemplo: Dispensar un código que estaba en estado "muestra"
NMVS_NC_PCK_27	Status change could not be performed.	El cambio de estado no se pudo llevar a cabo. Se está intentando desactivar un envase que ya había sido desactivado indicando un motivo diferente (Transacción entre mercados).	Errores nivel 5	Desactivación de un código que ya había sido desactivado por un motivo diferente. Este error se genera únicamente cuando la transacción es intermarket (entre diferentes mercados o países de la UE).
NMVS_NC_PCK_06	Actual pack status doesn't match the undo transaction (set and undo status must be equivalent).	El estado actual del envase no coincide con el estado de la reactivación. Se está intentando reactivar indicando un estado diferente al que fue desactivado.	Errores nivel 5	Reactivación de un código por un motivo diferente al que fue desactivado. Ejemplo: "revertir dispensación" de un código que está en estado "muestra".
NMVS_NC_PCK_20	Defined timeframe between setting this property and the undo was exceeded.	Se ha sobrepasado el tiempo máximo (10 días) para revertir el estado de este envase que ya fue desactivado por este mismo usuario.	Errores nivel 1-4	Error al intentar revertir el estado de un identificador único que fue desactivado por ese mismo usuario hace más de 10 días.



NMVS_NC_PCK_21	Undo can only be executed by the same user who previously set the attribute.	Solo puede revertir el estado del envase el mismo usuario que efectuó su desactivación.	Errores nivel 1-4	No se puede hacer revertir el estado del identificador único porque el usuario es distinto al que efectuó la desactivación.
NMVS_NC_PCK_28	Property is already set on pack (no alert).	Se está reactivando un envase que se encontraba ya en estado activo o en los estados: caducado, retirado o anulado.	Errores nivel 1-4	Reactivación de un código que se encontraba ya en estado activo o en los estados: expired, recalled o withdrawn.
NMVS_NC_PCK_30	Pack is already inactive (no alert).	Se está desactivando un envase que estaba activo a nivel de número de serie, pero inactivo a nivel de lote (caducado, retirado) o de producto (retirado).	Errores nivel 1-4	Desactivación de un código que estaba activo a nivel de número de serie, pero inactivo a nivel de lote (expired, recalled) o producto (withdrawn).
NMVS_NC_PCK_31	Status change could not be performed (no alert).	Se está desactivando un envase que estaba activo a nivel de número de serie, pero inactivo a nivel de lote (caducado, retirado) o de producto (retirado). Transacción entre mercados	Errores nivel 1-4	Desactivación de un código que estaba activo a nivel de número de serie, pero inactivo a nivel de lote (expired, recalled) o producto (withdrawn). Este error se genera únicamente cuando la transacción es intermarket. (entre diferentes mercados o países de la UE)
NMVS_SUCCESS	Successfully processed.	Transacción ejecutada con éxito	OK	Transacción ejecutada con éxito
NMVS_FE_LOT_15	Failed to find a batch for the given data.	No se ha podido encontrar un lote para los datos proporcionados en el repositorio nacional	Errores nivel 1-4	Error equivalente a la alerta de nivel 5 NMVS_FE_LOT_03 cuando esta última no viene con AlertID en casos muy poco frecuentes, como por ejemplo cuando el país de destino de la transacción intermarket no devuelve por error un alertID junto con el código de error NMVS_FE_LOT_03.
NMVS_FE_LOT_17	Expiry date does not match the date held in the NMVS (no alert).	La fecha de caducidad no coincide con la del repositorio nacional.	Errores nivel 1-4	Error equivalente a la alerta de nivel 5 NMVS_FE_LOT_12 cuando esta última no viene con AlertID en casos muy poco frecuentes, como por ejemplo cuando el país de destino de la transacción intermarket no devuelve por error un alertID junto con el código de error NMVS_FE_LOT_12.

NMVS_FE_LOT_18	The batch ID does not match the serial number in the NMVS (no alert).	El lote no coincide con el número de serie del repositorio nacional.	Errores nivel 1-4	Error equivalente a la alerta de nivel 5 NMVS_FE_LOT_13 cuando esta última no viene con AlertID en casos muy poco frecuentes, como por ejemplo cuando el país de destino de la transacción intermarket no devuelve por error un alertID junto con el código de error NMVS_FE_LOT_13.
-----------------------	---	---	-------------------	--

7.5 Listado de errores técnicos detectados en Nodofarma Verificación (códigos de error NFV)

Para la resolución de estos errores, se ha de contactar con el proveedor del programa de gestión.

NFV_AC_01	Error de acceso, consulte al administrador.
NFV_BULK_IT_00	Resultado de proceso bulk desconocido, consulte al administrador.
NFV_BULK_IT_01	Resultado de proceso bulk desconocido, consulte al administrador.
NFV_BULK_AT_00	Resultado de proceso bulk desconocido, consulte al administrador. (Problema de bloqueo en procesamiento. Reintentos de consulta superados)
NFV_BULK_AT_01	Resultado de proceso bulk desconocido, consulte al administrador. (Problema de bloqueo en procesamiento. Reintentos de envío superados, o se ha llegado a estado bloqueado)
NFV_BULK_AT_11	Resultado de proceso bulk desconocido, consulte al administrador. (Problema de bloqueo en procesamiento. Excepción en gestión del proceso)
NFV_BULK_PT_00	Procesando solicitud por lote
NFV_BULK_PT_01	Procesando solicitud por lote (IMT)
NFV_TR_00	ThrotlingException. Error interno del sistema. Bloqueo de operaciones por exceso de reintentos
NFV_BRI_01	Successfully received [repeated content].
NFV_CE_00	ConnectToRepositoryException. No se puede conectar al Repositorio Principal
NFV_CE_01	ConnectToRepositoryException No se puede conectar a Repositorio Principal
NFV_CE_02	InternalErrorException 01. Error interno del sistema.
NFV_IE_01	Internal Error. Error interno del sistema.



NFV_IE_02	Internal Error. Error interno del sistema.
NFV_ERR_CA1	Unexpected SeVEM Response
NFV_ERR_CA2	Unexpected SeVEM Response
NFV_RQ_00	EmptyContentBodyException Contenido de la petición vacío.
NFV_RQ_02	UndefinedOperationException Operacion no definida
NFV_RQ_03	JsonPathException (Formato incorrecto de Json)
NFV_RQ_04	CorruptJsonException (Formato incorrecto de Json)
NFV_RQ_05	MalformedPharmacyCodeException Farmacia con formato incorrecto
NFV_RQ_06	UserAgentNotFoundException Identificador de aplicación no proporcionado
NFV_RQ_07	UngrantedAccessException No tiene permiso para ejecutar llamada
NFV_RQ_08	RequestEntityTooLargeException Tamaño del cuerpo demasiado grande
NFV_SE_01	InvalidCredentialsException Credenciales incorrectas
NFV_SE_01	ValidateAccessTokenException Token invalido
NFV_SE_03	SecurityKeeperException Farmacia no Activa
NFV_SE_04	AuthorizationHeaderException Falta token en cabecera de autorización
NFV_SE_05	PharmacyNotExistException Usuario sin farmacia asociada
NFV_SE_06	PharmacyNotMatchException. Token no asociado a farmacia indicada
NFV_SE_07	InvalidScopeException Scope incorrecto
NFV_SE_08	InvalidClientException Usuario incorrecto al pedir token
NFV_SE_09	Demasiados reintentos incorrectos de solicitud de token
NFV_SUM_01	Sistema en mantenimiento
NFV_TI_00	InvalidTokenInfoException Error en información del token proporcionado
NFV_UM_01	Excepción general
NFV_EX_**	Excepción interna del sistema. Errores inesperados. (los ** serán cambiados por dígitos)

