República Argentina - Poder Ejecutivo Nacional
2021 - Año de Homenaje al Premio Nobel de Medicina Dr. César Milstein

Anexo

Número: IF-2021-50348419-APN-SSTIYC#JGM

CIUDAD DE BUENOS AIRES
Viernes 4 de Junio de 2021

Referencia: ANEXO I - REQUISITOS MÍNIMOS DE SEGURIDAD DE LA INFORMACIÓN PARA LOS ORGANISMOS DEL SPN

ANEXO I

REQUISITOS MÍNIMOS DE SEGURIDAD DE LA INFORMACIÓN [1]

PARA LOS ORGANISMOS DEL SECTOR PÚBLICO NACIONAL

I. INTRODUCCIÓN

Los organismos del Sector Público Nacional comprendidos en el artículo 8º de la Ley Nº 24.156 y sus modificatorias son de los principales receptores y productores de información de nuestro país. Esa información pertenece mayormente a sus habitantes y a las diversas entidades públicas y privadas que desarrollan sus actividades en su territorio. Todos ellos confían sus datos a los organismos que lo componen para distintos fines.

La información puede ser hoy en día objeto de una amplia gama de peligros, amenazas y usos indebidos e ilícitos, debiéndose, por lo tanto, extremar las medidas tendientes a la preservación de su confidencialidad, integridad y disponibilidad. Con esto se busca proteger los derechos y libertades individuales de las personas al tiempo de contribuir a la efectiva prestación continua e ininterrumpida de los diversos servicios prestados por las diferentes entidades y jurisdicciones y, al mismo tiempo, propender a su correcta y mejor gestión interna.

En un contexto de transversalidad en el uso de las tecnologías para la vida social, económica, política y cultural de las personas, la seguridad de la información cumple un rol fundamental. Por consiguiente, los agentes públicos, cualquiera sea el nivel jerárquico y la modalidad de contratación, tienen la obligación de dar tratamiento y hacer un uso responsable, seguro y cuidado de los datos que utilizan en sus labores habituales, adoptando todas las medidas a su alcance para protegerlos.

Los responsables de los activos de la información deben atender y diligenciar los recursos necesarios para asegurar el cumplimiento de los objetivos de la presente en el ámbito de su jurisdicción. En tal sentido, los datos gestionados en los organismos deben ser protegidos tanto dentro como fuera del ámbito institucional, con independencia del formato y del soporte en el que estén contenidos y si los mismos están siendo objeto de tratamiento electrónico, se encuentran almacenados o están siendo transmitidos.

Los organismos determinarán sus políticas, normas específicas, procedimientos y guías que, sobre la base de los siguientes requisitos mínimos, sean aplicables a los procesos específicos que desarrollen. Este conjunto de normas debe surgir a partir de un análisis de los riesgos para los procesos que lleven adelante.

Se entenderán como principios de seguridad de la información a la preservación de confidencialidad, integridad y disponibilidad de la información y de los activos de información del Sector Público Nacional.

II. OBJETIVOS

Objetivo general

Establecer los lineamientos generales y mínimos para los organismos del Sector Público Nacional comprendidos en el inciso a) del artículo 8º de la Ley Nº 24.156, con el fin de proteger los activos de información, frente a riesgos internos o externos, que pudieran afectarlos, para así preservar su confidencialidad, integridad y disponibilidad.

Objetivos específicos

- Proteger los derechos de los titulares de datos personales o propietarios de información que es tratada por el Sector Público Nacional.
- Proteger la información, los datos personales y activos de información propios del conjunto de organismos que componen el Sector Público Nacional.
- Promover una política pública que enmarque una conducta responsable en materia de seguridad de la información de los organismos que conforman el Sector Público Nacional, sus agentes y funcionarios.
- Evidenciar el compromiso e interés de quienes componen el Sector Público Nacional en pos del desarrollo de una cultura de ciberseguridad.

III. ALCANCE

Las directrices que surgen de los presentes requisitos mínimos de seguridad serán de aplicación obligatoria para todos los agentes y funcionarios que se desempeñan en los organismos que componen el Sector Público Nacional según el inciso a) del artículo 8º de la Ley Nº 24.156 y sus modificatorias, en la medida que les corresponda según su función. Las autoridades máximas de los organismos públicos serán las responsables de proveer los medios necesarios para su efectivo cumplimiento y de promover su utilización.

En el caso de los entes reguladores que estén comprendidos dentro del artículo 8º de la Ley Nº 24.156 y sus modificatorias, se recomienda el análisis de una eventual incorporación de los principios de la Seguridad de la

Información. Asimismo, se sugiere la evaluación de la oportunidad y pertinencia de establecer requisitos mínimos de seguridad de la información que más adelante se detallan en la sección V. Directrices, para el sector regulado.

El cumplimiento de los presentes requisitos mínimos de seguridad será también exigible a los terceros que contraten con el Sector Público Nacional, en las secciones que sean aplicables a las tareas que realizan y en los términos que establezca cada organismo en sus disposiciones normativas y contractuales.

IV. REVISIÓN Y ACTUALIZACIÓN

Los requisitos mínimos de Seguridad serán revisados por la Dirección Nacional de Ciberseguridad de la SECRETARÍA DE INNOVACIÓN PÚBLICA de la JEFATURA DE GABINETE DE MINISTROS, o el área que la reemplace en el futuro, cuando lo estime conveniente, con una periodicidad no superior a DOCE (12) meses, a partir de su publicación o última actualización. Serán publicados también en el sitio de Internet que, a tal fin, establezca la Dirección Nacional antes citada.

V. DIRECTRICES

1. Política de Seguridad de la Información del organismo

Los organismos deben desarrollar una Política de Seguridad de la Información compatible con la responsabilidad primaria y las acciones de su competencia, sobre la base de una evaluación de los riesgos que pudieran afectarlos. Los términos de dicha política deben ser consistentes con las directrices del presente documento.

Dicha política debe ser:

- aprobada por las máximas autoridades del organismo o por el funcionario a quien se le ha delegado la función.
- notificada y difundida a todo el personal y a aquellos terceros involucrados cuando resulte pertinente y en los aspectos que corresponda.
- cumplida por todos los agentes y funcionarios del organismo.
- revisada y eventualmente actualizada, con una periodicidad no superior a DOCE (12) meses.
- 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.
- informada a la Dirección Nacional de Ciberseguridad una vez aprobada.

2. Aspectos Organizativos de la Seguridad

Se debe desarrollar e implementar un marco organizativo que habilite una efectiva gestión y operación de la seguridad de la información en el organismo.

Esto implica que se debe:

- 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.

- 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.
- 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.
- 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.
- 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.
- 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.
- 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.

3. Seguridad Informática de los Recursos Humanos

Los organismos deben adoptar una perspectiva sistémica para proteger sus activos de información, dentro de la cual el personal debe ser considerado un recurso central. Asimismo, deben establecer una política de respeto de los derechos individuales de los empleados y resguardar su privacidad. Los agentes y funcionarios deben ser concientizados y capacitados para desarrollar habilidades y conocimientos en seguridad de la información, y hacer un uso responsable de la información y de los recursos utilizados en su gestión con el fin de prevenir riesgos.

Para ello será necesario:

- 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.
- promover el entrenamiento permanente de quienes desarrollan funciones en áreas de seguridad, tecnologías de la información, desarrollo de software e infraestructura.
- 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.
- establecer claramente los requerimientos de seguridad de la información, que incluya niveles de acceso a la

información para cada perfil de trabajo.
- incluir los aspectos de seguridad en las etapas de inducción de los agentes, y evaluarlos durante toda la relación laboral.
- requerir a los agentes y funcionarios, cuando el organismo lo considere necesario, de acuerdo a sus competencias, la firma de un acuerdo de confidencialidad.
- incorporar dentro de los procesos disciplinarios cualquier violación a las políticas de seguridad del organismo.

4. Gestión de Activos

Los activos de información del organismo deben ser gestionados y protegidos en forma efectiva. En el mismo sentido, deben ser clasificados según su criticidad para el organismo desde la perspectiva de su confidencialidad, integridad y disponibilidad, teniendo en cuenta sus funciones, la normativa que les sea aplicable y cualquier otro activo que pudieran contener de otros organismos públicos o entidades privadas, lo que permitirá adoptar las medidas de protección adecuadas.

Para ello se requiere:

- clasificar los activos de información, en línea con el tipo y la importancia de la información que gestionan para el organismo.
- 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.
- 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.
- 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.

5. Autenticación, Autorización y Control de Accesos

El acceso a los activos de información del organismo debe realizarse a partir de procesos y mecanismos de seguridad definidos e implementados según su nivel de criticidad, con el fin de proveer un nivel apropiado de protección. Los privilegios de acceso deben ser otorgados en forma expresa y formalmente autorizada a quienes los requieran para sus funciones.

En consiguiente se debe:

- 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.
- 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.
- realizar un seguimiento detallado sobre las cuentas con privilegios especiales.
- revisar periódicamente todos los permisos de acceso a los sistemas y a la infraestructura de procesamiento.
- 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.

- restringir y controlar la asignación y uso de derechos de accesos privilegiados.
- limitar y monitorear el acceso al código fuente de los programas.

6. Uso de herramientas criptográficas

La confidencialidad, integridad, autenticidad y/o no repudio de la información del organismo debe ser protegida mediante técnicas de cifrado, tanto si los datos se encuentran almacenados como cuando son transmitidos.

En este marco se debe:

- 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.
- proteger adecuadamente los dispositivos y las claves criptográficas durante todo su ciclo de vida.
- utilizar certificados digitales en todos los sitios de Internet del organismo.

7. Seguridad física y ambiental

Los activos de información del organismo deben ser protegidos mediante medidas que impidan accesos no autorizados, daños e interferencia, adoptando suficientes recaudos físicos y ambientales para minimizar los riesgos asociados.

Esto implica:

- la identificación y protección de áreas seguras contra desastres naturales, ataques maliciosos o accidentales.
- 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.
- el registro de los activos físicos que procesan información, indicando su identificación, localización física y asignación organizacional y personal para su uso.
- 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.
- el cuidado de los puestos de trabajo, mediante mecanismos de bloqueo de sesión y escritorio despejado.
- 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.
- la protección frente a interrupciones, interferencia o daños de los cables eléctricos y de red que transporten datos o apoyen los servicios de información.
- el mantenimiento del equipamiento para contribuir a su disponibilidad e integridad continuas.
- 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.

8. Seguridad operativa

Las operaciones del organismo deben desarrollarse en forma segura, en todas las instalaciones de procesamiento de información, minimizando la pérdida o alteración de datos.

Para ello se debe:

- establecer las responsabilidades y los procedimientos para la gestión y la operación para todas las instalaciones de procesamiento de información.
- revisar, monitorear y ajustar los requerimientos de capacidad desde la perspectiva de la seguridad de la información.
- 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.
- implementar un monitoreo continuo sobre la seguridad de los sistemas e infraestructuras que soportan las operaciones críticas del organismo.
- proteger las instalaciones contra infecciones de código malicioso.
- 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.
- llevar registro de todos los eventos de seguridad y revisarlo periódicamente con el fin de detectar posibles incidentes.
- mantener un control estricto sobre el software y su integridad, en entornos productivos.
- identificar y gestionar adecuadamente las vulnerabilidades, así como el proceso de gestión de actualizaciones de todo el 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.
- gestionar de manera apropiada los reportes de vulnerabilidades y recomendaciones de actualización.
- registrar y revisar periódicamente las actividades de los administradores y operadores.

9. Seguridad en las comunicaciones

La información de las redes del organismo debe ser protegida y controlada adecuadamente, tanto dentro de la organización como aquella que es transferida fuera de las instalaciones del organismo.

Se debe:

- Segregar, en la medida de las posibilidades, los grupos de servicios de información, usuarios y sistemas en las redes.
- 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.
- 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.
- incluir mecanismos que garanticen las transferencias seguras en los acuerdos de servicio celebrados, tanto para servicios internos como tercerizados.
- incorporar acuerdos y cláusulas de confidencialidad y no divulgación según las necesidades del organismo en todos los acuerdos que se suscriban.
- incorporar acuerdos y cláusulas de confidencialidad y no divulgación cuando el organismo entienda que resulta conveniente para el tipo de información que trate.

10. Adquisición, desarrollo y mantenimiento de sistemas de información

La seguridad de la información debe contemplarse como una parte integral de los sistemas de información en todas las fases de su ciclo de vida, incluyendo aquellos que brinden servicios o permitan la realización de trámites

a través de Internet.

Para ello se debe:

- 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.
- 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.
- 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.
- proteger los datos utilizados en las pruebas, evitando la utilización de bases de datos reales.
- utilizar protocolos que garanticen la transmisión o enrutamiento adecuados que eviten la divulgación, alteración o duplicación no autorizadas de transacciones.
- evaluar la seguridad de las aplicaciones antes de ponerlas productivas, especialmente aquellas que se gestionen a través de Internet.
- proteger la información gestionada por aplicaciones web contra la actividad fraudulenta y los incumplimientos contractuales y de las normas legales vigentes.
- controlar y supervisar el efectivo cumplimiento y las actividades realizadas por el cocontratante en aquellas contrataciones de bienes y servicios efectuadas por el organismo.

11. Relación con proveedores

La contratación, cualquiera sea la modalidad, realizada por el organismo para la provisión de un bien o servicio debe incluir en el pliego de bases y condiciones particulares cláusulas de cumplimiento efectivo por parte del cocontratante, relacionadas con la seguridad de la información, desde el inicio del procedimiento contractual y hasta la efectiva finalización del contrato.

Esto comprende:

- 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.
- 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.
- la supervisión y revisión por parte de los responsables asignados al proyecto de todos los niveles de seguridad acordados.
- la inclusión de cláusulas para mantenimiento del nivel de servicio, especialmente en servicios de provisión crítica, que permitan mantener su disponibilidad.
- la inclusión en el pliego de bases y condiciones de estipulaciones tendientes al cumplimiento de todas las normas legales y contractuales que sean aplicables.

12. Gestión de incidentes de seguridad

El organismo debe adoptar las medidas necesarias para prevenir, detectar, gestionar, resolver y reportar los incidentes de seguridad que puedan afectar sus activos de información.

Para ello debe:

- 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.
- contar con procedimientos de gestión de incidentes de seguridad documentados, aprobados y adecuadamente comunicados, de acuerdo a las áreas funcionales que considere necesarias.
- adoptar una estrategia clara de priorización y escalamiento, que incluya la comunicación a las áreas involucradas, autoridades y a las áreas técnicas.
- instruir a los agentes para la prevención, detección y reporte de incidentes de seguridad, según las responsabilidades correspondientes.
- 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.
- recopilar la evidencia necesaria para adoptar medidas administrativas o judiciales posteriores, de corresponder, resguardando la cadena de custodia.
- 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.

13. Aspectos de seguridad para la continuidad de la gestión

Los procedimientos de continuidad de la gestión del organismo ante la ocurrencia de eventos de crisis o aquellos no planificados que impidan seguir operando en las instalaciones habituales deben contemplar todos los aspectos de seguridad de la información involucrada.

Para ello se debe:

- 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.
- 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.
- verificar, revisar y evaluar a intervalos regulares los controles de continuidad de la seguridad de la información.
- implementar mecanismos para proteger la disponibilidad de la información crítica y de las instalaciones utilizadas para su procesamiento durante situaciones adversas.

14. Cumplimiento

En todos los casos el organismo debe cumplir con las disposiciones legales, normativas y contractuales que le sean aplicables, con el fin de evitar sanciones administrativas y/o legales y que los empleados incurran en responsabilidades civiles o penales como resultado de su incumplimiento.

Esto implica:

- la identificación, documentación y actualización periódica de los requisitos legales y contractuales para cada sistema de información que utilice.

- el cumplimiento de la Ley Nº 25.326 de Protección de los Datos Personales y sus normas reglamentarias y complementarias.
- la revisión periódica de los sistemas de información para verificar el cumplimiento de las políticas y normas de seguridad de la información del organismo.
- 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.
- 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.

VI. Glosario

Los términos utilizados en este documento se encuentran incluidos en el Glosario aprobado por la Resolución N° 1523/19 de la ex-SECRETARÍA DE GOBIERNO DE MODERNIZACIÓN y en la Ley Nº 25.326 de Protección de los Datos Personales.

---

[1] Para la elaboración del presente documento se han tomado como referencia estándares nacionales e internacionales reconocidos, tales como las Normas IRAM-ISO/IEC 27001, 27002 y 20000-1.

Digitally signed by Gestion Documental Electronica
Date: 2021.06.04 18:04:28 -03:00

Martín OLMOS
Subsecretario
Subsecretaría de Tecnologías de la Información y las Comunicaciones
Jefatura de Gabinete de Ministros