INFORME EJECUTIVO

1. OBJETO

Evaluar la seguridad, confidencialidad, disponibilidad de la base de datos de la Administración.

2. ALCANCE

El examen se realizó conforme las Normas de Auditoría Interna Gubernamental (Resolución SIGEN Nº 152/02), el Manual de Control Interno Gubernamental (Resolución SIGEN N° 03/11) y la Resolución SIGEN N° 172/2014 que aprueba las "Normas Generales de Control Interno para el Sector Público Nacional.

Las tareas de auditoría se desarrollaron durante los meses de abril a septiembre del año 2022, se realizaron en la sede central de la Administración Nacional de Medicamentos, Alimentos y Tecnología Médica (ANMAT) sito en Avenida de Mayo 869, CABA y en la sede de Avenida de Mayo 850, CABA, así como también en los institutos nacionales que de ella dependen tales como el Instituto Nacional de Medicamentos (INAME) sito en Avenida Caseros 2161, CABA, en el Instituto Nacional de Productos Médicos (INPM) ubicado en Avenida Belgrano 1480, CABA y en el Instituto Nacional de Alimentos (INAL) que se encuentra en la calle Estados Unidos 25, CABA.

El período de análisis abarcó hasta la fecha de la presente auditoria, efectuándose un seguimiento de las observaciones pendientes de regularización que surgen de los informes de auditoría de años anteriores.

El universo para la presente auditoría comprende los sistemas informáticos utilizados por las distintas direcciones que conforman la ANMAT, a saber:

- Instituto Nacional de Medicamentos
- Instituto Nacional de Productos Médicos
- Instituto Nacional de Alimentos
- Dirección General de Administración
- Dirección de Evaluación y Gestión de Monitoreo de productos para la salud
- Dirección de Gestión Técnica
- Dirección de Asuntos Jurídicos
- Dirección de Recursos Humanos
- Dirección de Relaciones Institucionales

A continuación se describen los sistemas informáticos en producción:

- Vademecum Nacional de Medicamentos (VNM): Es una base de datos de medicamentos de la ANMAT con datos de carácter público y propio de la Administración.

- Sistema Nacional de Trazabilidad de Medicamentos: consiste en la identificación individual y unívoca de cada unidad de las especialidades medicinales a ser comercializadas.
- Sistema Nacional de Trazabilidad de Productos Médicos: consiste en la identificación individual y unívoca de cada unidad de producto médico liberado al mercado.
- Sly Actor: Sistema de Evaluación y Registro de Especialidades Medicinales para el Art. 5º del Decreto 150/92. (Sistema por Imágenes).
- REM: Sistema de Evaluación y Registro de Especialidades Medicinales para los Art. 3° y 4° del Decreto 150/92, apto Firma Digital.
- SIFEGA: Sistema de Información Federal para gestión de control de los alimentos
- Sistema de Productos Cosméticos Grado I apto Firma Digital: Registra la inscripción de cosméticos Grado I.
- ECLIN: Sistema de Estudios de Farmacología Clínica apto Firma Digital:
- Sistema de Ordenes de Inspección: Generación de órdenes de inspección de los diferentes rubros de la ANMAT.
- Sistema de Farmacovigilancia: Reportes Online para las notificaciones de Reacciones Adversas, provenientes de Pacientes, de Profesionales Sanitarios y de Laboratorios TARC.
- Sistema VigiFlow: utilizado para la gestión de la incorporación de información a la base de datos mundial VigiBase Desarrollado por la OMS.
- GEMHA: Registro de habilitaciones de establecimientos de productos médicos.
- HELENA: Sistema de Registro de Productos Médicos. Inscripción, Registro, Modificación y Reválida de Productos Médicos Clase I, II, III y IV.
- COMEX: Sistema de importación de productos médicos.
- RAEM: Régimen de acceso de excepción a medicamentos (Uso Compasivo).
- Sistema NDS: trámites de importación y exportación de sustancias sujetas a control especial. Desarrollado por la ONU.
- Sistema PEN Online: trámites de exportación de precursores químicos. Desarrollado por la ONU.
- Sistema de Cobro electrónico de aranceles.
- Sistema de Tesorería: Realiza el cobro de los aranceles inferiores a $ 300.
- Sistema de DD.JJ de Registro de Especialidades Medicinales.
- Sistema de DD.JJ de Registro de Productos Médicos.
- Sistema de Expedientes: Registra los movimientos de los expedientes dentro de la administración.
- Sistema de Caratulación automática: Caratulación automática de expedientes de papel en las diferentes mesas de entrada.
- Sistema de Actuaciones Simples: Caratulación de actuaciones simples en las Mesas de Entrada.
- GDE.

- TAD.
- Sistema de Multas:
- E – SIDIF:
- COMPR.AR.
- Sistema de Registro de Operaciones de Comercio Interior de Sustancias Sujetas a Controles Especiales:
- Visor GEDO: Es utilizado por Aduana para verificar que la documentación en papel que se presenta sea copia fiel de los trámites hechos a distancia.
- TABLEAU: Herramienta de reporte de GDE.
- Sistema Tango – Modulo Sueldos y jornales:
- Sistema de Control Horario.

A los fines de la obtención de la muestra, se realizó un relevamiento de las áreas sustantivas cuya generación y utilización de bases de datos resultan relevantes y críticos para el correcto funcionamiento de la Administración.
A continuación, se detallan las áreas sustantivas relevadas:

Instituto Nacional de Medicamentos (INAME)

- Dirección de Evaluación y Registro de Medicamentos.
- Dirección de Fiscalización y Gestión de Riesgo.
- Dirección de Evaluación y Control de Biológicos y Radiofármacos.
- Departamento de Vigilancia Post Comercialización y Acciones Reguladoras (dependiente de la Dirección Nacional del INAME.
- Departamento de Sustancias Sujetas a Control Especial (dependiente de la Dirección Nacional del INAME).
- Departamento de Farmacovigilancia y Gestión de Riesgo (dependiente de la Dirección Nacional del INAME).
- Área de Comercio Exterior (dependiente informalmente de la Dirección Nacional del INAME).

Instituto Nacional de Productos Médicos (INPM)

- Dirección de Fiscalización y Gestión de Riesgo de Establecimientos de Productos Médicos.
- Dirección de Evaluación y Registro de Productos Médicos.
- Dirección de Vigilancia Post Comercialización y Acciones Reguladoras de Productos Médicos.

Instituto Nacional de Alimentos (INAL)

- Dirección de Fiscalización y Control.
- Dirección de Prevención, Vigilancia y Coordinación Jurisdiccional.
- Dirección de Legislación e Información Alimentaria para la Evaluación del Riesgo.

Dirección General de Administración (DGA).

- Dirección de Informática.

- Coordinación de Verificación de Actos Administrativos.

Administración Nacional

- Dirección de Gestión de Información Técnica (DGIT).
- Dirección de Evaluación y Gestión de Monitoreo de Productos para la Salud (DEGMPS).

Seguidamente, se enumeran los sistemas informáticos relevados:

- Sly Actor.
- REM.
- Sistema de Estudios de Farmacología Clínica apto Firma Digital (ECLIN).
- Sistema de Ordenes de Inspección.
- Sistema NDS.
- Sistema PEN Online.
- Sistema de Reportes Online.
- Sistema VigiFlow.
- Sistema de Registro de Productos Médicos Helena.
- GEMHA.
- Sistema de Información Federal para gestión de control de los alimentos (SIFEGA).
- Sistema de Vademécum Nacional de Medicamentos (VNM).
- Sistema Nacional de Trazabilidad de Medicamentos.
- Sistema de Productos Cosméticos Grado I apto Firma Digital.
- RAEM.
- COMEX.
- TABLEAU.
- GDE.
- Trámites a Distancia (TAD).

3. OBSERVACIONES

3.1 La observación que se detalla a continuación ha sido regularizada:

3.1.1 Informe 20 – Año 2015: Según personal de infraestructura la entidad cuenta con personal tercerizado con acceso a permisos de administrador. La falta de control por oposición sobre las actividades que se desarrollan externamente es un riesgo ante la pérdida, modificación o uso inadecuado de la información.

Comentario del Auditor: A fin que los desarrolladores externos puedan realizar las modificaciones a los fuentes que se encuentran en ANMAT de manera controlada por la Dirección de Informática, se verificó que el área de infraestructura de esa Dirección creó una carpeta virtual para cada aplicación (FTP) a través de la cual ingresa el desarrollador externo con usuario cuyo permiso es de "invitado" y tiene acceso de lectura y escritura sólo para la carpeta virtual a la que fue autorizado su ingreso.

3.2 En las siguientes observaciones, se evidenciaron acciones correctivas, a saber:
3.2.1 Informe 20 – Año 2015: Falta de integración de los datos que se administran en las áreas relevadas, lo que afecta al aprovechamiento de recursos. Esta carencia ocasiona poca interacción entre las áreas dado que algunas de estas utilizan aplicativos en los que vuelcan información que podría ser de utilidad en otras direcciones que carecen de dicha información. Esta situación genera redundancia, descentralización y desnormalización e integridad de datos.
3.2.2 Informe 20 – Año 2015: Se han encontrado bases de datos que de ser utilizadas en forma unificada permitirá la normalización de las mismas y evitaría la duplicación de datos.
Esta ausencia de una base datos integral, unificada y actualizada que integre a los diversos actores involucrados en el proceso genera como consecuencia dificultad para contar con estadísticas en tiempo real, disponibilidad y acceso a información pudiendo generar ciertos errores como omisiones en algunos casos o duplicaciones en otros, como así también genera poca información para la toma de decisiones que impliquen conocer la estadística. El impacto de la observación alcanza la integración de los sectores, la celeridad organizativa, y economía del proceso.
Opinión del Auditado: "Se conformó un equipo de trabajo, para el proyecto de unificación de las bases de datos del organismo. Actualmente el equipo de trabajo se encuentra trabajando en el desarrollo de "DISPOWEB". Este proyecto consiste en la carga y clasificación de las disposiciones emanadas de la ANMAT con el fin de obtener una herramienta de consulta permanente de todos los actos dispositivos, los cuales serán "tagueados" de acuerdo al formato al que corresponda, resultando que dicha metadata podrá ser filtrada y de esta forma obtener distintas consultas y filtros sobre la información existente. Dicho proyecto es la etapa inicial de la unificación de las Bases de Datos del Organismo. Se licitó la solución y el adjudicatario ya está trabajando en el relevamiento inicial."
Comentario del Auditor: Se mantiene la observación. Si bien hubo avances, el proyecto "DispoWeb" se encuentra en etapa de desarrollo y corresponde a la etapa inicial de la unificación e integración de las bases de datos.
3.2.3 Informe 20 – Año 2015: Existen algunos aplicativos (Sistema Nacional de Medicamentos -Vademécum, Sistema Nacional de Trazabilidad de Medicamentos, Sistema Nacional de Trazabilidad de Productos Médicos) que se encuentran en producción pero no se tiene acceso a los fuentes. Tampoco se evidenció la documentación del Sistema de Información Federal para Gestión del Control de los Alimentos – SIFEGA, lo que genera un riesgo potencial dado que quedan limitadas las modificaciones a dichos aplicativos y se carece de la posibilidad de realizar un seguimiento del código en caso que una transacción produzca un resultado inesperado.
Opinión del Auditado: "En cuanto al sistema SIFEGA, se realizó la transferencia técnica al INAL. A tal efecto dentro de la estructura del INAL y a su vez dependiendo de la Dirección de Legislación e Información Alimentaria para la Evaluación de Riesgo se encuentra el Departamento del Sistema Federal para la Gestión del Control de los Alimentos (SIFEGA)

encargado específicamente de estas tareas que incorporó un equipo de desarrollo específicamente para manejar esta solución y realizar el mantenimiento correctivo y evolutivo del mismo.
En cuanto a los sistemas: Sistema Nacional de Medicamentos -Vademécum, Sistema Nacional de Trazabilidad de Medicamentos, Sistema Nacional de Trazabilidad de Productos Médicos, se están manteniendo reuniones con PAMI para evaluar la transferencia tecnológica de estas aplicaciones. Respecto a las adecuaciones del plan de contingencia, las mismas serán contempladas de acuerdo a los lineamientos de la Decisión Administrativa N° 641/2021 que aprueba los "REQUISITOS MÍNIMOS DE SEGURIDAD DE LA INFORMACIÓN PARA LOS ORGANISMOS DEL SECTOR PÚBLICO NACIONAL"
Comentario del Auditor: Se mantiene la observación. Dado que se ha evidenciado el acceso a los fuentes del sistema SIFEGA, no así aún con el Sistema Nacional de Medicamentos -Vademécum, Sistema Nacional de Trazabilidad de Medicamentos y el Sistema Nacional de Trazabilidad de Productos Médicos.

3.3 A continuación se exponen las observaciones resultantes de la presente auditoría:
3.3.1 Se observa que muchas áreas no encuentran en los sistemas la posibilidad de almacenar toda la información necesaria que se maneja en las áreas teniendo que apelar al uso de documentos y planillas complementarias. Que los sistemas desarrollados no brinden todas las funcionalidades que requieren las áreas, genera redundancia en los datos que son almacenados fuera de la órbita de la Administración. Esta metodología de almacenamiento atenta contra los niveles de seguridad y respaldo adecuados, con lo cual se incrementa el riesgo de pérdida de información. Esta observación reemplaza la observación N° 8 del Informe 12/2008.
Recomendación: Identificar las necesidades específicas de cada dirección a los fines de diseñar e implementar adecuaciones de ser necesario para aquellos sistemas cuyas funcionalidades no resultan suficientes al accionar de las áreas.

3.3.2 Si bien los aplicativos poseen controles de acceso evitando que usuarios no autorizados ingresen a los mismos, no se ha obtenido evidencias de controles de intentos de acceso fallidos. Asimismo no se ha evidenciado el detalle de usuarios administradores de los sistemas aplicativos. La falta de control genera desconocimiento acerca de la actividad de los usuarios, impactando directamente contra la integridad de la información. Esta observación proviene del Informe N° 20/2015.
Recomendación: Establecer y documentar procedimientos de auditoría de control de accesos. Se deberá clasificar los recursos tecnológicos y sistemas de información según su criticidad y sensibilidad, estableciendo adecuados derechos de acceso a los datos administrados por los mismos. Los niveles de accesibilidad deberán diseñarse considerando qué usuarios o grupos de usuarios tendrán derecho de acceso y con qué privilegios accederán a los datos, funciones y servicios informáticos. Deberán implementarse adecuadas restricciones para la utilización de programas utilitarios sensitivos, editores y

compiladores, propios de los sistemas operativos de las distintas plataformas y herramientas de operación. Asimismo, deberán desarrollarse mecanismos formales para la asignación y la utilización de usuarios especiales con capacidades de administración, que puedan ser usados en caso de emergencia o interrupción de las actividades.
Los usuarios definidos con estas características deberán contar con adecuadas medidas de resguardo y acceso restringido, registrando su utilización y realizando controles posteriores sobre los reportes de eventos, analizando la concordancia entre las tareas realizadas y el motivo por el cual se los solicitó. También se deberán implementar reportes de seguridad que registren las actividades de los usuarios, los intentos fallidos de acceso y bloqueos de cuentas, la utilización de usuarios con accesos especiales y el uso de utilitarios sensitivos. Se deberá proteger la integridad de la información registrada en dichos reportes.

3.3.3 Si bien la Dirección Informática cuenta con un conjunto de procedimientos, algunos de ellos carecen de detalles relevantes para guiar la ejecución de su accionar y no se encuentran aprobados formalmente. La carencia de procedimientos delineados podría incurrir en incumplimientos de los objetivos, que los proyectos informáticos no puedan ejecutarse por falta de presupuesto e incrementar los riesgos en materia de seguridad informática.
Recomendación: Revisión y elaboración de políticas, normas, estándares, procedimientos y/o prácticas para los aspectos relacionados con la planificación, seguridad, operación y control de los sistemas de información y su tecnología asociada, de acuerdo a los lineamientos de la Decisión Administrativa N° 641/2021 que aprueba los "REQUISITOS MÍNIMOS DE SEGURIDAD DE LA INFORMACIÓN PARA LOS ORGANISMOS DEL SECTOR PÚBLICO NACIONAL"

3.3.4 No se ha obtenido documentación técnica ni manuales de usuarios para las aplicaciones de la entidad. La falta de dicha documentación podría fomentar dependencia con el desarrollador de la aplicación, ya que esta carencia impide que personas autorizadas tengan disponible el conocimiento necesario para realizar correcciones de errores y/o hacer ajustes para el correcto mantenimiento de la aplicación.
Recomendación: Elaborar documentación técnica y manuales de usuarios de los sistemas aplicativos, del equipamiento informático y su software de base, diagramas topológicos de las redes de telecomunicaciones y toda aquella documentación relacionada con los recursos de información.

3.3.5 El plan de contingencias no contempla detalle de los procedimientos a llevar a cabo en caso que tenga que ser aplicado. El hecho de no prever íntegramente en el plan de contingencias los riesgos que pudieran afectar la continuidad de los servicios críticos de la Administración, incrementa los riesgos ante la falta de accesibilidad a los datos, fallas y hasta pérdida de la información.

Recomendación: Realizar una adecuada evaluación de los riesgos de acuerdo a la criticidad de la información y objetivos del negocio. De esta manera se permitirá identificar y administrar los riesgos inherentes al procesamiento informático a fines de no interrumpir las actividades normales y procesos críticos de la Administración.
Se sugiere desarrollar un plan de contingencias y que el mismo sea aprobado formalmente, de acuerdo a los lineamientos de la Decisión Administrativa N° 641/2021 que aprueba los "REQUISITOS MÍNIMOS DE SEGURIDAD DE LA INFORMACIÓN PARA LOS ORGANISMOS DEL SECTOR PÚBLICO NACIONAL". El mencionado plan deberá establecer con claridad y precisión los cursos de acción a seguir, los tiempos a cumplir, la definición de responsabilidades, el equipamiento alternativo, los archivos, las telecomunicaciones, los proveedores de servicios de tecnología y sistemas de información y todos aquellos recursos necesarios para lograr la continuidad del procesamiento.

3.3.6 La documentación recibida referente a los procesos de backups y recuperación de la información no se corresponden con los procedimientos relevados en las reuniones mantenidas en su oportunidad. Los procedimientos DI-009 (Generación de respaldos de servidores) y DI-010 (Restauración de respaldos en servidores) no detallan los procesos relacionados con las librerías de cintas que se encuentran en uso, es decir, que no detallan los procesos implementados para el almacenamiento de los backups. No se han obtenido evidencias de pruebas de recuperación de la información (restore), como así tampoco que se cumple el punto 3.0.9 del documento DI-009 que instruye a guardar una copia de backups mensual en un ente externo. Tal situación reduce las posibilidades de recuperar información ante un siniestro que afecte al sector de sistemas en cuyo caso se perderían todas las copias existentes impactando directamente sobre la disponibilidad de la información.
Recomendación: Diseñar un esquema de backups y recuperación de la información que incluya el almacenamiento de copias en una locación distante de manera de preservar la información ante un siniestro general en el centro de datos. Adecuar y aprobar formalmente los procedimientos DI-009 y DI-010, de acuerdo a los lineamientos de la Decisión Administrativa N° 641/2021 que aprueba los "REQUISITOS MÍNIMOS DE SEGURIDAD DE LA INFORMACIÓN PARA LOS ORGANISMOS DEL SECTOR PÚBLICO NACIONAL.

3.3.7 Se ha verificado que no existe una adecuada separación entre ambientes de producción y ambientes de desarrollo. La falta de separación de ambientes incrementa los riesgos que van desde la inestabilidad de los aplicativos en producción hasta la posibilidad de alteración de información sensitiva. Esta observación proviene del Informe N° 20/2015.
Recomendación: A fin de minimizar el riesgo de actualizaciones accidentales en el entorno productivo (sistemas en funcionamiento), el ingreso de programas no probados, evitar accesos no autorizados a los datos y garantizar la correspondencia entre los programas "fuentes" y los programas "ejecutables", se deberá definir un adecuado esquema de separación entre sus ambientes informáticos de procesamiento (desarrollo, prueba y producción) asegurando que los analistas y programadores de sistemas no tengan acceso al

entorno productivo, ni los operadores accedan al ambiente ni a las herramientas utilizadas para el desarrollo y el mantenimiento de los sistemas de aplicación.

3.3.8 La Dirección de Informática no cuenta con políticas, normas y procedimientos referidos a seguridad lógica, de acuerdo a los lineamientos de la Decisión Administrativa N° 641/2021 que aprueba los "REQUISITOS MÍNIMOS DE SEGURIDAD DE LA INFORMACIÓN PARA LOS ORGANISMOS DEL SECTOR PÚBLICO NACIONAL. Este incumplimiento normativo representa un riesgo dado que usuarios no autorizados podrían leer o alterar información con consecuencias impredecibles.
Recomendación: Redactar políticas, normas y procedimientos sobre seguridad lógica conforme lo establece la Decisión Administrativa N° 641/2021.

3.3.9 La Dirección de Informática no cuenta con políticas, normas y procedimientos referidos a la protección de datos transmitidos y recibidos mediante redes locales, externas y VPN, incumpliendo con los lineamientos de la Decisión Administrativa N° 641/2021 que aprueba los "REQUISITOS MÍNIMOS DE SEGURIDAD DE LA INFORMACIÓN PARA LOS ORGANISMOS DEL SECTOR PÚBLICO NACIONAL. La carencia de esta documentación no garantiza el intercambio de información con total seguridad, confidencialidad e integridad para prevenir su pérdida, modificación o uso inadecuado. Esta observación proviene del Informe N° 20/2015.
Recomendación: Redactar políticas, normas y procedimientos sobre protección de datos en redes de comunicaciones, de acuerdo a la normativa vigente. Se deberá establecer mecanismos de protección para los datos que se transmiten por las redes de telecomunicaciones, mediante técnicas de encriptación por "hardware" y/o "software" que garanticen el intercambio de información con total seguridad, implementando técnicas y procesos de autenticación, confidencialidad e integridad de la información para prevenir su pérdida, modificación o uso inadecuado.

3.3.10 A raíz de las entrevistas mantenidas con las áreas sustantivas se detectó que al no resultarles suficientes los sistemas utilizados recurren a la elaboración de archivos Excel complementarios. Los mismos almacenan información sensible que en algunos casos son guardados en servidores de empresas privadas extranjeras (Google Drive) o en soportes externos. Esta situación incrementa la posibilidad de filtración de datos y/o pérdida de la información, poniendo en riesgo la seguridad, integridad y soberanía de dicha información.
Recomendación: Se recomienda establecer un entorno interno seguro en el que se migre la información que actualmente se encuentra alojada tanto en servidores de empresas privadas extranjeras como en soportes externos extraíbles, bajo la órbita, el control y las buenas prácticas de la Dirección de Informática, incluyendo procesos de backup con el fin de preservar esa información.

4. CONCLUSION

Como resultado de las tareas realizadas y en base al objeto de la auditoría que implica evaluar la seguridad, confidencialidad, disponibilidad de la base de datos de la Administración, surgen como observaciones más relevantes la falta de integración de las bases de datos, lo que afecta al aprovechamiento de recursos e imposibilita la integración de información que puede resultar útil a otras áreas. Se han encontrado bases de datos que de ser utilizadas en forma unificada permitiría la normalización de las mismas y evitaría la duplicación de datos. Se detectaron áreas que no encuentran en los sistemas la posibilidad de almacenar toda la información que generan por lo que tienen que apelar al uso de documentos y planillas complementarias que se encuentran alojadas en servidores de empresas privadas extranjeras, poniendo en riesgo la seguridad, integridad y soberanía de dicha información

Asimismo, se observó que el plan de contingencia no contempla todos los riesgos que pudieran afectar la continuidad de los servicios críticos, la falta de procedimientos operativos aprobados formalmente y la carencia de un esquema de backup y recuperación de la información.

Es del caso resaltar que, para consolidar la gestión de la seguridad de la información de la ANMAT, la Dirección de Informática se encuentra abocada a la aprobación de la política de seguridad de la información. La misma resulta de suma importancia a los fines de proteger la información y continuidad de los procesos y/o servicios, a través del resguardo de la confidencialidad, conservación de la integridad y mantenimiento de la disponibilidad de la información de todos los recursos tecnológicos de la ANMAT.

Cabe destacar, que se encuentra en ejecución la etapa inicial de la unificación de las Bases de Datos del Organismo, ello a través de la conformación de un equipo de trabajo para el desarrollo del proyecto denominado “DISPOWEB” que es una herramienta de consulta de los actos dispositivos emanados del organismo.

Por otro lado, es dable mencionar que ante la declaración de la pandemia y el rol de suma importancia que debió asumir el organismo, las áreas debieron implementar soluciones alternativas como compartir la información sensible a través herramientas que están fuera de la órbita de la ANMAT para garantizar la continuidad de las actividades críticas.

Por lo expuesto, se concluye que la integración e unificación de las bases de datos y la aprobación e implementación de las políticas de seguridad de la información de la ANMAT permitirán un avance sustancial de mejora ante las debilidades aquí planteadas.

Ciudad Autónoma de Buenos Aires, 30 de Septiembre de 2022.