Plan de Seguridad del Ministerio de Ciencia, Tecnología e Innovación de la Nación

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 del Ministerio de Ciencia, Tecnología e Innovación (MINCYT) fue cumplimentado mediante la comunicación NO-2021-59940174-APN-MCT, recayendo la asignación de funciones referida en la Dirección de Sistemas Informáticos (DSI) de la Subsecretaría de Gestion Administrativa.

La DSI 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 MINCYT, 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 laborado 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 DSI 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	SÍ	NO – N/A	
1	Política de Seguridad de la Información del organismo	6	0	6	0%
2	Aspectos Organizativos de la Seguridad	7	3	4	43%
3	Seguridad Informática de los Recursos Humanos	7	3	4	43%
4	Gestión de Activos	4	3	1	75%
5	Autenticación, Autorización y Control de Accesos	7	6	1	86%
6	Uso de herramientas criptográficas	3	2	1	67%
7	Seguridad física y ambienta	9	8	1	89%
8	Seguridad operativa	11	9	2	82%
9	Seguridad en las comunicaciones	6	4	2	67%
10	Adquisición, desarrollo y mantenimiento de sistemas de información	8	6	2	75%
11	Relación con proveedores	5	5	0	100%
12	Gestión de incidentes de seguridad	7	4	3	57%
13	Aspectos de seguridad para la continuidad de la gestión	4	2	2	50%
14	Cumplimiento	5	2	3	40%

CRONOGRAMA DE ADECUACIONES PREVISTO Y ÁREAS INVOLUCRADAS

Se presenta a continuación el detalle de los lineamientos –organizados en función de las fechas objetivo y 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:

DSI Dirección de Sistemas Informáticos
DRRHH Dirección de Recursos Humanos
DIYSG Dirección de Infraestructura y Servicios Generales
DGAJ Dirección General de Asuntos Jurídicos
DCYC Dirección de Compras y Contrataciones
SSGA Subsecretaría de Gestión Administrativa
UM Unidad Ministro
SUST Áreas sustantivas del organismo

Objetivos de adecuación para el 2do trimestre 2022

Item	Directrices	Descripción/Justificación	Obstáculos (optativo)	ÁREAS
1.0	Política de Seguridad de la Información del organismo			
1.1	Aprobaron por las máximas autoridades del organismo o por el funcionario a quien se le ha delegado la función.	Se encuentra en trámite (EX-2021-62120670- -APN-DDYGD#MCT) la revisión y aprobación de la Política de Seguridad de la Información. Se prevé su revisión final y aprobación en el período indicado.	Restricciones para la afectación de dedicación suficiente en cada una de las áreas implicadas (Dirección de Sistemas Informáticos, Dirección de Infraestructura y Servicios Generales, Dirección de Recursos Humanos, Dirección de Compras y Contrataciones, Dirección General de Asuntos Jurídicos, Subsecretaría de Gestión Administrativa), en un contexto afectado por presencialidad parcial y la priorización forzosa de la gestión operativa de corto plazo luego del retraimiento impuesto por la pandemia COVID-19.	DSI SSGA
1.2	Notificaron y difundieron a todo el personal y a aquellos terceros involucrados cuando resulte pertinente y en los aspectos que corresponda.	Se prevé que la Política de Seguridad, una vez aprobada, sea notificada al personal y a los terceros cuando resulte pertinente y en los aspectos que corresponda.		DRRHH DCYC
1.6	Es informada a la Dirección Nacional de Ciberseguridad una vez aprobada.	Se prevé informar a la Dirección Nacional de Ciberseguridad sobre la aprobación de la Política de Seguridad y sus posteriores modificaciones.		DSI
3.0	Seguridad Informática de los Recursos Humanos			
3.2	Promueven el entrenamiento permanente de quienes desarrollan funciones en áreas de seguridad, tecnologías de la información, desarrollo de software e infraestructura.	El entrenamiento tiene lugar en el marco de proyectos y/o implementaciones específicas, o frente a cambios significativos en la infraestructura. Se prevé ampliar el entrenamiento en cuestiones de Gestión de la Seguridad de la Información, con una actualización recurrente en base anual.	Competencia entre las dedicaciones propias de la gestión de objetivos de corto plazo y las que demanden programas de entrenamiento periódicos.	DSI

4.0	Gestión de Activos			
4.4	Efectúan 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.	La destrucción segura de este tipo de medios de almacenamiento de datos tiene lugar como parte de la disposición de equipamiento defectuoso y de rezago. No obstante, esa tarea no responde a un procedimiento documentado.		DSI
5.0	Autenticación, Autorización y Control de Accesos			
5.3	Realizan un seguimiento detallado sobre las cuentas con privilegios especiales.	Las cuentas con privilegios especiales -asociadas al otorgamiento de credenciales de usuario y a la provisión de perfiles, así como a su revocación y modificación- no son objeto de un seguimiento diferenciado.		DSI
8.0	Seguridad operativa			
8.7	Llevan registro de todos los eventos de seguridad y lo revisan periódicamente con el fin de detectar posibles incidentes.	Los eventos de seguridad son registrados cuando tienen lugar, a efectos de darles tratamiento operativo. Son comunicados dentro del ámbito de su resolución en base a su gravedad o impacto en el funcionamiento de los sistemas. Una formalización del registro y reporte, así como de su revisión periódica podría adoptarse sobre la base de los lineamiento de la Política de Seguridad del organismo, una vez aprobada.		DSI
8.11	Registran y revisan periódicamente las actividades de los administradores y operadores.	No se encuentra en vigor un procedimiento recurrente de revisión de la actividad de los usuarios de los niveles referidos.		DSI
13.0	Aspectos de seguridad para la continuidad de la gestión			
13.2	Establecen, documentan, implementan y mantienen los procesos, procedimientos y controles tendientes al mantenimiento de un nivel de continuidad de la seguridad de la información durante situaciones adversas.	Las prácticas que integran los procedimientos, procesos y controles de la infraestructura no se encuentran enteramente documentados ni integran un conjunto de lineamientos formalmente aprobado.		DSI

13.3	Verifican, revisan y evalúan a intervalos regulares los controles de continuidad de la seguridad de la información.	La revisión que se realiza de los controles de continuidad en la seguridad de la información no responde a una periodicidad regular, sino a la detección de condiciones que afectan su formulación vigente.		DSI DIYSG

Objetivos de adecuación para el 3er trimestre 2022

Item	Directrices	Descripción/Justificación	Obstáculos (optativo)	ÁREAS
2.0	Aspectos Organizativos de la Seguridad			
2.6	Incluyen 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.	La inclusión dentro de los instrumentos referidos de cláusulas vinculadas al incumplimiento de la Política de Seguridad será aplicable una vez que la Política de Seguridad se encuentre aprobada.		DRRHH
3.0	Seguridad Informática de los Recursos Humanos			
3.1	Realizan e implementan 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.	Existe una comunicación frecuente de pautas y lineamientos de uso seguro de los recursos, así como indicaciones para la prevención frente a 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 SSGA
3.3	Establecen 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.	Este tipo de compromisos están presentes, en general. Sin embargo, el establecimiento de su obligatoriedad podrá tener lugar sobre la base de la aprobación de la Política de Seguridad del organismo.		SSGA DRRHH DGAJ

3.5	Incluyen los aspectos de seguridad en las etapas de inducción de los agentes, y evaluarlos durante toda la relación laboral.	La inducción de los agentes contempla, a través de diversos recursos, la comunicación de lineamientos asociados a la Seguridad de la Información y las obligaciones que se asume en relación con ellos. No se realiza una evaluación regular específica al respecto a lo largo de la relación laboral. Se prevé trabajar con la Coordinación de Capacitación y Desarrollo de Carrera de la Dirección de Recursos Humanos en este sentido, sobre la base de la aprobación de la Política de Seguridad del organismo.		DRRHH
4.0	Gestión de Activos			
4.1	Clasifican los activos de información, en línea con el tipo y la importancia de la información que gestionan para el organismo.	Existe una clasificación asistemática de los activos de información en el marco de los procesos en los que éstos son producidos o incorporados, con el propósito de darles un tratamiento acorde con su tipo e importancia. Una sistematización de esos mecanismos de clasificación podrá abordarse como parte de dispositivos asociados a la adopción plena de los lineamientos de la Política de Seguridad del organismo una vez aprobada.	Necesidad de instrumentar el entrenamiento en prácticas consistentes y homogéneas de clasificación de los activos, y de diseñar prácticas compatibles con la dedicación disponible en el marco de las diferentes iniciativas sustantivas.	DSI SUST
9.0	Seguridad en las comunicaciones			
9.2	Protegen 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.	La transferencia de información dentro de la infraestructura del organismo se encuentra protegida por diferentes medidas de seguridad. Existen prácticas para promover la preservación de la seguridad en información que es transferida fuera del organismo, si bien estas no responden a lineamientos homogéneos o de aplicación exigida.	Identificación de opciones técnicas convenientes para una instrumentación efectiva de controlable.	DSI

9.5	Incorporan acuerdos y cláusulas de confidencialidad y no divulgación según las necesidades del organismo en todos los acuerdos que se suscriban.	No se dispone de una identificación precisa de todos los acuerdos y ámbitos operativos en los que esas cláusulas serían aplicables. Una revisión de ese universo por los funcionarios competentes podría verificar el grado de cumplimiento de este lineamiento.		SSGA DGAJ
10.0	Adquisición, desarrollo y mantenimiento de sistemas de información			
10.2	Utilizan una metodología de desarrollo seguro, capacitando a los desarrolladores e incorporando cláusulas en las especificaciones técnicas de los pliegos de bases y condiciones particulares.	Se emplean metodologías de desarrollo seguro y se incluyen cláusulas específicas al respecto en los términos de referencia de las contrataciones. Se prevé un incremento de las instancias de capacitación específica en estos aspectos en el futuro.	Competencia entre las dedicaciones propias de la gestión de objetivos de corto plazo y las que demanden programas de entrenamiento periódicos.	DSI DRRHH
12.0	Gestión de incidentes de seguridad			
12.2	Cuentan con procedimientos de gestión de incidentes de seguridad documentados, aprobados y adecuadamente comunicados, de acuerdo a las áreas funcionales que considere necesarias.	Las prácticas para la gestión de incidentes no se encuentran formalizadas en procedimientos documentados y aprobados.		DSI
12.4	Instruyen a los agentes para la prevención, detección y reporte de incidentes de seguridad, según las responsabilidades correspondientes.	El reporte de incidentes de seguridad por los agentes ajenos a la gestión de los sistemas informáticos tiene lugar en base a la disposición general del personal. No existe una instrucción expresa que incluya lineamientos para la formlación y encaminamiento del reporte, salvo en contextos de amenazas flagrantes, claramente caracterizadas.		DSI DRRHH
12.5	Notifican 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.	No se encuentran en vigor prácticas que vehiculicen este reporte oportuno a la Dirección Nacional de Ciberseguridad.		DSI

Objetivos de adecuación para el 4to trimestre 2022

Item	Directrices	Descripción/Justificación	Obstáculos (optativo)	ÁREAS
1.0	Política de Seguridad de la Información del organismo			
1.3	La cumplen por todos los agentes y funcionarios del organismo.	Se prevén controles para un seguimiento sobre el cumplimiento progresivo de la Política de Seguridad por parte del personal y los funcionarios.		DRRHH DSI SSGA
1.4	Revisan y eventualmente actualizan, con una periodicidad no superior a DOCE (12) meses.	Se prevén controles para la revisión y actualización anual de la Política de Seguridad.		DSI DRRHH DIYSG DCYC DGAJ SSGA
1.5	Es 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.	Una vez aprobada, se prevé promover la consideración de la Política de Seguridad en la elaboración de las normas, procedimientos, lineamientos y guías vinculadas a los procesos del organismo.		DSI DRRHH DIYSG DCYC DGAJ SSGA
2.0	Aspectos Organizativos de la Seguridad			
2.2	Segregan las funciones y áreas de responsabilidad en conflicto para incrementarlos 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.	La segregación de las funciones de Seguridad de la Información de las correspondientes a la gestión de las Tecnologías de la Información y las Comunicaciones en el organismo será puesta a consideración de las autoridades competentes.	Restricciones para la habilitación de cargos para una gestión segregada en una unidad operativa diferente de la Dirección de Sistemas pero con las competencias técnicas requeridas.	SSGA UM

2.4	Abordan 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.	Los aspectos referidos a la Seguridad de la Información son considerados en la gestión y diseño de proyectos. Se prevé una formalización de esa consideración -con la generación de evidencia expresa- a partir la aprobación de la Política de Seguridad, y su difusión a los funcionarios involucrados en la gestión y diseño de proyectos.		UM SSGA SUST
2.5	Establecen 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 delas acciones legales que pudieran corresponder.	El establecimiento como falta del incumplimiento de la Política de Seguridad en los términos señalados solo será factible una vez que la Política se encuentre aprobada, haya sido comunicada y atendiendo los lineamientos que se adopten para su adopción progresiva.		SSGA DRRHH
3.0	Seguridad Informática de los Recursos Humanos			
3.7	Incorporan dentro de los procesos disciplinarios cualquier violación a las políticas de seguridad del organismo.	La incorporación de estas violaciones dentro de los procesos disciplinarios solo podrá ser aboradada progresivamente y luego de la aprobación de la Política de Seguridad y de su comunicación efectiva.	Requerimientos para que los procesos disciplinarios puedan apoyarse en información objetiva relativa a violaciones de este tipo, en el contexto de una adopción progresiva de los lineamientos de seguridad, dentro del marco temporal comprometido.	DRRHH
6.0	Uso de herramientas criptográficas			
6.1	Requieren 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.	La adopción de mecanismos de cifrado de dispositivos y la exigencia de su uso para las situaciones indicadas requiere de una identificación precisa de esas situaciones, del análisis del impacto operativo y de la consideración de opciones convenientes.	Falta de visibilidad de situaciones que derivan en el traslado fuera de la sede de información prevista para un uso interno. Debe considerarse el traslado de responsabilidad hacia el funcionario que solicita/autoriza la salida de dispositivos y el agente que la opera.	DSI SSGA SUST
7.0	Seguridad física y ambienta			

7.9	Tienen 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	La adopción de medidas de seguridad para los activos trasladados fuera del organismo requiere de una identificación precisa de las situaciones que lo ameritan, del impacto operativo y de las opciones técnicas convenientes.	Falta de visibilidad de situaciones que derivan en el traslado fuera de la sede de información prevista para un uso interno. Debe considerarse el traslado de responsabilidad hacia el funcionario que solicita/autoriza la salida de dispositivos y el agente que la opera.	DSI SSGA SUST
14.0	Cumplimiento			
14.1	Identifican, documentan y actualizan periódica de los requisitos legales y contractuales para cada sistema de información que utilice.	No existen en vigor prácticas orientadas a una revisión periódica de esos aspectos.		DSI
14.3	Revisan periódica de los sistemas de información para verificar el cumplimiento de las políticas y normas de seguridad de la información del organismo.	No existen en vigor prácticas orientadas a una revisión periódica de esos aspectos, complementarias de las prácticas mencionadas en los lineamientos vinculados a la adquisición y/o desarrollo de los sistemas.		DSI
14.4	Supervisan el 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 se encuentran en vigencia dispositivos orientados a este tipo de supervisión, los que deberían basarse en los lineamientos de la Política de Seguridad, una vez aprobada y comunicada.		SSGA SUST

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

Hoja Adicional de Firmas
Informe gráfico

Número: IF-2021-124886472-APN-DSI#MCT

CIUDAD DE BUENOS AIRES
Jueves 23 de Diciembre de 2021

Referencia: Plan de Seguridad (MINCYT) - DA 641/2021

El documento fue importado por el sistema GEDO con un total de 11 pagina/s.

Digitally signed by Gestion Documental Electronica
Date: 2021.12.23 14:20:10 -03:00

Andrés José D'Alessio
Director
Dirección de Sistemas Informáticos
Ministerio de Ciencia, Tecnología e Innovación

Digitally signed by Gestion Documental Electronica
Date: 2021.12.23 14:20:11 -03:00