República Argentina - Poder Ejecutivo Nacional
AÑO DE LA DEFENSA DE LA VIDA, LA LIBERTAD Y LA PROPIEDAD

Informe

Número: IF-2024-07952715-APN-DGA#ANMAT

CIUDAD DE BUENOS AIRES
Martes 23 de Enero de 2024

Referencia: PLAN DE SEGURIDAD DE LA A.N.M.A.T

Plan de Seguridad de la A.N.M.A.T.

Para la adecuación a los “Requisitos Mínimos de Seguridad de la Información para los Organismos del Sector Público Nacional” aprobados por la Decisión Administrativa 641/2021.

CONTEXTO

La Jefatura de Gabinete de Ministros del Gobierno Nacional aprobó, mediante la Decisión Administrativa Nº 641/2021, los “REQUISITOS MÍNIMOS DE SEGURIDAD DE LA INFORMACIÓN PARA LOS ORGANISMOS DEL SECTOR PÚBLICO NACIONAL”, a la vez que estableció el deber de que cada organismo apruebe un Plan de Seguridad que establezca los plazos en que dará cumplimiento a cada uno de esos “requisitos mínimos”, plazos que no deberán exceder la fecha del 31 de diciembre de 2022.

El mismo acto administrativo estableció el deber de que la máxima autoridad de cada organismo asigne las funciones relativas a la seguridad de sus sistemas de información al área con competencia en la materia e informar, mediante Comunicación Oficial a través del Sistema de Gestión Documental Electrónica (GDE) a la Dirección Nacional de Ciberseguridad de la Secretaría de Innovación Pública de la Jefatura de Gabinete de Ministros el nombre, apellido y datos de contacto del responsable del área designada, lo que en el ámbito de la A.N.M.A.T. fue cumplimentado mediante la comunicación NO-2021-70972143-APN-ANMAT#MS, recayendo la asignación de funciones referida en la Dirección de Informática (DINF).

La DINF realizó una revisión de los lineamientos que integran los requisitos mínimos establecidos, confrontándolos con prácticas y procedimientos vigentes en el ámbito operativo de las áreas involucradas en ANMAT, considerando las dependencias instrumentales existentes entre esos lineamientos, estimando preliminarmente el impacto operativo de las adecuaciones necesarias y estructurando un cronograma consistente con esas observaciones y con la fecha límite fijada.

Como resultado de esa tarea, se ha elaborado el presente Plan de Seguridad, que deberá guiar las acciones de los próximos meses, orientadas a realizar las adecuaciones operativas para dar cumplimiento a los requisitos mínimos de seguridad de la información en vigor.

SÍNTESIS DE LA SITUACIÓN OBSERVADA

El siguiente cuadro resume cuantitativamente las observaciones realizadas por la Dirección de Informática en relación con el grado de cumplimiento de los lineamientos que integran cada una de las directrices que surgen de los requisitos mínimos de seguridad de la información aprobados.

Directrices	Lineamientos				Grado de adecuación
	Total	Si	No	N/A	
1 Política de Seguridad de la Información del Organismo	6	0	6		0%
2 Aspectos Organizativos de la Seguridad	7	2	5		29%
3 Seguridad Informática de los RRHH	7	0	7		0%
4 Gestión de Activos	4	0	4		0%
5 Autenticación, Autorización y Control de Accesos	7	4	3		57%
6 Uso de herramientas criptográficas	3	1	2		33%
7 Seguridad física y ambiental	9	3	6		33%
8 Seguridad Operativa	11	3	8		27%
9 Seguridad en las comunicaciones	6	3	3		50%

10	Adquisición, desarrollo y mantenimiento de sistemas de información	8	5	3	62%
11	Relación con proveedores	5	3	2	60%
12	Gestión de incidentes de seguridad	7	3	4	43%
13	Aspectos de seguridad para la continuidad de la gestión	4	0	4	0%
14	Cumplimiento	5	1	4	20%

CRONOGRAMA DE ADECUACIONES PREVISTO Y ÁREAS INVOLUCRADAS

Se presenta a continuación el detalle de los lineamientos agrupados bajo las directrices establecidas por la DA 641/2021, para los que se ha previsto la necesidad de realizar algún grado de adecuación en el marco del presente plan.

Para cada uno de esos lineamientos se identifica(n) la(s) unidad(es) operativa(s) en cuyo ámbito se desarrollan las prácticas afectadas, o que deberá(n) intervenir primariamente en ese proceso de adecuación.

Las unidades operativas aparecen identificadas de acuerdo a la siguiente codificación:

UAI		Unidad de Auditoría Interna
CPEYPR		Coordinación de Planificación y Evaluación de Impacto de Procesos Regulatorios
DGA		Dirección General de Administración

DINF		Dirección de Informática
DRRHH		Dirección de Recursos Humanos
DAJ		Dirección de Asuntos Jurídicos
CC		Coordinación de Compras
ASUST		Áreas sustantivas del organismo

ITEM	DESCRIPCION	CUMPLE	Descripción/justificación	Áreas	Fecha Regularización
1	**Política de Seguridad de la Información del organismo**				
1.1	Aprobada por las máximas autoridades del organismo o por el funcionario a quien se le ha delegado la función.	SI	Se encuentra aprobada mediante la Disposición ANMAT N° DI-2022-9703-APN-ANMAT#MS		
1.2	Notificada y difundida a todo el personal y a aquellos terceros involucrados cuando resulte pertinente y en los aspectos que corresponda.	NO	Se prevé notificar y difundir la política de seguridad a todo el personal y a aquellos terceros cuando resulte pertinente.	DRRHH	OCTUBRE 2023
1.3	Cumplida por todos los agentes y	NO	Se confeccionarán indicadores los cuales	DRRHH	JULIO 2024

	funcionarios del organismo.		permitirán medir el grado de cumplimiento de la política de seguridad por parte del personal del organismo.	DGA DINF	
1.4	Revisada y eventualmente actualizada, con una periodicidad no superior a DOCE (12) meses.	NO	Se prevé su revisión y actualización anual.	DINF DAJ DGA	ENERO 2025
1.5	Utilizada como base para establecer un conjunto de normas, procedimientos, lineamientos y guías acordes a los procesos que se llevan adelante en el organismo, su plataforma tecnológica y demás recursos de los que disponga.	SI	Una vez aprobada, se utilizará como base para la elaboración de las normas y procedimientos vinculados a los procesos del Organismo.		
1.6	Informada a la Dirección Nacional de Ciberseguridad una vez aprobada.	SI	Fue informada a la Dirección Nacional de Ciberseguridad mediante nota NO-2022-132504526-APN-DGA#ANMAT|		
2.0	**Aspectos Organizativos de la Seguridad**				
2.1	Asignar a un área del organismo con competencia en la materia las responsabilidades relativas a la seguridad de la información, incluyendo el cumplimiento de las directrices del presente documento. Se deberá informar a la Dirección Nacional de Ciberseguridad el nombre y datos de contacto del responsable del área a la que se le han asignado las funciones y mantener dichos datos actualizados.	SI			
2.2	Segregar las funciones y áreas de responsabilidad en conflicto para incrementar los niveles de seguridad de la información. En la medida de lo posible, se recomienda que las funciones de seguridad de la información no dependan del área de Sistemas o Tecnología de la Información.	NO	La segregación de las funciones de seguridad de la información será puesta a consideración de las autoridades competentes debido a la falta de personal idóneo. A tal fin, se prevé la contratación de un servicio externo que realice dicha tarea.	DINF DGA	JULIO 2024

2.3	Impulsar desde el mayor nivel jerárquico las iniciativas que se propongan con el objeto de preservar la confidencialidad, integridad y disponibilidad de la información que se gestiona.	SI			
2.4	Abordar los aspectos referidos a la seguridad de la información en el diseño y la gestión de todos los proyectos que lleve adelante el organismo, dejando evidencia de tal intervención.	NO	Actualmente los aspectos referidos a la seguridad de la información son realizados informalmente, a partir de la aprobación y difusión de las políticas de seguridad, se formalizarán los mismos.	DGA ASUST	ENERO 2025
2.5	Establecer como falta, sobre la base del régimen sancionatorio establecido en la Ley Marco de Regulación de Empleo Público Nacional N° 25.164, su Decreto Reglamentario N° 1421/02 y sus normas modificatorias y complementarias, el incumplimiento de la Política de Seguridad del organismo y de los requisitos mínimos contenidos en el presente documento, por parte de los agentes y funcionarios, incluyendo una graduación en las responsabilidades y sanciones administrativas que se aplicarán de acuerdo a la gravedad de la infracción cometida, sin perjuicio de las acciones legales que pudieran corresponder.	NO	El establecimiento como falta del incumplimiento de la Política de Seguridad en los términos señalados, será factible una vez que la política se encuentre aprobada, comunicada y atendiendo progresivamente los lineamientos adoptados.	DGA DRRHH DAJ	JULIO 2024
2.6	Incluir en los contratos, Términos de Referencia o en el instrumento mediante el cual se materialice la contratación del personal que se emplee bajo las modalidades que correspondan, cláusulas que contemplen el incumplimiento de la Política de Seguridad del organismo y de los requisitos mínimos contenidos en el presente documento, incluyendo una graduación en las responsabilidades y sanciones que se aplicarán de acuerdo a la gravedad de la infracción cometida, sin perjuicio de las acciones legales que pudieran corresponder.	NO	La inclusión de cláusulas vinculadas al incumplimiento de la política de seguridad será aplicable una vez que la política de seguridad se encuentre aprobada.	DRRHH	OCTUBRE 2023

2.7	Establecer mecanismos adecuados de seguridad para el trabajo remoto y para el uso de dispositivos móviles, sean estos provistos por el organismo o propiedad de agentes y funcionarios, según la criticidad de la información involucrada y del nivel jerárquico del funcionario.	NO	Los mencionados mecanismos serán establecidos una vez aprobada la política de Seguridad de la información.	DINF	ENERO 2025
3.0	**Seguridad Informática de los Recursos Humanos**				
3.1	Realizar e implementar planes de concientización en el uso seguro y responsable de los activos de información, que incluyan capacitaciones periódicas destinadas a todos los agentes y funcionarios del organismo, diseñándolos para cada tipo de público y con distintas temáticas.	NO	Existe una comunicación frecuente de pautas y lineamientos de uso seguro de los recursos, así como indicaciones para la prevención de amenazas incidentales. Se prevé una formalización y adecuación a diferentes públicos de estas comunicaciones, sobre la base de los lineamientos de la política de seguridad, una vez aprobada.	DRRHH DINF DGA	JULIO 2024
3.2	Promover el entrenamiento permanente de quienes desarrollan funciones en áreas de seguridad, tecnologías de la información, desarrollo de software e infraestructura.	NO	Se pondrá al alcance del personal de informática que desarrollen funciones de seguridad, oferta de cursos afines.	DINF	JULIO 2024
3.3	Establecer la obligatoriedad de la suscripción de actas o compromisos respecto a la seguridad de la información para todos los empleados del organismo, cualquiera sea su modalidad de contratación, teniendo en cuenta que las responsabilidades correspondientes pueden exceder la vigencia de la relación laboral.	NO	Este tipo de compromisos está presente en general. Sin embargo, el establecimiento de su obligatoriedad podrá tener lugar sobre la base de la operación de la política de seguridad del organismo.	DRRHH DAJ DGA	OCTUBRE 2023
3.4	Establecer claramente los requerimientos de seguridad de la información, que incluya niveles de acceso a la información para cada perfil de trabajo.	NO	Si bien hoy se segmentan los requerimientos informalmente, luego de la aprobación de la Política de seguridad, se realizará formalmente.	DINF	JULIO 2024
3.5	Incluir los aspectos de seguridad en las etapas de inducción de los agentes, y evaluarlos durante toda la relación laboral.	NO	Dichos aspectos serán contemplados sobre la base de la operación de la política de seguridad del organismo.	DRRHH	OCTUBRE 2023

3.6	Requerir a los agentes y funcionarios, cuando el organismo lo considere necesario, de acuerdo a sus competencias, la firma de un acuerdo de confidencialidad.	NO	Dicha tarea está prevista una vez aprobada la política de seguridad.	DRRHH	OCTUBRE 2023
3.7	Incorporar dentro de los procesos disciplinarios cualquier violación a las políticas de seguridad del organismo.	NO	La incorporación dentro de los procesos disciplinarios de las mencionadas violaciones será abordada luego de la aprobación y difusión de la política de seguridad.	DRRHH DAJ	OCTUBRE 2023
4.0	**Gestión de Activos**				
4.1	Clasificar los activos de información, en línea con el tipo y la importancia de la información que gestionan para el organismo.	NO	Actualmente existe una clasificación asistemática de los activos de información con el propósito de darles un tratamiento acorde a su tipo de importancia. Los mismos se clasificarán sistemáticamente con la adopción de la Política de Seguridad una vez aprobada.	DINF	ENERO 2025
4.2	Llevar un inventario actualizado en el que se detallen los datos necesarios para conocer la ubicación, el propietario y las responsabilidades correspondientes de cada activo.	NO	El mencionado inventario se confeccionará bajo los lineamientos de la Política de Seguridad.	DINF	ENERO 2025
4.3	Exigir a todos los agentes y empleados la devolución de los activos de información en su poder al finalizar la relación laboral o cuando un cambio en las funciones lo requiera.	NO	Dicha tarea se desarrollará bajo los lineamientos de la Política de Seguridad una vez aprobada.	DINF	ENERO 2025
4.4	Efectuar una destrucción segura de cualquier medio que pueda contener información o datos personales, en función de su nivel de criticidad, sobre la base de un procedimiento documentado, una vez que se haya catalogado como defectuoso o rezago.	NO	Dicha tarea se desarrollará bajo los lineamientos de la Política de Seguridad una vez aprobada.	DINF	ENERO 2025
5.0	**Autenticación, Autorización y Control de**				

	Accesos				
5.1	Utilizar en todos los casos el principio de “necesidad de saber”, es decir que solo se otorguen privilegios de acceso en la medida en que sean requeridos para las actividades y tareas que cada empleado o funcionario debe llevar adelante.	SI	https://webinterna.anmat.gob.ar/gestion-administrativa-direccion-informatica		
5.3	Hacer una adecuada y oportuna gestión de las altas y bajas de cuentas de usuario y privilegios, coordinando con las áreas de Recursos Humanos y aquellas en las que el empleado se desempeña toda novedad que pudiera impactar en ellos.	SI	Mails de alta y baja usuarios desde RRHH		
5.4	Realizar un seguimiento detallado sobre las cuentas con privilegios especiales.	NO	Se prevé realizar un inventario sobre las cuentas de privilegios especiales y luego un seguimiento de las mismas.	DINF	JULIO 2024
5.5	Revisar periódicamente todos los permisos de acceso a los sistemas y a la infraestructura de procesamiento.	NO	Se definirá un procedimiento que realice esta revisión.	DINF	JULIO 2024
5.6	Requerir a los agentes, funcionarios y demás usuarios un uso responsable de sus dispositivos y datos de autenticación, dejando sentado que se encuentra estrictamente prohibido compartirlos y que deben ser mantenidos seguros en forma permanente.	NO	Se pondrá en conocimiento la Política de Uso Aceptable (PUA) luego de la aprobación de la Política de Seguridad.	DINF	JULIO 2024
5.7	Restringir y controlar la asignación y uso de derechos de accesos privilegiados.	SI	https://webinterna.anmat.gob.ar/gestion-administrativa-direccion-informatica		
5.8	Limitar y monitorear el acceso al código fuente de los programas.	SI	Se utiliza Microsoft teams para gestionar fuentes y versionados solo acceden desarrolladores		
6.0	**Uso de herramientas criptográficas**				

6.1	Requerir el cifrado de cualquier dispositivo del organismo que contenga información considerada crítica y cuando involucre datos personales, especialmente cuando este se lleve fuera de la institución.	NO	En cada caso se evaluará las mejores opciones disponibles para el traslado de la información fuera de la institución.	DINF ASUST	ENERO 2025
6.2	Proteger adecuadamente los dispositivos y las claves criptográficas durante todo su ciclo de vida.	NO	Este punto será previsto en la Política de Uso Aceptable (PUA) luego de la aprobación de la Política de Seguridad.	DINF ASUST	ENERO 2025
6.3	Utilizar certificados digitales en todos los sitios de Internet del organismo.	SI	Certificados y wildcards de renovación anual		
7.0	**Seguridad física y ambiental**				
7.1	La identificación y protección de áreas seguras contra desastres naturales, ataques maliciosos o accidentales.	NO	Dicha tarea está prevista y se desarrollará bajo los lineamientos de la Política de Seguridad una vez aprobada.	DINF DGA	JULIO 2024
7.2	La incorporación de controles físicos de ingreso/egreso, con los respectivos controles de identificación, cronológicos y de funcionamiento asociados, en aquellas áreas donde se encuentren resguardados los activos de información.	SI	Acceso mediante imagen del rostro.		
7.3	El registro de los activos físicos que procesan información, indicando su identificación, localización física y asignación organizacional y personal para su uso.	NO	Dicha tarea está prevista y se desarrollará bajo los lineamientos de la Política de Seguridad una vez aprobada.	DINF	ENERO 2025
7.4	La adopción de medidas de seguridad para que el equipamiento sea ingresado o retirado del organismo con una autorización previa y habiéndose adoptado todos los recaudos del caso.	SI	Se utilizan notas de entrada y salida para movimiento de equipamiento, identificándolo con su número de serie y patrimonio		
7.5	El cuidado de los puestos de trabajo, mediante mecanismos de bloqueo de sesión	NO	Mediante la implementación de la Política de Seguridad se informará a los usuarios	DINF DRRHH	JULIO 2024

	y escritorio despejado.		sobre las buenas prácticas de utilización de recursos.		
7.6	La adopción de medidas para evitar la pérdida, daño, robo o el compromiso de los activos de información del organismo y la interrupción de sus operaciones.	NO	Mediante la implementación de la Política de Seguridad se informará a los usuarios sobre las buenas prácticas de utilización de recursos.	DINF DRRHH	JULIO 2024
7.7	La protección frente a interrupciones, interferencia o daños de los cables eléctricos y de red que transporten datos o apoyen los servicios de información.	NO	Se adoptarán las medidas de protección mencionadas a través de la implementación de la Política de Seguridad. Se deberá abrir una licitación para convertir enlaces entre dependencias a alta disponibilidad, mediante la duplicación del servicio.	DINF DGA	ENERO 2025
7.8	El mantenimiento del equipamiento para contribuir a su disponibilidad e integridad contínua.	SI	Se contrata anualmente mantenimiento de servidores con resposición de partes		
7.9	La adopción de medidas de seguridad para los activos informáticos que deben llevarse fuera del organismo, considerando los distintos riesgos de trabajar fuera de sus dependencias, en lo que hace al resguardo de la información y a la seguridad física de los dispositivos.	NO	Al no ser una modalidad de trabajo habitual, requiere de una identificación precisa de las situaciones que lo ameritan, del impacto operativo y las opciones técnicas convenientes.	DINF ASUST	ENERO 2025
8.0	**Seguridad operativa**				
8.1	Establecer las responsabilidades y los procedimientos para la gestión y la operación para todas las instalaciones de procesamiento de información.	NO	Se establecerán las responsabilidades en la Política de Seguridad y en los procedimientos del área.	DINF DGA	ENERO 2024
8.2	Revisar, monitorear y ajustar los requerimientos de capacidad desde la perspectiva de la seguridad de la información.	NO	Actualmente se realiza esta tarea de manera informal, ampliando capacidades de procesamiento y almacenamiento de las maquinas virtuales. Se confeccionará un procedimiento que describa esta tarea	DINF	ENERO 2024

			formalmente.		
8.3	Minimizar los riesgos de acceso o de cambios no autorizados en entornos productivos, separando los entornos de desarrollo, prueba y producción, en los casos que corresponda.	NO	En la actualidad se hayan separados los mencionados entornos, pero las aplicaciones legacy no cumplen con esta prerrogativa; debido a la complejidad de las mencionadas aplicaciones se deberá aguardar al cumplimiento del ciclo de vida de las mismas.	DINF	JULIO 2024
8.4	Implementar un monitoreo continuo sobre la seguridad de los sistemas e infraestructuras que soportan las operaciones críticas del organismo.	NO	Se prevé la implementación de herramientas de monitoreo estilo NAGIOS	DINF	JULIO 2024
8.5	Proteger las instalaciones contra infecciones de código malicioso.	SI	Programación con buenas practicas contra inyección de sql, antivirus, antispam, firewall y demás herramientas de seguridad informática vigente	DINF	
8.6	Realizar copias de resguardo del software y la información con una periodicidad y modalidad acordes con su criticidad de los datos y con los procesos que se lleven a cabo, probándolas periódicamente y estableciendo un registro de las pruebas de restauración que permitan conocer quién participó del proceso, cuándo y cómo lo hizo y dónde se encuentra la copia.	NO	Se utiliza veeam backup (mostrar reglas de backup)		ENERO 2024
8.7	Llevar registro de todos los eventos de seguridad y revisarlo periódicamente con el fin de detectar posibles incidentes.	NO	Se confeccionará un procedimiento que describa esta tarea formalmente.	DINF	ENERO 2024
8.8	Mantener un control estricto sobre el software y su integridad, en entornos productivos.	SI	Microsoft teams		
8.9	Identificar y gestionar adecuadamente las vulnerabilidades, así como el proceso de gestión de actualizaciones de todo el	SI	A través de las contrataciones de mantenimiento de software evolutivo y correctivo, de igual forma internamente con		

	software utilizado. En los casos que el mismo sea provisto por terceros, contar con una política de actualización para evitar que se afecte la operación.		apps propias		
8.10	Gestionar de manera apropiada los reportes de vulnerabilidades y recomendaciones de actualización.	NO	Actualmente se reciben novedades y actualizaciones del cert.ar debido a que ANMAT es miembro partícipe de la ciberseguridad del estado. Se confeccionará un procedimiento para informar las novedades de su incumbencia.	DINF	ENERO 2024
8.11	Registrar y revisar periódicamente las actividades de los administradores y operadores	NO	No se encuentra en vigor un procedimiento recurrente de revisión de la actividad de los usuarios de los niveles referidos.	DINF	JULIO 2024
9.0	**Seguridad en las comunicaciones**				
9.1	Segregar, en la medida de las posibilidades, los grupos de servicios de información, usuarios y sistemas en las redes.	SI	Nuevo AD con políticas y permisos		
9.2	Proteger adecuadamente la información que se transfiera dentro del organismo y hacia cualquier entidad externa, incluyendo aquella que se transmita a través de servicios de correo electrónico.	NO	Esto se implementará a partir de la aprobación de las políticas de seguridad del organismo.	DINF DGA DRRHH	JULIO 2024
9.3	Exigir el uso de la cuenta de correo electrónico institucional a todos los agentes y funcionarios del organismo para toda comunicación vinculada con sus funciones, informando los riesgos de este incumplimiento.	NO	Esto se implementará a partir de la aprobación de las políticas de seguridad del organismo,	DINF DGA DRRHH	JULIO 2024
9.4	Incluir mecanismos que garanticen las transferencias seguras en los acuerdos de servicio celebrados, tanto para servicios internos como tercerizados.	NO	Se incluirán en los pliegos que se generen a partir de la aprobación de las políticas de seguridad del organismo.	DINF CC	JULIO 2024

9.5	Incorporar acuerdos y cláusulas de confidencialidad y no divulgación según las necesidades del organismo en todos los acuerdos que se suscriban.	SI	Copia de algún pliego de contratación (están hechos en base a modelos de ONTI y supervisado por ellos)		
9.6	Incorporar acuerdos y cláusulas de confidencialidad y no divulgación cuando el organismo entienda que resulta conveniente para el tipo de información que trate.	SI	Copia de algún pliego de contratación (están hechos en base a modelos de ONTI y supervisado por ellos)		
10.0	**Adquisición, desarrollo y mantenimiento de sistemas de información**				
10.1	Especificar lineamientos de seguridad desde la fase inicial del proceso de adquisición o desarrollo de un sistema (seguridad desde el diseño), cuando el proceso de contratación sea gestionado por el propio organismo.	SI	Copia de algún pliego de contratación (están hechos en base a modelos de ONTI y supervisado por ellos)		
10.2	Utilizar una metodología de desarrollo seguro, capacitando a los desarrolladores e incorporando cláusulas en las especificaciones técnicas de los pliegos de bases y condiciones particulares.	SI	Copia de algún pliego de contratación (están hechos en base a modelos de ONTI y supervisado por ellos)		
10.3	Controlar los cambios que se realicen a las aplicaciones, implementando controles adecuados en las instancias de desarrollo, prueba y producción e incorporando efectivos controles cruzados o por oposición.	NO	Se generará un procedimiento de control de cambios de software.	DINF	JULIO 2024
10.4	Proteger los datos utilizados en las pruebas, evitando la utilización de bases de datos reales.	SI			
10.5	Utilizar protocolos que garanticen la transmisión o enrutamiento adecuados que eviten la divulgación, alteración o duplicación no autorizadas de transacciones.	NO	Esto se implementará a partir de la aprobación de las políticas de seguridad del organismo.	DINF	JULIO 2024

10.6	Evaluar la seguridad de las aplicaciones antes de ponerlas productivas, especialmente aquellas que se gestionen a través de Internet.	SI			
10.7	Proteger la información gestionada por aplicaciones web contra la actividad fraudulenta y los incumplimientos contractuales y de las normas legales vigentes.	NO	Esto se implementará a partir de la aprobación de las políticas de seguridad del organismo.	DINF DAJ UAI	JULIO 2024
10.8	Controlar y supervisar el efectivo cumplimiento y las actividades realizadas por el contratante en aquellas contrataciones de bienes y servicios efectuadas por el organismo.	SI	Los pliegos tienen etapas de conformidad donde se controla el cumplimiento		
11	**Relación con proveedores**				
11.1	La consideración de aspectos vinculados con la identificación, análisis y gestión de riesgo desde el estudio de factibilidad de cualquier decisión de contratación de bienes y servicios bajo cualquier modalidad contractual.	NO	Esto se implementará a partir de la aprobación de las políticas de seguridad del organismo.	DINF DGA	ENERO 2025
11.2	El establecimiento e inclusión en el pliego de bases y condiciones particulares de todos los requisitos de seguridad de la información pertinentes, en los acuerdos que se suscriban con cada proveedor que pueda acceder, procesar, almacenar, comunicar o proporcionar componentes de infraestructura tecnológica al organismo.	NO	Esto se implementará a partir de la aprobación de las políticas de seguridad del organismo.	DINF DGA CC	ENERO 2025
11.3	La supervisión y revisión por parte de los responsables asignados al proyecto de todos los niveles de seguridad acordados.	SI	Ver las finalizaciones de etapas		
11.4	La inclusión de cláusulas para mantenimiento del nivel de servicio,	SI	Ver los SLA en los pliegos		

	especialmente en servicios de provisión crítica, que permitan mantener su disponibilidad.				
11.5	La inclusión en el pliego de bases y condiciones de estipulaciones tendientes al cumplimiento de todas las normas legales y contractuales que sean aplicables.	SI	Ver pliegos actuales		
12	**Gestión de incidentes de seguridad**				
12.1	Identificar las debilidades en los procesos de gestión de información del organismo, de manera de adoptar las medidas que prevengan la ocurrencia de incidentes de seguridad.	NO	Se conformarán grupos de trabajo para los procesos definidos en el manual de gestión de la Organización 1000-MGO versión vigente para abordar esta tarea.	DINF DGA CPYEIPR ASUST	ENERO 2025
12.2	Contar con procedimientos de gestión de incidentes de seguridad documentados, aprobados y adecuadamente comunicados, de acuerdo a las áreas funcionales que considere necesarias.	NO	Los mismos serán confeccionados bajo los lineamientos de la Política de Seguridad una vez formalizada en el Sistema de Gestión Documental.	DINF CPYEIPR	ENERO 2025
12.3	Adoptar una estrategia clara de priorización y escalamiento, que incluya la comunicación a las áreas involucradas, autoridades y a las áreas técnicas.	NO	A tal fin, se confeccionarán procedimientos bajo los lineamientos de la Política de Seguridad.	DINF	ENERO 2025
12.4	Instruir a los agentes para la prevención, detección y reporte de incidentes de seguridad, según las responsabilidades correspondientes.	NO	Esto se implementará a partir de la aprobación de las políticas de seguridad del organismo.	DINF DGA DRRHH	JULIO 2024
12.5	Notificar a la Dirección Nacional de Ciberseguridad de la ocurrencia de incidentes de seguridad, en un plazo no superior a CUARENTA Y OCHO (48) horas de su detección.	SI			

12.6	Recopilar la evidencia necesaria para adoptar medidas administrativas o judiciales posteriores, de corresponder, resguardando la cadena de custodia	SI			
12.7	En el caso en que el incidente de seguridad hubiere afectado activos de información y hubiere comprometido información y/o datos personales de terceros, se deberá informar públicamente tal ocurrencia.	SI			
13	**Aspectos de seguridad para la continuidad de la gestión**				
13.1	Identificar los requisitos necesarios para cumplir todos los requerimientos de seguridad de la información ante un evento inesperado que impida seguir operando, con foco en los servicios esenciales que preste el organismo.	NO	Dicha tarea se realizará a fin de actualizar el plan de contingencia.	DINF	ENERO 2025
13.2	Establecer, documentar, implementar y mantener los procesos, procedimientos y controles tendientes al mantenimiento de un nivel de continuidad de la seguridad de la información durante situaciones adversas.	NO	Dicha tarea se realizará a fin de actualizar el plan de contingencia.	DINF	ENERO 2025
13.3	Verificar, revisar y evaluar a intervalos regulares los controles de continuidad de la seguridad de la información.	NO	Dicha tarea se realizará a fin de actualizar el plan de contingencia.	DINF	ENERO 2025
13.4	Implementar mecanismos para proteger la disponibilidad de la información crítica y de las instalaciones utilizadas para su procesamiento durante situaciones adversas.	NO	Dicha tarea se realizará a fin de actualizar el plan de contingencia.	DINF	ENERO 2025
14	**Cumplimiento**				
14.1	La identificación, documentación y actualización periódica de los requisitos	NO	Se deberá generar un procedimiento para la actualización periódica.	DINF DAJ	JULIO 2024

	legales y contractuales para cada sistema de información que utilice.				
14.2	El cumplimiento de la Ley No 25.326 de Protección de los Datos Personales y sus normas reglamentarias y complementarias.	SI			
14.3	La revisión periódica de los sistemas de información para verificar el cumplimiento de las políticas y normas de seguridad de la información del organismo.	NO	Se confeccionará un procedimiento para la actualización periódica.	DINF	JULIO 2024
14.4	La supervisión del cumplimiento de todos los requisitos de seguridad contenidos en la legislación aplicable, incluyendo las directrices del presente documento, y en las políticas y procedimientos del organismo, por parte de los responsables de cada área del organismo, respecto a su personal y a la información que gestiona.	NO	Esto se implementará a partir de la aprobación de las políticas de seguridad del organismo.	ASUST	JULIO 2024
14.5	Considerar la adopción de las medidas correctivas que surjan de auditorías y revisiones periódicas de cumplimiento de los presentes requisitos, sean estas realizadas por personal del área, de organismos competentes o de terceros habilitados a tal fin.	SI			

Digitally signed by GESTION DOCUMENTAL ELECTRONICA - GDE
Date: 2024.01.23 13:07:44 -03:00

Pablo Scagliarini
Director
Dirección General de Administración
Administración Nacional de Medicamentos, Alimentos y Tecnología Médica

Digitally signed by GESTION DOCUMENTAL ELECTRONICA - GDE
Date: 2024.01.23 13:07:45 -03:00