

GACETA OFICIAL



DE LA REPÚBLICA DE CUBA

MINISTERIO DE JUSTICIA

EDICIÓN ORDINARIA LA HABANA, VIERNES 13 DE SEPTIEMBRE DE 2024 AÑO CXXII

Sitio Web: <http://www.gacetaoficial.gob.cu/>—Calle Zanja No. 352 esquina a Escobar, Centro Habana

Teléfonos: 7878-4435 y 7870-0576

Número 88

Página 1457

SUMARIO

CONSEJO DE ESTADO.....	1457
Decreto-Ley 78/2023 “Sobre la seguridad y protección de la información clasificada y limitada” (GOC-2024-525-O88)	1457
CONSEJO DE MINISTROS.....	1466
Decreto 104/2024 “Reglamento de la seguridad y protección de la información clasificada y limitada” (GOC-2024-526-O88).....	1466

CONSEJO DE ESTADO

GOC-2024-525-O88

JUAN ESTEBAN LAZO HERNÁNDEZ, Presidente de la Asamblea Nacional del Poder Popular.

HAGO SABER: Que el Consejo de Estado ha acordado lo siguiente:

POR CUANTO: La información es un activo importante para la gestión del Estado y del Gobierno que, en el contexto de ajustes del modelo económico y social del país, requiere una actualización de las medidas encaminadas a lograr mejor eficiencia en su seguridad y protección.

POR CUANTO: El desarrollo de las tecnologías de la información y las tecnologías operacionales, así como el proceso de transformación digital de la sociedad cubana, exigen el empleo de medidas de seguridad para almacenar, procesar y transmitir información y datos, cuyo diseño y aplicación requieren disponer de un sistema con una alta especialización y coordinación estatal.

POR CUANTO: La Constitución de la República de Cuba consigna el derecho de todas las personas a la transparencia y acceso a la información que se genere en los órganos, organismos y entidades del Estado, a la vez que establece los límites de este y de cualquier otro, a partir de los derechos de los demás, la seguridad colectiva, el bienestar general, el respeto al orden público, a la Constitución y las leyes.

POR CUANTO: Las experiencias en la aplicación del Decreto-Ley 199 “Sobre la Seguridad y Protección de la Información Oficial”, de 25 de noviembre de 1999, de la Resolución 1 del ministro del Interior que pone en vigor el “Reglamento de Seguridad y Protección de la Información Oficial”, de 26 de diciembre de 2000, así como de otras disposiciones complementarias en esta materia; unido a las nuevas condiciones que tienen lugar en el país y a la práctica internacional en cuestiones de seguridad y protección de la información, demuestran la necesidad de actualizar la referida legislación.

POR TANTO: El Consejo de Estado, en uso de las atribuciones que le están conferidas en el Artículo 122, inciso c), de la Constitución de la República de Cuba, acuerda dictar el siguiente:

DECRETO-LEY 78
SOBRE LA SEGURIDAD Y PROTECCIÓN DE LA INFORMACIÓN
CLASIFICADA Y LIMITADA

CAPÍTULO I
DISPOSICIONES GENERALES

Artículo 1. El presente Decreto-Ley tiene como objetivo establecer las reglas para garantizar la seguridad y protección de aquella información y datos en cualquier soporte, que reflejen la actividad del Estado o información emitida por otra persona jurídica o natural, siempre que sea reconocida legalmente por el Estado cubano, cuando su divulgación o conocimiento no autorizado, alteración o no disponibilidad, le represente un riesgo, amenaza o daño.

Artículo 2. La seguridad y protección de la información a la que se refiere el artículo anterior, se concibe como el conjunto de estructuras organizativas, procesos, funciones y regulaciones legales, que de manera coordinada desarrollan acciones dirigidas a detectar, impedir y erradicar las vulnerabilidades y condiciones que puedan favorecer las acciones nocivas para su obtención, sustracción, distorsión o no disponibilidad.

Artículo 3. Lo establecido en el presente Decreto-Ley es de aplicación a los órganos, organismos y entidades del Estado, sistema empresarial, organizaciones políticas, sociales y de masas, representaciones cubanas en el exterior, en lo adelante sujetos, así como a cualquier otra persona natural o jurídica que almacene, procese o transmita información a la que se refiere el Artículo 1.

Artículo 4. A los fines de establecer las medidas para la seguridad y protección, la información a la que se refiere el Artículo 1 se divide en información clasificada y en información limitada.

CAPÍTULO II
DE LA INFORMACIÓN CLASIFICADA Y LA LIMITADA

SECCIÓN PRIMERA

Generalidades

Artículo 5.1. La información clasificada y la limitada, independientemente del soporte que la contenga, se señala con la categoría que le corresponda, según lo establecido.

2. De igual forma, se señalizan los soportes que las contienen, en correspondencia con la máxima clasificación de la información que almacenen.

Artículo 6.1. Toda persona con acceso a información clasificada y limitada mantiene la debida compartimentación y se responsabiliza con protegerla y no divulgarla sin la autorización correspondiente.

2. No cumplir lo establecido, puede ser objeto de sanción en el orden administrativo o penal, según sea el caso.

Artículo 7. La información clasificada y la limitada no puede ser modificada, alterada o destruida sin la debida autorización y el control requerido.

SECCIÓN SEGUNDA

Información clasificada

Artículo 8. La información clasificada tiene las categorías de Secreto de Estado, Secreto y Confidencial.

Artículo 9. La categoría Secreto de Estado es aquella cuyo conocimiento o divulgación no autorizada, o su alteración o falta de disponibilidad puede poner en peligro la defensa y seguridad nacionales, la integridad o estabilidad del Estado cubano.

Artículo 10. La categoría Secreto es aquella cuyo conocimiento o divulgación no autorizada, o su alteración o falta de disponibilidad puede causar o cause daños o perjuicios en las esferas política, militar, económica, científica, técnica, cultural, social o cualquier otra de importancia para el funcionamiento del Estado o el Gobierno.

Artículo 11. La categoría Confidencial es aquella cuyo conocimiento o divulgación no autorizada, o su alteración o falta de disponibilidad puede causar o cause daños o perjuicios a la producción, los bienes, los servicios, los aseguramientos para la defensa y en general a la gestión de cualquiera de ellos.

Artículo 12. El tratamiento de la información clasificada mediante tecnologías de información en las representaciones y delegaciones estatales cubanas fuera del territorio nacional y en sistemas de trabajo y actividades clasificados dentro y fuera del territorio nacional, se rigen por medidas especiales de seguridad y protección de las tecnologías de la información y de las tecnologías operacionales que procesan datos, establecidas y controladas por el Ministerio del Interior.

Artículo 13. El Primer Secretario del Partido Comunista de Cuba, el Presidente de la República, el Presidente de la Asamblea Nacional del Poder Popular, el Primer Ministro, el Presidente del Tribunal Supremo Popular, el Fiscal General de la República, el Contralor General de la República, el Presidente del Consejo Electoral Nacional, y los ministros, están facultados para acceder a información clasificada de cualquier categoría.

Artículo 14.1. Los cargos no comprendidos en el artículo anterior requieren autorización para el acceso a la información clasificada, según la categoría de esta, atendiendo a las siguientes facultades:

- a) Para acceder a información categoría Secreto de Estado: por el Primer Secretario del Partido Comunista de Cuba, Presidente de la República, Presidente de la Asamblea Nacional del Poder Popular y Primer Ministro.
- b) Para acceder a información categoría Secreto: por cualquiera de los mencionados en el Artículo 13, así como los titulares de las organizaciones políticas y de masas, o por delegación de estos a los vicetitulares.
- c) Para acceder a información categoría Confidencial: además de los facultados en el inciso b), los vicetitulares o por delegación de estos a directivos intermedios o ejecutivos.

2. El acceso de los extranjeros a información clasificada, a solicitud de los sujetos referidos en el Artículo 3 se determina, en correspondencia con la categoría de la información, por los mismos niveles que el numeral anterior.

SECCIÓN TERCERA

Información limitada

Artículo 15. La información limitada es aquella que, sin poder ser conceptuada como clasificada, por su importancia o carácter sensible para los sujetos referidos en el Artículo 3 o las personas, no resulta conveniente su difusión pública, su alteración o falta de disponibilidad, y requiere medidas de protección en cuanto a la elaboración, certificación, conservación, desclasificación y destrucción.

Artículo 16. La información limitada se actualiza anualmente por los jefes a cada nivel y se señala con el término limitada.

CAPÍTULO III

DE LA CLASIFICACIÓN Y DESCLASIFICACIÓN**DE LA INFORMACIÓN**

SECCIÓN PRIMERA

Del ciclo de vida de la información clasificada y la limitada

Artículo 17. El ciclo de vida de la información clasificada y la limitada comprende la clasificación, elaboración, registro y control, reproducción, transmisión, archivo y conservación, desclasificación y destrucción.

Artículo 18.1. La clasificación es la identificación de la categoría de la información, en correspondencia con la lista interna de los órganos, organismos, entidades del Estado, sistema empresarial, organizaciones políticas, sociales y de masas.

2. El responsable de clasificar la información es quien la elabora o genera.

Artículo 19. La información clasificada y la limitada, y los soportes que la contienen, una vez determinada su categoría, se registran para su control, reproducción, tramitación o destrucción, en los libros de registros establecidos por el Ministerio del Interior.

Artículo 20. La información clasificada y la limitada se elabora, certifica y conserva cumpliendo medidas de seguridad que aseguren su confidencialidad, integridad y disponibilidad en cualquier soporte.

Artículo 21. La desclasificación de la información procede en los casos de:

- a) La información clasificada, al cumplirse el período de vigencia aprobado en las listas general e interna para la clasificación y desclasificación de la información, a propuesta de los jefes de los sujetos establecidos en el Artículo 3 del presente Decreto -Ley, o cuando por acuerdo del Consejo de Ministros se apruebe la desclasificación excepcional de la información clasificada en la lista general que aún no vence su periodo de vigencia;
- b) la información limitada, cuando deja de ser sensible para quien la generó o las personas y puede ser difundida públicamente por los jefes que corresponda a cada nivel.

Artículo 22.1. La destrucción total de la información clasificada y la limitada se aprueba por quien la genera, y procede cuando no posea valor patrimonial.

2. Los destinatarios de la información clasificada y la limitada pueden destruir las copias, cuando pierdan valor de uso.

SECCIÓN SEGUNDA

**Comisión Estatal para la Clasificación y Desclasificación
de la Información Clasificada**

Artículo 23. La Comisión Estatal para la Clasificación y Desclasificación de la Información Clasificada, en lo adelante la Comisión, es la encargada de dirigir, ejecutar y

controlar el proceso de clasificación y desclasificación de la información clasificada del Estado cubano, y de elaborar la lista general para la clasificación y desclasificación de la información que somete a la aprobación del Consejo de Ministros.-

Artículo 24. La Comisión está presidida por el Ministerio del Interior e integrada por representantes permanentes de los órganos y organismos del Estado que ocupen cargo de viceministro u otro equivalente, designados por cada titular.

Artículo 25. Son invitados permanentemente a las sesiones de la Comisión, representantes de las organizaciones políticas y de masas, así como otros sujetos que la Comisión determine.

Artículo 26. El funcionamiento, atribuciones y funciones de la Comisión se establecen en el Reglamento del presente Decreto-Ley.

SECCIÓN TERCERA

Lista general para la clasificación y desclasificación de la información

Artículo 27. La lista general para la clasificación y desclasificación de la información, en lo adelante, la lista general, es el documento oficial donde se define el conjunto de asuntos considerados clasificados en la República de Cuba.

Artículo 28. A la lista general solo tienen acceso los representantes e invitados de la comisión, sus jefes y el personal autorizado por estos que por sus funciones así lo requieran.

Artículo 29. Toda propuesta de clasificación, modificación o desclasificación que requiera efectuarse a la lista general, debe presentarse por los jefes de los órganos y organismos del Estado a la Comisión, que previo acuerdo, la eleva al Consejo de Ministros para su aprobación.

SECCIÓN CUARTA

De la lista interna para la clasificación y desclasificación de la información y la lista de información limitada

Artículo 30. La lista interna para la clasificación y desclasificación de la información, en lo adelante la lista interna, es el documento oficial contentivo de las informaciones que se generan por los sujetos referidos en el Artículo 3, que se correspondan con los asuntos definidos en la lista general, adecuados a la misión y funciones específicas de cada uno de ellos.

Artículo 31.1. Los jefes de los órganos, organismos y entidades del Estado, sistema empresarial y organizaciones políticas, sociales y de masas aprueban mediante Resolución, su lista interna, previo dictamen del Ministerio del Interior.

2. La lista interna tiene un alcance ramal, y en su elaboración participa todo el personal que apruebe el jefe.

Artículo 32. A la lista interna tienen acceso los jefes y el personal autorizado por estos, que, en atención a las funciones que realizan, deben utilizar esa información.

Artículo 33. Toda modificación que se requiera efectuar a la lista interna, cuando afecte la lista general, se somete a consulta de la Comisión, que, de estar de acuerdo, la eleva al Consejo de Ministros para su aprobación.

Artículo 34.1. La lista de información limitada es el documento que contiene las informaciones que se generan por los sujetos referidos en el Artículo 3 y es resultante del proceso de conformación de la lista interna, adecuada a la misión y funciones específicas de cada uno de ellos.

2. A la lista de información limitada tienen acceso los jefes y el personal autorizado por estos, en correspondencia a las funciones que realizan.

3. Las modificaciones a la lista de información limitada, se realizan conforme al plazo previsto en el Artículo 16 del presente Decreto-Ley.

CAPÍTULO IV

SOBRE LA CATEGORIZACIÓN DE LOS SUJETOS, SUS SISTEMAS DE TRABAJO Y ACTIVIDADES, Y LOS CORRESPONDIENTES ESQUEMAS DE SEGURIDAD

Artículo 35.1. Las sujetos referidos en el Artículo 3, sus sistemas de trabajo y actividades, se categorizan en correspondencia con la información clasificada que generen, en tres niveles: máxima seguridad, seguridad media y seguridad básica.

2. La propuesta de categorización se presenta a la aprobación del Ministerio del Interior por los jefes de los sujetos descritos en el Artículo 3 y debe modificarse cuando se transformen los elementos que fundamentaron la propuesta inicial.

Artículo 36. Se consideran de máxima seguridad los sujetos referidos en el Artículo 3, sus sistemas de trabajo y actividades, en los que prevalecen informaciones relacionadas con objetivos estratégicos de la defensa y seguridad nacionales, políticos, económicos, científico-técnicos, culturales y sociales, cuya divulgación o conocimiento no autorizado, su alteración o no disponibilidad, pueda causar o cause daños o perjuicios al Estado cubano.

Artículo 37. Se consideran de seguridad media los sujetos referidos en el Artículo 3, sus sistemas de trabajo y actividades, en los que prevalecen informaciones relacionadas con objetivos de la producción, los bienes y los servicios cuya divulgación o conocimiento no autorizado o su alteración o no disponibilidad pueda causar o cause daños o sea perjudicial.

Artículo 38. Se consideran de seguridad básica los sujetos referidos en el Artículo 3, sus sistemas de trabajo y actividades, en los que para el cumplimiento de su misión y funciones requieren de medidas de seguridad mínimas o elementales.

Artículo 39.1. A cada nivel de categorización le corresponde un esquema de seguridad genérico, entendido como el conjunto de medidas organizativas y técnicas que diseña el Ministerio del Interior para la gestión de riesgos, evaluación de amenazas, análisis de vulnerabilidades, supervisión proactiva y gestión de incidentes relativos a la seguridad y protección de la información clasificada y la limitada de las los sujetos referidos en el Artículo 3.

2. El esquema de seguridad se personaliza en correspondencia con la categorización aprobada para cada sujeto, sus sistemas de trabajo y actividades.

3. En el caso de la categoría de máxima seguridad, el Ministerio del Interior participa en la personalización del correspondiente esquema de seguridad genérico, y para emplear servicios de terceros se requiere aprobación de la autoridad competente.

CAPÍTULO V

DE LOS IMPLICADOS EN LA SEGURIDAD Y PROTECCIÓN DE LA INFORMACIÓN CLASIFICADA Y LIMITADA

SECCIÓN PRIMERA

De las responsabilidades de los jefes

Artículo 40. Los jefes de los sujetos referidos en el Artículo 3 para asegurar, controlar y exigir el cumplimiento de lo establecido en cuanto a la seguridad y protección de la información clasificada y la limitada, están en la obligación de:

- a) Conocer y hacer cumplir las disposiciones establecidas en este Decreto-Ley, su Reglamento y demás disposiciones complementarias;

- b) educar, preparar y concientizar al personal subordinado en mantener la debida discreción y compartimentación en cuanto a la información clasificada o limitada que conozca en razón de su cargo, así como en cumplir las medidas que se establecen en materia de seguridad y protección de esta información;
- c) ejercer especial control sobre el uso de las tecnologías de la información, sus soportes u otro material de trabajo fuera de los locales autorizados, cuando contengan información clasificada o limitada;
- d) garantizar el proceso de habilitación y preparación del personal vinculado a la seguridad y protección de la información clasificada y la limitada; y
- e) garantizar que, ante la ocurrencia de infracciones de la seguridad y protección de la información clasificada y la limitada, se proceda a su investigación con vistas a la exigencia de la responsabilidad administrativa o penal según sea el caso, a los responsables directos y colaterales.

Artículo 41. Además de las descritas en el artículo anterior, los jefes de órganos, organismos y entidades del Estado, sistema empresarial y de las organizaciones políticas, sociales y de masas, están en la obligación de:

- a) Proponer al Ministerio del Interior su categorización y la de sus sistemas de trabajo y actividades, e implementar lo establecido en correspondencia con la categoría aprobada;
- b) personalizar el esquema de seguridad, y en los casos de que estén categorizados de máxima seguridad, presentarlo a la aprobación del Ministerio del Interior;
- c) determinar, como parte de su esquema de seguridad, la información que debe transmitirse con protección criptográfica, y decidir cuándo, por los riesgos que su conocimiento pueda producir, deba ser tratada en contactos personales exclusivamente o con la utilización de los correos diplomáticos cuando sea trasladada hacia o desde el exterior del país;
- d) aprobar su lista interna, previo dictamen del Ministerio del Interior;
- e) definir, actualizar y aprobar la lista de información limitada que se genera en su ámbito de competencia;
- f) aprobar el plan de evacuación para la conservación y destrucción de la información clasificada y la limitada ante situaciones excepcionales y de desastres, previo dictamen del Ministerio del Interior;
- g) aprobar, previa consulta con el Ministerio del Interior, la creación de Oficinas de Procesamiento y Control de la Información Clasificada, en lo adelante OPCIC, o Norma de Control, según corresponda;
- h) incluir, en los planes económicos anuales y perspectivas, los recursos financieros y materiales necesarios para la adquisición, instalación y mantenimiento de las medidas, medios técnicos y físicos requeridos para la seguridad y protección de la información clasificada y limitada, y garantizar su ejecución en el período establecido;
- i) informar al Ministerio del Interior los resultados de las investigaciones realizadas ante la ocurrencia de infracciones de la seguridad y protección de la información clasificada y limitada en su órgano, organismo o entidad del Estado, sistema empresarial, organización política, social o de masas, así como los responsables directos y colaterales y las medidas a ellos aplicadas; y

- j) autorizar dar a conocer información clasificada generada en su órgano, organismo o entidad del Estado, sistema empresarial, organización política, social o de masas, procediendo de acuerdo con la categoría de clasificación que posea esta.

Artículo 42. La facultad para autorizar a los portadores de información clasificada a viajar al exterior, es del nivel que autoriza su acceso a la información clasificada, conforme a lo previsto en los artículos 13 y 14.1 de este Decreto-Ley.

Artículo 43. Los sujetos referidos en el Artículo 3 brindan al Ministerio del Interior la información que este solicite en materia de seguridad y protección de la información clasificada y la limitada, en la forma y plazos que se establezcan en las disposiciones complementarias del presente Decreto-Ley.

SECCIÓN SEGUNDA

Del personal de seguridad y protección de la información clasificada y la limitada

Artículo 44. El personal de seguridad y protección de la información clasificada y la limitada, es el vinculado directamente a la seguridad y protección de la información en los sujetos referidos en el Artículo 3, y se integra por:

- a) Jefes, especialistas o técnicos de OPCIC o Norma de Control;
- b) especialista de seguridad y protección o persona designada para realizar las funciones de asesorar, dirigir y controlar lo establecido en este Decreto-Ley, su Reglamento y demás disposiciones complementarias;
- c) personal vinculado a los sistemas de protección criptográfica;
- d) administradores de red y responsables de ciberseguridad, en los sujetos categorizados de máxima y media seguridad; y
- e) personal vinculado con la protección de los datos de las tecnologías operacionales.

Artículo 45. El personal de seguridad y protección de la información clasificada y la limitada cumple las funciones siguientes:

- a) Responde por la dirección, ejecución y control de la seguridad y protección de la información clasificada y la limitada; y
- b) supervisa y controla el cumplimiento de las medidas de seguridad, protección y compartimentación de la información clasificada y la limitada en los lugares donde se almacena, procesa y transmite información por medio de las tecnologías de la información y sus soportes.

Artículo 46.1. Para realizar las funciones enunciadas en el artículo anterior, el personal requiere habilitación.

2. Corresponde al Ministerio del Interior la habilitación del personal de la seguridad y protección de la información de los sujetos categorizados como máxima seguridad.

3. Para las categorías de media y básica seguridad, el personal se habilita por los sujetos cumpliendo lo establecido por el Ministerio del Interior.

SECCIÓN TERCERA

De la autoridad competente

Artículo 47. El Ministerio del Interior es el organismo encargado de proponer y, una vez aprobada, dirigir, ejecutar y controlar la política del Estado en cuanto a la seguridad y protección de la información clasificada y la limitada.

Artículo 48. Para el cumplimiento de la misión asignada en el artículo anterior, el Ministerio del Interior tiene las funciones siguientes:

- a) Dictar normas y procedimientos en materia de seguridad y protección de la información clasificada y la limitada;

- b) aprobar la categorización de los sistemas de trabajo y actividades de los sujetos referidos en el Artículo 3;
- c) diseñar el esquema genérico de seguridad que se emplea por los sujetos referidos en el Artículo 3 donde se almacena, procesa y transmite información clasificada y limitada por medio de las tecnologías de la información;
- d) aprobar los esquemas de seguridad vinculadas a la protección de la información clasificada y limitada, en los sujetos referidos en el Artículo 3, sus sistemas de trabajo y actividades categorizados de máxima seguridad;
- e) establecer los requisitos para elaborar el plan de evacuación para la conservación y destrucción de la información clasificada y la limitada ante situaciones excepcionales y de desastres;
- f) realizar inspecciones, diagnósticos, controles y recontroles de la seguridad y protección de la información clasificada y limitada, así como autorizar a un tercero a realizarlas en ámbitos específicos;
- g) promover la formación de personal calificado y el desarrollo de la ciencia y la tecnología en materia de seguridad y protección de la información clasificada y limitada, incluyendo la ciberseguridad asociada a la protección de información clasificada;
- h) realizar las acciones necesarias para cumplir y hacer cumplir los objetivos y funciones determinados en el presente Decreto-Ley;
- i) proponer al Consejo de Ministros las conductas que constituyen infracciones graves en materia de seguridad y protección de la información clasificada y la limitada;
- j) determinar, a través de las acciones de control, las infracciones de la seguridad y protección de la información clasificada y limitada y sus responsables directos y colaterales; solicitando la aplicación de medidas administrativas o penales según sea el caso;
- k) dictaminar los planes de evacuación para la conservación y destrucción de la información clasificada y la limitada ante situaciones excepcionales y de desastres y listas internas de los objetivos categorizados de máxima seguridad;
- l) dictaminar las informaciones y las violaciones de la seguridad y protección de la información clasificada y limitada, asociadas a posibles delitos;
- m) establecer los requisitos para la habilitación del personal que responde por la seguridad y protección de la información clasificada y limitada; y habilitar los vinculados a los sujetos, sus sistemas de trabajo y actividades categorizados de máxima seguridad; y
- n) controlar el cumplimiento del esquema de seguridad donde se almacena, procesa o transmite información clasificada y limitada.

DISPOSICIÓN TRANSITORIA

ÚNICA: El proceso de categorización de los sujetos referidos en el Artículo 3, sus sistemas de trabajo y actividades; y de personalización de esquemas de seguridad se desarrolla en un plazo de hasta un año posterior a la publicación del presente Decreto-Ley en la Gaceta Oficial de la República.

DISPOSICIONES FINALES

PRIMERA: Se faculta a los ministros de las Fuerzas Armadas Revolucionarias y del Interior, según corresponda, para adecuar en lo que resulte necesario, las disposiciones establecidas en el presente Decreto-Ley, en correspondencia con las particularidades de las funciones, misiones y características de la información clasificada y limitada de dichos organismos.

SEGUNDA: El Consejo de Ministros, a propuesta del ministro del Interior, en un plazo de hasta noventa días posteriores a la publicación del presente Decreto-Ley en la Gaceta Oficial de la República, dicta el Decreto que lo reglamenta.

TERCERA: Las infracciones de la seguridad y protección de la información clasificada y limitada, entendidas como la inobservancia de lo dispuesto en este Decreto-Ley, su Reglamento y en las normas complementarias que emitan las autoridades facultadas en esta materia, se establecen en el Reglamento de este Decreto-Ley.

CUARTA: La Comisión Estatal para la Clasificación y Desclasificación de la Información Clasificada presenta al Consejo de Ministros, en un plazo de hasta noventa días, contados a partir de la publicación del presente Decreto-Ley en la Gaceta Oficial de la República de Cuba, la propuesta de actualización de la lista general para la clasificación y desclasificación de la información clasificada.

QUINTA: Derogar el Decreto-Ley 199 “Sobre la Seguridad y Protección de la Información Oficial”, de 25 de noviembre de 1999; el Artículo 2 del Decreto 202, “Contravenciones sobre Protección Física, Secreto Estatal, Sustancias Radioactivas y otras fuentes de radiaciones ionizantes y sustancias peligrosas”, de 13 de octubre de 1995; y las demás disposiciones normativas que se contrapongan a lo establecido por el presente Decreto-Ley.

SEXTA: El presente Decreto-Ley entra en vigor a los noventa días posteriores a su publicación en la Gaceta Oficial de la República de Cuba.

PUBLÍQUESE en la Gaceta Oficial de la República de Cuba.

DADO en La Habana, a los 26 días del mes de octubre de 2023.

Juan Esteban Lazo Hernández

CONSEJO DE MINISTROS

GOC-2024-526-O88

MANUEL MARRERO CRUZ, Primer Ministro.

HAGO SABER: Que el Consejo de Ministros ha considerado lo siguiente:

POR CUANTO: El Decreto-Ley 78 “Sobre la Seguridad y Protección de la Información Clasificada y Limitada”, de 26 de octubre de 2023, en su Disposición Final Segunda dispone que el Consejo de Ministros dicta el Decreto que pone en vigor el Reglamento en esta materia.

POR CUANTO: Resulta necesaria la instrumentación y aplicación de medidas de seguridad y protección de la información clasificada y limitada, que obstaculicen e impidan el acceso a estas informaciones de personas no autorizadas, por lo que se atempera y moderniza la legislación vigente con la actual y perspectiva evolución política, socioeconómica, tecnológica del país y con la práctica internacional reconocida en esta materia.

POR TANTO: El Consejo de Ministros, en el ejercicio de las atribuciones que le están conferidas en el Artículo 137, incisos ñ) y o), de la Constitución de la República de Cuba, dicta el siguiente:

DECRETO 104
REGLAMENTO DE LA SEGURIDAD Y PROTECCIÓN
DE LA INFORMACIÓN CLASIFICADA Y LIMITADA

CAPÍTULO I

DISPOSICIONES GENERALES

Artículo 1. Este Reglamento tiene como objeto actualizar las normas conforme a lo dispuesto por el Decreto-Ley 78 “Sobre la seguridad y protección de la información clasificada y limitada”, de 26 de octubre de 2023, referente a:

- a) El ciclo de vida de la información clasificada y limitada;
- b) las reglas para el acceso a la información clasificada, incluidas las que deben cumplir los portadores;
- c) la integración, atribuciones y funciones de la comisión estatal para la clasificación y desclasificación de la información clasificada;
- d) las reglas de conformación de la lista general para la clasificación y desclasificación de la información;
- e) el trabajo con la lista interna para la clasificación y desclasificación de la información;
- f) la organización de las oficinas de procesamiento y control de la información clasificada;
- g) el proceso de habilitación del personal implicado en la seguridad y protección de la información clasificada;
- h) las acciones de control de la seguridad y protección de la información clasificada y limitada;
- i) el proceso de categorización de los sujetos, sistemas de trabajo y actividades, y de personalización de los esquemas de seguridad;
- j) las atribuciones y obligaciones vinculadas a la información clasificada y limitada; y
- k) las infracciones graves que afectan la seguridad y protección de la información clasificada, así como las medidas disciplinarias a aplicar.

Artículo 2. Los sujetos previstos en el Artículo 3 del Decreto-Ley 78 de 2023 cumplen lo establecido en el presente Reglamento.

CAPÍTULO II

DEL CICLO DE VIDA DE LA INFORMACIÓN CLASIFICADA Y LIMITADA

SECCIÓN PRIMERA

De la clasificación

Artículo 3. La clasificación es la acción de asignar a una información, en cualquier soporte, la categoría establecida en las listas interna y limitada para los sujetos, que se ejecuta por quien elabora la información, en lo adelante ejecutor.

Artículo 4. La categoría de clasificación de la información, en cualquier soporte, se señala en la parte superior derecha del documento y en cada una de las hojas que lo conforman, se consigna además, el número de ejemplar y de páginas.

Artículo 5.1. El documento clasificado o limitado destinado al conocimiento de una persona, se identifica con la letra P, que significa personal, y se coloca a continuación de la categoría de clasificación que le corresponda.

2. El destinatario del documento identificado con la letra P, es el único facultado para determinar si otra persona, por necesidades de trabajo, debe acceder a este, y tiene que cumplir con lo establecido en cuanto a los niveles de acceso y el control.

3. Cuando se cumple el apartado anterior, el destinatario elimina del documento la condicionante que lo identifica como personal.

SECCIÓN SEGUNDA

De la elaboración de la información clasificada y limitada

Artículo 6. Los documentos clasificados y sus versiones, en cualquier formato, se elaboran previo registro por el personal de la Oficina de Procesamiento y Control de la Información Clasificada, identificada por sus siglas OPCIC, o por la persona designada para atender el registro y control de la información clasificada, en lo adelante norma de control.

Artículo 7. Cuando se elabore un documento con contenidos de diferentes categorías de clasificación se asume la de mayor nivel.

Artículo 8.1. Para la elaboración de la información clasificada y limitada en tecnologías de la información, se utilizan los Servicios de Protección Criptográfica, en lo adelante SPC, aprobados a tales efectos.

2. Estas acciones se realizan en equipamientos desconectados de redes de alcance global.

SECCIÓN TERCERA

Registro, control y certificación de la información clasificada y limitada

Artículo 9. Todo documento clasificado se registra, a los efectos del control de la documentación, en el libro de registro que constituye el Anexo I de este Reglamento.

Artículo 10.1. Cuando el registro se gestiona mediante un sistema informatizado, tiene que contener los indicadores previstos en el libro de registro y cumplir con las medidas de seguridad criptográficas y de salvaguardas aprobadas, para asegurar la debida confidencialidad, autenticidad, integridad y disponibilidad de la información.

2. El sistema informatizado para el registro de la información clasificada se certifica por el Ministerio del Interior, en lo adelante MININT.

Artículo 11.1. A cada documento clasificado en cualquier soporte, se le asigna un número de registro que lo identifica durante su ciclo de vida.

2. El registro comienza con el 01 en cada año natural de forma consecutiva.

Artículo 12. El libro de registro tiene todas sus páginas foliadas y se inicia y cierra cada año natural mediante un certificado que relaciona los datos siguientes:

- a) Certificado de inicio: fecha de apertura, número del libro y el de inventario según modelo de control de materiales que constituye el Anexo II de este Reglamento, y cantidad de hojas foliadas.
- b) Certificado de cierre: fecha de cierre, número del libro y del inventario según modelo de control de materiales y último folio.

Artículo 13. En el libro de registro o sistema informatizado se consigna el lugar y soportes donde se conserva el documento clasificado.

Artículo 14.1. Ante errores durante la anotación en el libro de registro de información clasificada, se anula la línea con color rojo y se consigna en la siguiente los datos del documento.

2. En los sistemas informatizados, los errores corregidos deben poder comprobarse mediante el registro de traza del sistema, determinarse el contenido de los cambios, la fecha y hora en que ocurrieron y el ejecutor que los realizó.

Artículo 15.1. Para el registro, control y certificación de la información limitada, el jefe facultado según lo dispuesto en el Artículo 171 de este Reglamento, establece los procedimientos internos.

2. El registro de la información limitada es independiente del habilitado para la información clasificada y consigna de forma obligatoria: fecha, ejecutor, nombre del documento, cantidad de ejemplares, destinatarios, reproducciones con sus destinos, lugar de conservación, fecha en que se borra o destruye, fecha en que pierde la condición de Limitado y pase al sistema de gestión documental que implemente el sujeto.

Artículo 16. La certificación del documento clasificado se ubica al final de este y comprende los datos siguientes:

- a) Cantidad de ejemplares;
- b) cantidad de hojas;
- c) cantidad de anexos, si los tuviese;
- d) destinatario por ejemplar;
- e) ejecutor o mecanógrafo;
- f) número de información según lista interna;
- g) período de vigencia según lista interna;
- h) número de registro otorgado por la OPCIC o norma de control; y
- i) fecha de elaboración.

Artículo 17. Cuando el documento clasificado tiene hasta cinco destinatarios se consignan en la certificación, si supera esta cifra se declara en la lista de destinatarios que se anexa y se archiva en la OPCIC; además, se señala en la certificación con la sigla SLD, que significan según lista de destinatarios.

Artículo 18. A los efectos del registro de la información identificada con la letra P, se cumplen las reglas particulares siguientes:

- a) La OPCIC o Norma de Control no abre la correspondencia con esta identificación, solo consigna en el libro de registro los datos que aparecen en el embalaje y en el comprobante de entrega de documentos;
- b) en el libro de registro o sistema informatizado solo se consigna número de registro, y en el título o asunto, se escribe la categoría P; y
- c) cuando la información es en soporte papel, el destinatario está obligado a anotar en el documento el registro de entrada y la fecha que aparece reflejada en el embalaje.

Artículo 19. Como parte del control de la información clasificada, las tecnologías de la información vinculadas a su ciclo de vida tienen que estar visiblemente señalizadas y debidamente inventariadas en el modelo de control de materiales de trabajo.

SECCIÓN CUARTA

Impresión y reproducción de la información clasificada

Artículo 20.1. La impresión o reproducción de los documentos clasificados se realiza centralizadamente por la OPCIC o Norma de Control.

2. Cuando la impresión o reproducción se realice fuera de la OPCIC o Norma de Control, se garantiza el conocimiento por el jefe de esta para el registro efectivo de este proceso.

Artículo 21. La impresión o reproducción en imprenta de un documento clasificado, se autoriza por el jefe del ejecutor a través de la Orden de trabajo, que conforma el Anexo III de este Reglamento.

Artículo 22. El jefe de la OPCIC o Norma de Control, de conjunto con el de seguridad y protección del sujeto, o personas con acceso a información clasificada previamente aprobado por el jefe facultado, se responsabiliza con las medidas de seguridad de los documentos clasificados a imprimir o reproducir en el lugar donde se ejecuta este proceso; garantiza el control de desechos, materiales u otros soportes utilizados que son

posteriormente destruidos conforme a lo establecido en este Reglamento, así como el borrado seguro de los ficheros, en caso de tratarse de soportes digitales para los originales empleados.

Artículo 23. Cuando el sujeto gestiona la información clasificada mediante el sistema informatizado, la impresión se controla de forma automática.

Artículo 24.1. En el caso de los documentos clasificados recibidos, que se autorice su reproducción por el facultado, se consignan en el libro de registro la cantidad de ejemplares reproducidos.

2. Cuando la reproducción sea parcial, se consigna en el libro de registro los números de las hojas reproducidas.

SECCIÓN QUINTA

Del traslado, transmisión y recepción de la información clasificada

Artículo 25.1. Una vez registrada y certificada la documentación clasificada, su movimiento interno se controla por la OPCIC o la Norma de Control en el libro de registro como constancia de entrega de los documentos impresos o digitales a los destinatarios internos que se agrupan por áreas.

2. El modelo de entrega de correspondencia interna constituye el Anexo IV de este Reglamento, y consigna los documentos impresos o digitales que se generen o reciban en el área y señala dónde se encuentra el ejemplar digital o de archivo.

Artículo 26.1. Cuando un documento clasificado, en cualquier soporte, se remite a una entidad externa, la constancia queda en el modelo de comprobante de entrega, que constituye el Anexo V de este Reglamento.

2. Cuando la remisión se realiza por un canal digital, tiene que cumplir con los requerimientos técnicos y de seguridad criptográficos aprobados por la Dirección de Criptografía del MININT y la entrega y recepción se comprueba por los registros de traza del sistema empleado.

Artículo 27.1. El embalaje de los documentos y materiales clasificados tiene que garantizar la no visibilidad del contenido, y que el sistema de sellaje permita detectar su apertura.

2. En el embalaje se consignan los datos siguientes:

- a) Categoría de clasificación, en el extremo superior derecho;
- b) cargo, nombre y apellidos del remitente;
- c) cargo, nombre y apellido del destinatario;
- d) número de registro correspondiente a cada documento o material que se envía; y
- e) fecha de emisión.

Artículo 28. Cuando se envíen varios documentos clasificados a un destinatario, pueden colocarse en un solo embalaje, y se consigna en su parte exterior la clasificación mayor de estos y los números de registros de cada uno.

Artículo 29.1. El comprobante de entrega de documentos se confecciona por triplicado y la OPCIC o Norma de Control retiene uno firmado por el personal de correo como constancia de la entrega.

2. El personal de correo recibe dos ejemplares del comprobante, y una vez firmados en el lugar de destino, deja uno y devuelve el otro a la OPCIC o Norma de Control, en ambos casos como constancia de la entrega.

3. El personal de la OPCIC o Norma de Control destruye en presencia del personal de correo el comprobante de entrega retenido y archiva el firmado por el receptor.

Artículo 30. El personal de correo debe comprobar la integridad de los embalajes que recibe y exigir que, en el comprobante de entrega de documentos, quede legible el nombre y apellidos de quien recibe la documentación clasificada, así como su firma.

Artículo 31. Los comprobantes de entrega se folian de forma consecutiva por año natural, se inicia por el 01, y se archivan en ese orden, conservándose hasta que el documento se destruya o desclasifique.

Artículo 32.1. La documentación clasificada se transporta en valijas o maletas con cierres de seguridad y mecanismos para el sellaje.

2. La transportación se realiza en vehículos cerrados, por el personal de correo, que se compone de dos personas; durante la transportación de esta documentación solo puede viajar en los vehículos el personal de correo.

3. Cuando no exista personal de correo disponible, el jefe facultado designa quién asume esta responsabilidad, el que debe observar el cumplimiento de lo establecido para la transportación de documentos.

Artículo 33. El embalaje de documentos clasificados que transita por puntos de control o estafetas antes de llegar a la OPCIC o Norma de Control, no puede ser abierto, se registran solo los datos que aparecen en él.

Artículo 34.1. Para la recepción de los documentos clasificados en puntos de control o estafetas, OPCIC o Norma de Control, se comprueba la integridad de las medidas de seguridad de los cierres, se verifican los números de registros del embalaje con los del comprobante de entrega, se firma este, y se archiva una copia.

2. Si se detectan irregularidades, el personal de los puntos de control o estafetas, OPCIC o Norma de Control no recibe los documentos clasificados, comunica al del correo los motivos y deja constancia por escrito de las razones por las que no se reciben estos.

Artículo 35.1. Cuando en la OPCIC o Norma de Control se detecta alguna irregularidad entre los datos del embalaje y su contenido, o documentos faltantes, se informa al jefe de esta, quien se comunica con el emisor para corregir la irregularidad.

2. De no resolverse la irregularidad en diez días, el jefe de la OPCIC o Norma de Control envía nota al emisor, de la cual se conserva copia, hasta la solución.

SECCIÓN SEXTA

Del traslado y transmisión de información clasificada al extranjero o hacia nuestro país

Artículo 36. El traslado de información clasificada al extranjero, o hacia nuestro país, en cualquier soporte, se realiza a través del sistema de correo diplomático del Ministerio de Relaciones Exteriores de la República de Cuba o por la persona autorizada por el jefe correspondiente.

Artículo 37. La facultad para autorizar el traslado y transmisión de información clasificada al extranjero, se efectúa conforme a lo previsto en el Artículo 14 del Decreto-Ley 78 de 2023.

Artículo 38. La transmisión de información clasificada al extranjero o hacia nuestro país a través de las tecnologías de la información, se realiza por el Servicio Central de Cifras del MININT.

Artículo 39. Para trasladar documentos clasificados al extranjero o hacia nuestro país en cualquier soporte, se solicita autorización al jefe facultado conforme a lo dispuesto en el Artículo 41, inciso c) del Decreto-Ley 78 de 2023.

Artículo 40. La autorización del jefe facultado se consigna por escrito y relaciona la información siguiente:

- a) Título de los documentos que se solicitan trasladar;
- b) número de registro y cantidad de ejemplares;
- c) categoría de clasificación;
- d) fundamentación de la necesidad de dicho traslado;
- e) evento o reunión en que serán utilizados;
- f) tiempo de permanencia;
- g) país al que se traslada;
- h) personas que tienen acceso a los documentos;
- i) de trasladarse la información clasificada en tecnologías de la información, especificar cuál es el SPC que se emplea;
- j) consignación de la devolución de documentos y tecnologías de la información; y
- k) cualquier otro dato de interés.

Artículo 41.1. El plazo para tramitar la solicitud y aprobación del traslado de la información es de hasta quince días antes de la fecha prevista de salida.

2. La autorización firmada por el jefe facultado se archiva en la OPCIC o Norma de Control a los efectos de controlar los documentos y las tecnologías de la información que se trasladen al extranjero y su posterior devolución, lo que se consigna una vez ejecutado, en el documento de autorización, que se conserva en la OPCIC o Norma de Control.

3. Los documentos clasificados y las tecnologías de la información que se autorizan para el traslado quedan bajo la custodia de la persona autorizada, quien se responsabiliza con la seguridad de estos.

Artículo 42.1. Ante la ocurrencia de incidentes durante el traslado o estancia en el extranjero de la información clasificada, de la tecnología de la información o del medio criptográfico autorizado a trasladar información clasificada, el funcionario a cargo debe informarlo inmediatamente al jefe que autorizó.

2. El funcionario a cargo, al arribar a territorio nacional confecciona un informe sobre lo acontecido, que entrega al jefe que autorizó el traslado y al órgano competente del MININT.

SECCIÓN SÉPTIMA

Archivo y conservación de la información clasificada y limitada

Artículo 43.1. La información clasificada se archiva por asuntos en expedientes numerados, y las hojas de los documentos se folian en orden consecutivo.

2. En cualquier formato en que se archive información clasificada, se garantiza el índice de su contenido, conforme al modelo de relación interior de documentos, que constituye el Anexo VI de este Reglamento en su variante uno.

Artículo 44.1. En cada lugar donde se archive información clasificada se confecciona una guía por asuntos y su ubicación.

2. Cada mueble donde se archive documentación clasificada se identifica de acuerdo con la organización establecida en la guía de archivo.

3. En caso de que el archivo sea mediante un sistema informatizado, debe contar con módulos de archivo y su guía.

Artículo 45.1. Los materiales clasificados que no puedan ser archivados dentro del expediente tales como fotografías, maquetas, CD, cintas u otros, se archivan de acuerdo con sus características y se consigna su ubicación en el expediente.

2. Cuando estos materiales no estén vinculados con expedientes, se archivan por asuntos o temas.

Artículo 46.1. El archivo y conservación de la información limitada se realiza conforme a los procedimientos internos que establece el jefe facultado.

2. Excepcionalmente, se puede autorizar archivar y conservar información clasificada y limitada juntas o en el mismo mueble, aunque se identifican diferenciadamente.

Artículo 47.1. El préstamo de documentos clasificados en cualquier soporte o de materiales de trabajo a personas autorizadas, se efectúa mediante el modelo de control de préstamo, que constituye el Anexo VII de este Reglamento.

2. Cuando el documento está archivado en un sistema informatizado, se controla mediante el acceso creado en este.

Artículo 48. Durante el archivo de información clasificada y limitada se tiene en cuenta además, lo aprobado en el plan de evacuación para la conservación y destrucción de la información clasificada y limitada del sujeto.

Artículo 49. Para la organización del archivo y conservación de la información clasificada, el ejecutor precisa a la OPCIC o Norma de Control las fechas de desclasificación y destrucción, lo que consignan en el documento.

Artículo 50. A los archivos donde obre documentación clasificada solo tienen acceso las personas responsabilizadas con su control y los funcionarios que por sus responsabilidades lo requieran y estén autorizados por el jefe facultado.

SECCIÓN OCTAVA

De la desclasificación de la información clasificada

Artículo 51. La desclasificación es el proceso mediante el cual se suprime la categoría de clasificación por los motivos siguientes:

- a) Al desaparecer los elementos que le dieron dicha categoría;
- b) por el vencimiento del período de permanencia de clasificación que señala la lista interna para la clasificación y desclasificación de la información; y
- c) o cuando se autoriza por los jefes facultados, en el caso de que el período de permanencia de la información sea hasta que se autorice su desclasificación.

Artículo 52. La permanencia de una información con carácter clasificado se establece en fases, en años o puede no estar determinada en el tiempo, caso en que denomina: hasta que se autorice su desclasificación.

Artículo 53. La información clasificada por el período de permanencia hasta que se autorice su desclasificación, se analiza anualmente por el ejecutor o su jefe inmediato.

Artículo 54.1. La desclasificación por vencimiento del período de permanencia, se realiza en consulta con el ejecutor o su jefe inmediato.

2. De considerarse necesaria mantener la clasificación, se prorroga por un año.

Artículo 55. El jefe de OPCIC o Norma de Control realiza anualmente el análisis de todos los documentos clasificados que obran en su ámbito y cuyo período de permanencia ha vencido, a los efectos de proceder a su desclasificación, en consulta con el ejecutor.

Artículo 56. Una vez desclasificado un documento, se comunica por el jefe de OPCIC o Norma de Control, a todas las personas que fueron destinatarias de este.

Artículo 57. Para proceder a la desclasificación de la información el jefe de OPCIC o Norma de Control sigue los pasos siguientes:

- a) El libro de registro, consiga la fecha y firma del jefe facultado en la columna correspondiente; y

- b) en el documento, circula en rojo la categoría anterior y consigna la palabra Desclasificado, la fecha y su firma.

Artículo 58.1. La desclasificación de una parte del documento se aprueba, excepcionalmente, por el jefe facultado a propuesta del ejecutor.

2. La parte que mantiene la clasificación se señala, y su vigencia se prorroga por un año.

3. Este nuevo documento se registra según lo establecido.

Artículo 59. Los documentos desclasificados que mantengan valor patrimonial o de uso pasan al control de la gestión documental.

SECCIÓN NOVENA

De la destrucción de la información clasificada y limitada

Artículo 60.1. La destrucción es el proceso mediante el cual se tritura totalmente o incinera la información clasificada y limitada, mientras que se aplica herramienta de borrado seguro, certificada por el MININT en el caso de la conservada en tecnologías de la información.

2. La destrucción se ejecuta por el jefe de OPCIC o Norma de Control.

Artículo 61.1. El órgano competente del MININT distribuye controladamente el programa de borrado seguro.

2. El soporte contentivo del software de instalación del programa de borrado seguro es registrado y custodiado en la OPCIC o Norma de Control.

Artículo 62. La información clasificada que carece de valor patrimonial se destruye por las razones siguientes:

- a) Una vez conocido su contenido y no se requiera para el trabajo posterior;
- b) cuando se precise que una vez conocido debe destruirse inmediatamente;
- c) se determine la fecha en que se debe destruir en el archivo.

Artículo 63.1. La aprobación de la destrucción consta por escrito a través del modelo de acta de destrucción, que constituye el Anexo VI de este Reglamento en su variante dos.

2. Las actas de destrucción deben estar enumeradas consecutivamente en el año en curso.

Artículo 64. Los documentos clasificados se destruyen en cada lugar de conservación que consigna el libro de registro o sistema informatizado, incluida la información digital mediante la aplicación del programa de borrado seguro.

Artículo 65.1. La destrucción debe garantizar que los documentos no puedan ser reconstruidos o recuperados total o parcialmente.

2. Cuando no existan posibilidades de trituración total del documento, se procede a incinerar, previa fragmentación o trituración parcial, se colocan los restos en sacos o depósitos, sin exceder los treinta días fuera de archivo.

Artículo 66. No pueden mantenerse documentos pendientes a destruir fuera de la OPCIC o Norma de Control.

Artículo 67. El jefe facultado establece los procedimientos internos para la destrucción de la información limitada.

SECCIÓN DÉCIMA

Del tratamiento a la información Secreto de Estado

Artículo 68.1. La elaboración de la información Secreto de Estado se realiza en cabinas especiales, certificadas por el MININT, solo en presencia de las personas autorizadas para ello, en único ejemplar de forma manuscrita, que se remite al destinatario quien debe devolverlo al emisor en un plazo que no exceda los treinta días posteriores a su recibo.

2. Cuando se elabora en tecnologías de la información aprobadas para estos fines, con SPC, concluido el proceso, se imprime el único ejemplar.

3. Cuando el ejemplar es devuelto por el destinatario, se aplica en la tecnología de la información el mecanismo de borrado seguro aprobado.

Artículo 69. A los efectos del registro de la información Secreto de Estado, se cumple lo establecido en este Reglamento y las reglas particulares siguientes:

- a) La OPCIC o Norma de Control no abre la correspondencia con esta clasificación, solo consigna en el libro de registro los datos que aparecen en el embalaje y en el comprobante de entrega de documentos;
- b) en el libro de registro o sistema informatizado solo se consigna número de registro, y en el título o asunto se escribe: Secreto de Estado;
- c) el destinatario está obligado a anotar en el documento el registro de entrada y la fecha, que aparece reflejada en el embalaje; y
- d) se consigna la fecha de devolución al ejecutor, en la casilla observaciones.

Artículo 70. Los documentos Secreto de Estado no se reproducen, se accede a su contenido previa autorización del destinatario.

Artículo 71. El cierre de los embalajes contentivos de los documentos y materiales clasificados como Secreto de Estado se efectúa por el jefe de la OPCIC o Norma de Control, en presencia del que los elabora, garantizando su protección.

Artículo 72. Los documentos Secreto de Estado:

- a) No se envían con otros de diferente clasificación;
- b) su transportación se realiza con escolta armada;
- c) se archivan en cajas fuertes, sin mezclar con otro tipo de información, con medidas que garanticen la no visibilidad del contenido y la detección de violaciones del cierre;
- d) no se trasladan, ni transmiten al extranjero;
- e) nunca se digitalizan para su conservación; y
- f) su destrucción se consigna en acta independiente.

Artículo 73.1. La desclasificación de un documento Secreto de Estado, cuyo período de permanencia no ha vencido o sea hasta que se autorice su desclasificación, solo puede ejecutarse previa consulta del jefe facultado al destinatario.

2. Igual procedimiento se realiza cuando vence el período de permanencia de un Secreto de Estado y el jefe facultado considera que debe mantenerse clasificado.

CAPÍTULO III

DEL ACCESO A LA INFORMACIÓN CLASIFICADA

SECCIÓN PRIMERA

Disposiciones generales

Artículo 74. La información clasificada solamente puede ser conocida por las personas autorizadas para ello.

Artículo 75.1. Toda persona a la que se autorice el acceso a información clasificada, está obligada a firmar el modelo de nivel personal de acceso y acta de responsabilidad, que constituye el Anexo VIII de este Reglamento.

2. El modelo que acredita el acceso a la información clasificada permanece por tiempo indefinido archivado en la OPCIC o Norma de Control.

Artículo 76. Los extranjeros que se autoricen a acceder a información clasificada, conforme a lo previsto en el Artículo 14.2 del Decreto-Ley 78 de 2023, firman cláusulas

de confidencialidad con el objetivo de controlar y conocer las informaciones a las que tienen acceso, así como su compromiso de no divulgarlas.

Artículo 77. Los jefes en cualquier nivel tienen la obligación de garantizar que las cláusulas de confidencialidad especifiquen las informaciones que resulta necesario proteger, canales de comunicación y sus medidas de seguridad, así como las responsabilidades en que incurre en caso de violar dichos acuerdos, tener en cuenta los daños o perjuicios que su conocimiento o divulgación no autorizada pueda producir al Estado cubano.

Artículo 78.1. Toda persona que en función del cargo que ocupa requiera tener conocimiento de la información clasificada, asume la responsabilidad desde su nombramiento.

2. La firma del acta de responsabilidad debe ejecutarse en un plazo que no exceda los diez días posteriores al nombramiento.

Artículo 79. El jefe inmediato propone al jefe facultado para aprobar el acceso a información clasificada, el personal subordinado que requiere acceso y a qué información accede, en correspondencia con el cargo que desempeña, en un plazo de hasta treinta días posteriores al nombramiento.

Artículo 80. El acceso a información clasificada puede ser eventual, por un período determinado por funciones de trabajo, quedando constancia por escrito de la fecha en que se otorga y se suprime.

Artículo 81. En el modelo de Nivel Personal de Acceso y Acta de Responsabilidad, se consigna: se otorga acceso a toda la información clasificada, en los casos de los cargos a los que se autoriza acceder a toda la información clasificada que se elabore y reciba en el sujeto.

SECCIÓN SEGUNDA

Los portadores de información clasificada

Artículo 82. Los portadores de información clasificada, en lo adelante portadores, son aquellos que poseen aprobación para acceder a esta.

Artículo 83.1. El control de los portadores se realiza por la OPCIC o Norma de Control, hasta que mantenga vigencia la información clasificada a la cual se le otorgó acceso, aun cuando la persona no permanezca en el cargo por cualquier motivo, lo cual se consigna en las observaciones del modelo del nivel personal de acceso y acta de responsabilidad.

2. En el caso de los accesos a extranjeros, el control se realiza a partir de la cláusula de confidencialidad que constan en la OPCIC o Norma de Control del sujeto vinculante como clasificada.

Artículo 84. Los portadores se regulan migratoriamente, por el período de permanencia de la información a la que acceden, a consideración de los jefes facultados.

Artículo 85.1. Si el portador requiere cumplir misión oficial de trabajo al exterior, se analiza su salida temporal, por el órgano consultivo que corresponda a la categoría del trabajador y se aprueba por el titular del sujeto o la persona en quien se delega esta obligación.

2. Si el portador labora en entidad ajena a la que lo controla como tal, el trámite de solicitud de permiso de salida temporal por asuntos oficiales se realiza entre los jefes de ambos sujetos, previa fundamentación de la solicitud.

Artículo 86.1. Corresponde al jefe facultado establecer por resolución los procedimientos para la autorización temporal o definitiva de salida al exterior de un portador por asuntos personales.

2. La solicitud de permiso de salida temporal o definitiva por asuntos personales se realiza por el portador al jefe responsable de su regulación migratoria.

3. Durante la evaluación de la autorización temporal o definitiva de salida al exterior, prevalece la decisión colegiada del órgano establecido en la resolución que autoriza los procedimientos, expresada en el numeral 1 de este artículo; y se le comunica el resultado al solicitante.

Artículo 87.1. Ante la autorización de salida al exterior de un portador, por misión oficial o por asuntos personales, los jefes de seguridad y protección o la persona designada por el jefe facultado, garantizan instruirlo en cuanto a la confidencialidad de la información clasificada que porta, así como de la responsabilidad en que incurre en caso de violar lo establecido, proceso del que se deja constancia escrita.

2. En caso de misión oficial, además se instruye en el uso de la tecnología de la información y el SPC a emplear si la información es digital.

Artículo 88.1. Como constancia de esta instrucción se llenan los datos siguientes:

- a) Nombre y apellidos del portador que viaja;
- b) cargo que ocupa;
- c) país o países a visitar;
- d) motivo de la salida;
- e) constancia por la OPCIC sobre la entrega de documentos clasificados, tecnologías de la información y comunicaciones, SPC implementado, revisión de la información autorizada a extraer del país, sellos u otros materiales utilizados para la información clasificada;
- f) constancia por los responsables de la ciberseguridad y la criptografía, sobre las medidas tecnológicas y de seguridad criptográficas aplicadas a las tecnologías de la información y comunicaciones y el medio de protección criptográfica, respectivamente, autorizados a extraer del país;
- g) fecha de viaje, desde y hasta;
- h) firma y fecha del portador que viaja como constancia de la instrucción; y
- i) firma y fecha del jefe o persona designada que instruye.

2. Esta información se conserva en la OPCIC o Norma de Control por un período de dos años.

Artículo 89. En caso de deserción de un portador de información clasificada, el jefe de seguridad y protección informa al órgano competente del MININT nombre y apellidos, cargo, motivo de la salida, fecha de salida y país donde ocurre la deserción, informaciones clasificadas a las que tuvo acceso, valor y período de permanencia de estas, control de daños, fecha y forma en que se detectó.

Artículo 90. El portador que reciba o compre en el extranjero una tecnología de la información o soporte, antes de ser utilizado para procesar información clasificada, dentro o fuera del territorio nacional, debe informarse al jefe y al órgano competente del MININT, con el fin de tomar las medidas técnicas, de revisión y compatibilización con la defensa y seguridad nacional según corresponda, previo a su uso.

SECCIÓN TERCERA

Modificación y supresión del acceso a información clasificada

Artículo 91.1. La OPCIC o Norma de Control, a propuesta del jefe inmediato, modifica el acceso a la información clasificada cuando el portador, por cumplimiento de otras funciones, requiere nuevos accesos a esta información clasificada en el modelo de nivel personal de acceso y acta de responsabilidad.

2. En este caso se refleja la causa de modificación en las observaciones del modelo de nivel personal de acceso y acta de responsabilidad y se elabora otro, anexo al anterior, con los nuevos accesos autorizados.

Artículo 92. La OPCIC o Norma de Control, a propuesta del jefe inmediato, suprime el acceso a la información clasificada en caso de prolongada enfermedad, traslados de centro de trabajo, cambio de responsabilidad en las funciones en la que no precisa el acceso otorgado, o cuando pierda las cualidades que le hicieron acreedor de este; y se deja constancia en las observaciones del nivel personal de acceso y en el acta de responsabilidad, del motivo y la fecha.

Artículo 93. Cuando se modifique o suprima el acceso de una persona a informaciones clasificadas, se le comunica por el jefe inmediato a la OPCIC o Norma de Control, para proceder con lo dispuesto en esta sección.

Artículo 94. Cuando se suprime el acceso, el portador no puede divulgar las informaciones a las que tuvo conocimiento hasta su desclasificación.

Artículo 95. Cuando se modifique o suprima el acceso, la OPCIC o Norma de Control cambia o recoge, según corresponda, sellos, llaves, documentos y medios técnicos que contengan información clasificada que obren en poder del portador, así como modifica o invalida los privilegios para el acceso y manejo de informaciones clasificadas en las tecnologías de la información.

CAPÍTULO IV

DE LA COMISIÓN ESTATAL PARA LA CLASIFICACIÓN Y DESCLASIFICACIÓN DE LA INFORMACIÓN CLASIFICADA

SECCIÓN PRIMERA

De las funciones de la Comisión y las atribuciones y obligaciones de sus integrantes

Artículo 96. La Comisión Estatal para la Clasificación y Desclasificación de la Información Clasificada, en lo adelante la Comisión, tiene como funciones las siguientes:

- a) Elaborar y someter a la aprobación del Consejo de Ministros el proyecto de lista general para la clasificación y desclasificación de la información;
- b) analizar las propuestas que formulen los órganos y organismos del Estado sobre la clasificación y desclasificación de la información que generan, cuando tiene impacto en la lista general para la clasificación y desclasificación de la información;
- c) presentar al Consejo de Ministros para su aprobación, los acuerdos adoptados por la Comisión en relación con las propuestas de clasificación y desclasificación de las informaciones;
- d) analizar los factores coyunturales en el orden político, militar, económico, científico-técnico, cultural, social o de cualquier otro tipo a fin de atemperar el establecimiento de la política de clasificación y desclasificación de la información a situaciones existentes, de acuerdo con intereses del Estado y de la defensa del país; y
- e) conocer el estado de los procesos para la clasificación y desclasificación de la información en órganos y organismos del Estado.

Artículo 97. El presidente de la Comisión tiene las atribuciones y obligaciones siguientes:

- a) Dirigir las actividades de la Comisión y su secretariado ejecutivo;
- b) convocar y presidir las reuniones ordinarias y extraordinarias que se realicen;
- c) determinar la fecha, lugar, hora y temas a desarrollar en las reuniones u otras actividades que realiza la Comisión;

- d) aprobar la elaboración de los documentos a tratar en las reuniones;
- e) orientar los asuntos, coordinaciones y objetos de atención de la Comisión con vistas a obtener elementos, informaciones y opiniones sobre temas a evaluar;
- f) notificar a la Comisión los acuerdos adoptados por el Consejo de Ministros con relación a las propuestas de clasificación y desclasificación de la información aprobadas; y
- g) exigir el cumplimiento de los acuerdos adoptados.

Artículo 98. El vicepresidente de la Comisión tiene las atribuciones y obligaciones siguientes:

- a) Sustituir al presidente de la Comisión en su ausencia;
- b) organizar con el secretario las reuniones ordinarias y extraordinarias que se convoque; y
- c) cumplir con las tareas que la Comisión y el presidente le asignen.

Artículo 99. El secretario de la Comisión tiene las atribuciones y obligaciones siguientes:

- a) Elaborar y conservar las actas de las sesiones que celebre la Comisión;
- b) controlar los acuerdos adoptados e informarle a los miembros que no hubieran concurrido a la sesión en que fueron tomados;
- c) asistir al presidente en todo lo relacionado con el desarrollo de las sesiones de la Comisión;
- d) asesorar a los integrantes de la Comisión;
- e) elaborar la convocatoria a las reuniones de la Comisión, así como los documentos para el desarrollo de las sesiones de trabajo;
- f) tramitar los asuntos que no requieran convocar a la Comisión;
- g) asesorar a las subcomisiones constituidas para el análisis de aspectos a debatir en sesiones de la Comisión;
- h) controlar el cumplimiento de los acuerdos adoptados por la Comisión; y
- i) cumplir las demás tareas que le asigne la Comisión y el presidente.

Artículo 100. El Secretariado Ejecutivo de la Comisión tiene las funciones siguientes:

- a) Evaluar asuntos que deben ser analizados, sin necesidad de convocar la Comisión;
- b) evaluar propuestas de modificaciones en listas internas con impacto en la lista general para someter al análisis de la Comisión; y
- c) cumplir las tareas que le atribuya la Comisión o el presidente.

Artículo 101.1. Los representantes de la Comisión, en relación con la seguridad y protección de la información clasificada y limitada, tienen las atribuciones y obligaciones siguientes:

- a) Asesorar y mantener informado al jefe sobre lo relacionado con la clasificación y desclasificación de la información;
- b) organizar, participar y controlar el proceso de elaboración y actualización de las listas internas para la clasificación y desclasificación de la información;
- c) presidir los estudios sobre el comportamiento de la aplicación de lo establecido en la lista interna de su órgano u organismo e informar a su jefe sobre el particular;
- d) controlar el uso de la lista interna e informar a su jefe sobre el particular;
- e) someter al análisis de la Comisión las propuestas de clasificación y desclasificación elaboradas en su órgano u organismo, previa aprobación del jefe;
- f) contribuir con la solución de las infracciones señaladas en materia de seguridad y protección de la información clasificada;

- g) exigir la aplicación de medida disciplinaria ante la ocurrencia de infracciones graves conforme a lo establecido en este Reglamento, y alertar al jefe en caso de incumplimientos;
 - h) validar el análisis de informaciones enmarcadas en temas específicos de la lista general, vinculadas con las misiones del órgano u organismo que represente, con el objetivo de lograr una concepción integral y proponer a la Comisión; y
 - i) cumplir cualquier tarea que como miembro de la Comisión le sea asignada.
2. Rendir cuenta a la Comisión de sus gestiones en cuanto al cumplimiento de lo dispuesto para la seguridad y protección de la información clasificada y limitada en su órgano u organismo;

SECCIÓN SEGUNDA

De la integración y funcionamiento de la Comisión Estatal para la Clasificación y Desclasificación de la Información Clasificada

Artículo 102. La Comisión, conforme a lo dispuesto en el Artículo 24 del mencionado Decreto-Ley 78 de 2023, la preside el Ministerio del Interior, cuenta con un vicepresidente y la integran representantes permanentes de todos los órganos del Estado y organismos de la Administración Central del Estado que ocupen el cargo de viceministro u equivalente.

Artículo 103. La Comisión cuenta con un secretariado ejecutivo que se conforma por el presidente, el vicepresidente, que es el representante del Ministerio de Economía y Planificación, y la integran un secretario designado por el ministro del Interior y por los representantes permanentes del Banco Central de Cuba y de los ministerios de Relaciones Exteriores, de las Fuerzas Armadas Revolucionarias, del Interior, de Finanzas y Precios, del Comercio Exterior y la Inversión Extranjera, de Ciencia, Tecnología y Medio Ambiente.

Artículo 104.1. Cuando un miembro de la Comisión no pueda continuar en esta, se reemplaza por uno nuevo designado por el jefe del órgano u organismo de la Administración Central del Estado o el Banco Central de Cuba, según sea el caso.

2. El miembro saliente queda liberado de la Comisión en el momento en que se presenta formalmente su sustituto.

3. El miembro saliente hace entrega al sustituto de toda la documentación inherente a esta responsabilidad.

Artículo 105. La Comisión sesiona de forma ordinaria una vez al año y el presidente convoca con carácter extraordinario cuando el trabajo así lo requiera.

Artículo 106. La Comisión, a propuesta del secretariado ejecutivo, organiza subcomisiones para actualizar la lista general para la clasificación y desclasificación de la información.

Artículo 107. La Comisión mantiene informado al Consejo de Ministros de su gestión, cuando corresponda.

CAPÍTULO V

LISTA GENERAL PARA LA CLASIFICACIÓN Y DESCLASIFICACIÓN DE LA INFORMACIÓN

Artículo 108. La lista general para la clasificación y desclasificación de la información, en lo adelante lista general, se conforma por denominaciones e indicadores considerados clasificados para el Estado cubano, agrupados en capítulos.

Artículo 109. El proceso de actualización de la lista general se realiza cada cinco años.

Artículo 110. Una vez transcurrido el término mencionado en el artículo anterior se actualiza la lista general, para lo cual cada uno de los jefes de los órganos y organismos de la Administración Central del Estado presentan a la Comisión las propuestas de desclasificación, modificación, supresión e inclusión de denominaciones, categorías y

períodos de permanencia, a partir de la evaluación previa de su lista interna, y fundamenta cada propuesta conforme al Anexo IX de este Reglamento.

Artículo 111.1. El proyecto de lista general se circula por la Comisión a los sujetos previstos en el Artículo 3 del Decreto-Ley 78 de 2023 para ser evaluado y emitir consideraciones.

2. Recibidas las consideraciones y una vez realizado y concluido el proceso de conciliación, la Comisión presenta al Consejo de Ministros la propuesta de lista general, acompañada de un resumen del proceso.

Artículo 112. Cuando una denominación de la lista general deba ser modificada como resultado de la actualización anual de las listas internas, se presenta la propuesta conforme al Anexo IX para su evaluación en la Comisión.

Artículo 113. La lista general se clasifica como Secreto y tienen acceso a ella las personas establecidas en el Artículo 28 del Decreto-Ley 78 de 2023.

CAPÍTULO VI

TRABAJO CON LA LISTA INTERNA PARA LA CLASIFICACIÓN Y DESCLASIFICACIÓN DE LA INFORMACIÓN

SECCIÓN PRIMERA

Lista interna para la clasificación y desclasificación de la información

Artículo 114.1. Los jefes de los sujetos definidos en el Artículo 3 del Decreto-Ley 78 de 2023 son los encargados de aprobar la lista interna para la clasificación y desclasificación de la información, en lo adelante lista interna, que contiene informaciones, en lugar de denominaciones o asuntos como se nombran en la lista general.

2. Las informaciones se derivan de las denominaciones o asuntos de la lista general, de acuerdo con el encargo estatal del sujeto.

3. La lista interna constituye un material de consulta permanente para los portadores de información clasificada.

Artículo 115. En el extremo izquierdo de la lista interna se inserta una columna correspondiente al número consecutivo de la información que se clasifica.

SECCIÓN SEGUNDA

De la elaboración y actualización de la lista interna y lista de información limitada

Artículo 116.1. Para la elaboración y actualización de la lista interna y lista de información limitada, el jefe de los sujetos crea un grupo de trabajo que preside el representante del sujeto en la Comisión.

2. En el grupo de trabajo participa el jefe del órgano de seguridad y protección, el especialista de protección de la información clasificada y cuantos jefes o especialistas se consideren necesarios, de manera que se garantice la representación de todas las estructuras.

3. La lista interna se elabora cuando se crea un sujeto obligado de la norma y se actualiza anualmente.

Artículo 117. Para la elaboración y actualización de la lista interna, además de las denominaciones de la lista general que impactan en el sujeto, se declaran aquellas informaciones propias de su encargo estatal que, a pesar de no estar explícitamente recogidas en la lista general, requieran ser clasificadas.

Artículo 118. La lista de información limitada del sujeto la conforman aquellas informaciones que no integran la lista interna, y no son públicas.

Artículo 119.1. El proceso de actualización de la lista interna y la lista de información limitada, se realiza anualmente y los jefes facultados presentan al órgano competente del MININT sus resultados en el mes de enero.

2. El órgano competente del MININT dispone de hasta quince días hábiles para emitir el dictamen de las propuestas de modificaciones que se le formulen; de existir algún señalamiento, debe ser corregido en el plazo de treinta días.

Artículo 120.1. La lista interna y lista de información limitada se aprueba por resolución del jefe facultado, posterior al dictamen favorable del órgano competente del MININT, y antes que concluya el mes de febrero de cada año, cuando exista modificación.

2. La lista interna se clasifica Secreta y la lista de información limitada se clasifica Limitada.

3. Copia de la resolución de la lista interna aprobada se envía al órgano competente del MININT.

Artículo 121. Los jefes facultados elaboran y actualizan sus listas internas, para lo cual tienen en cuenta la del sector a que pertenecen, y la adecúan a su misión y funciones específicas.

Artículo 122. De cada estudio anual que se realice para la actualización de las listas se conserva en un expediente las actas de los eventos de dirección y el resumen del proceso, lo cual se custodia por la OPCIC o Norma de Control, durante un año.

Artículo 123. Ante modificaciones a la lista general se realizan las correspondientes actualizaciones a las listas internas, siguiendo lo establecido en los artículos de esta sección.

CAPÍTULO VII

ORGANIZACIÓN DE LAS OFICINAS DE PROCESAMIENTO Y CONTROL DE INFORMACIÓN CLASIFICADA

Artículo 124.1. La OPCIC se crea y organiza, atendiendo a la estructura y categorización de cada sujeto, sistemas de trabajo y actividades, para el control de la información clasificada y limitada.

2. Se pueden crear una o varias OPCIC de acuerdo con el volumen de la información a controlar.

Artículo 125. En los casos donde la información clasificada no constituya un volumen considerable, se crea una Norma de Control a cargo de una persona no profesional que desempeñe las funciones establecidas en este Reglamento.

Artículo 126.1. La propuesta de creación de la OPCIC o de una Norma de Control, se realiza por el jefe facultado al órgano competente del MININT, y debe incluir las medidas internas, externas, de seguridad tecnológica y el SPC a implementar.

2. El órgano competente del MININT, mediante inspección, comprueba las medidas y emite el correspondiente dictamen.

Artículo 127.1. Pueden coexistir en un sujeto una o más OPCIC y una Norma de Control, cuando existan condiciones que lo justifiquen.

2. La OPCIC se subordina administrativamente al jefe del sujeto, quien designa a la persona responsable de esta oficina.

Artículo 128. Cuando coexistan más de una forma de control de la información clasificada, estas se responsabilizan con el control de la que gestionan, y sus jefes o persona designada responden por el cumplimiento de las funciones de cada una.

Artículo 129.1. El control de la información clasificada y limitada se realiza a través de los modelos de control establecidos en este Reglamento.

2. Cuando los modelos de control se soportan en sistemas informatizados requieren ser certificados por el MININT, en garantía de la seguridad de la confidencialidad, autenticidad, integridad, no repudio y disponibilidad de la información clasificada que gestiona, para lo cual deben contar con las medidas de seguridad criptográficas, de respaldo energético, salvadas de la información y protección física.

3. Los sistemas informatizados garantizan la generación de datos que se exigen en el sistema de modelaje del control de la información clasificada.

Artículo 130. La OPCIC o Norma de Control está en la obligación de controlar los documentos clasificados en cualquiera de las etapas de su ciclo de vida.

Artículo 131.1. Cuando se produzca la sustitución de un jefe de OPCIC o Norma de Control, este debe declarar mediante acta el estado de la información clasificada bajo su control, consignando lo siguiente:

- a) Fecha de entrega;
 - b) correspondencia entre el control de la información y su existencia física en cualquier soporte;
 - c) estado de actualización del registro y control de la información clasificada mediante el sistema informatizado o modelos establecidos; y
 - d) firmas del personal entrante y saliente con el visto bueno del jefe del sujeto.
2. El acta de entrega se conserva en la OPCIC o Norma de Control.

CAPÍTULO VIII

DE LA HABILITACIÓN DEL PERSONAL IMPLICADO EN LA SEGURIDAD Y PROTECCIÓN DE LA INFORMACIÓN CLASIFICADA

Artículo 132. Se entiende por habilitación la conclusión satisfactoria del proceso mediante el cual se comprueba la confiabilidad del personal que opta por cargos vinculados a la seguridad y protección de la información clasificada y para ello cumple los requisitos siguientes:

- a) Ser mayor de 18 años;
- b) ser ciudadano cubano;
- c) estar apto física y mentalmente;
- d) valorar, en caso de poseer antecedentes penales, la lesividad social del hecho y su vinculación con el cargo a desempeñar;
- e) no haber sido separado deshonrosamente de instituciones armadas, ni de cualquier otra actividad laboral;
- f) poseer título de enseñanza media o superior en correspondencia con el cargo a ocupar; y
- g) acreditar la experiencia en la actividad de seguridad y protección de la información o haber prestado servicio en instituciones de las FAR o el MININT, en caso de tenerla.

Artículo 133. Para la habilitación, los jefes de las entidades y sistemas de trabajo y actividades categorizadas de máxima seguridad, presentan al órgano competente del MININT un expediente que acredite los requisitos establecidos, conforme al Anexo X de este Reglamento.

Artículo 134.1. El proceso de habilitación no excede los cuarenta y cinco días, contados a partir de la entrega de la documentación requerida.

2. En caso necesario la autoridad habilitante puede convocar a entrevista individual al candidato para esclarecer elementos de interés.

3. Cuando la autoridad habilitante es el órgano competente del MININT, una vez realizadas las investigaciones pertinentes, devuelve al sujeto el expediente y propone la aprobación o no del candidato.

4. Cuando quien habilita es el órgano de seguridad y protección del sujeto, una vez concluido el expediente decide la aprobación o no del candidato.

5. El proceso de habilitación concluye en todos los casos con la notificación al solicitante de su aprobación o no, acción que realiza el sujeto.

Artículo 135. Una vez habilitado el personal implicado en la seguridad y protección de la información clasificada, el sujeto procede a su certificación.

CAPÍTULO IX

SOBRE LAS ACCIONES DE CONTROL

SECCIÓN PRIMERA

Disposiciones generales

Artículo 136. Se entiende por acciones de control de la seguridad y protección de la información clasificada y limitada, las acciones de diagnosticar, inspeccionar, controlar y recontrolar el cumplimiento de las medidas de seguridad y protección de la información clasificada y limitada.

Artículo 137.1. En los sujetos, sistemas de trabajo y actividades categorizados de máxima seguridad las acciones de control se realizan por especialistas del órgano competente del MININT.

2. Excepcionalmente, los especialistas del órgano competente del MININT controlan sujetos, sistemas de trabajo y actividades categorizados de media y básica seguridad, ante requerimientos del jefe de los sujetos o hechos extraordinarios.

Artículo 138. Los jefes de seguridad y protección, y de la OPCIC y la Norma de Control, realizan acciones de control interno sobre la seguridad y protección de la información clasificada y limitada en su ámbito de atención.

Artículo 139. Las acciones de control en materia de seguridad y protección de la información clasificada y limitada a desarrollar en las representaciones cubanas en el exterior que se realizan por el MININT, se coordinan previamente con el Ministerio de Relaciones Exteriores, o se realizan a solicitud de este organismo.

Artículo 140. Las acciones de control a la información clasificada y limitada, tienen los objetivos siguientes:

- a) Comprobar y evaluar el cumplimiento de lo establecido en relación con la seguridad y protección de la información clasificada y limitada;
- b) evaluar el cumplimiento de obligaciones y funciones por los portadores, jefes y personal implicado en la seguridad y protección de la información clasificada;
- c) identificar amenazas, riesgos y vulnerabilidades que presenta la seguridad y protección de la información clasificada; y
- d) proponer y exigir la aplicación de medidas disciplinarias que correspondan ante las infracciones graves detectadas.

Artículo 141. Las acciones de control se programan, organizan y comunican oportunamente; se ejecutan de forma sorpresiva, o ante la detección o evidencia de infracciones.

Artículo 142. Los especialistas del órgano competente del MININT en las acciones de control que realicen, tienen las facultades y atribuciones siguientes:

- a) Acceder y revisar en el sujeto, todas las informaciones públicas, clasificadas y limitadas en cualquier soporte;

- b) identificar el o los responsables de las infracciones y proponer la aplicación de la medida disciplinaria que corresponda;
- c) solicitar al personal del sujeto, la presentación de informaciones por escrito o declaraciones acerca de cuestiones relacionadas con las acciones de control que se realicen;
- d) preservar evidencias durante las acciones de control para demostrar las infracciones;
- e) ocupar mediante acta, documentos y materiales para el trabajo con la información clasificada que son probatorios de infracciones detectadas durante una acción de control, bajo la obligación de debida custodia; y
- f) comunicar a los sujetos controlados, los términos fijados para responder los requerimientos realizados.

Artículo 143.1. De toda acción de control se deja constancia por escrito en un acta que suscriben ambas partes y que se corresponde con el objetivo de la acción de control.

2. Se elaboran dos ejemplares, para el controlado y el controlador, que recoge los aspectos siguientes:

- a) Sujeto donde se realizó la acción de control;
- b) modalidad de la acción de control;
- c) fecha en que se realiza;
- d) infracciones detectadas;
- e) infracciones graves, responsables, propuesta de medida disciplinaria;
- f) sugerencias, recomendaciones e indicaciones;
- g) conclusiones; y
- h) firma y cargos de los controlados y el controlador.

Artículo 144. El plan de medidas para solucionar las infracciones se ajusta al formato que establece el Anexo XI de este Reglamento.

SECCIÓN SEGUNDA

Diagnóstico, inspección, control, recontrol

Artículo 145.1. El diagnóstico es la acción de control que se ejecuta con carácter preventivo para comprobar el estado de la seguridad y protección de la información clasificada y limitada, en un sujeto.

2. Solo se exige plan de medidas resolutivo con plazo inmediato para la transformación de infracciones detectadas, lo que se controla en correspondencia con las fechas de cumplimiento aprobadas.

3. Se realizan a solicitud de un jefe o por interés del órgano competente del MININT.

Artículo 146. La inspección es la acción de control que se efectúa sistemáticamente en un sujeto, con el propósito de verificar el cumplimiento de lo que establece este Reglamento para garantizar la seguridad y protección de la información clasificada y limitada.

Artículo 147. El control es la acción que anualmente se planifica y ejecuta con alcance nacional, con el propósito de comprobar integralmente el estado de la seguridad y protección de la información clasificada y limitada en un sujeto, mediante la comprobación del cumplimiento de su esquema de seguridad.

Artículo 148.1. El recontrol es la acción que se planifica y ejecuta con alcance nacional, con el objetivo de comprobar el cumplimiento de planes de medidas de los sujetos para transformar el estado de la seguridad y protección de la información clasificada y limitada, posterior a un control.

2. El recontrolado presenta un informe valorativo del seguimiento y evaluación del cumplimiento del plan de medidas, las medidas disciplinarias aplicadas y la efectividad de la implementación de este plan en las infracciones que fueron objeto de análisis durante el control realizado el año anterior.

3. El recontrol tiene una evaluación a partir de la efectividad alcanzada en la transformación de infracciones en correspondencia con los criterios siguientes:

- a) Avance: cumplimiento alcanzado del ochenta por ciento en adelante, de las medidas adoptadas para erradicar las infracciones detectadas y las causas y condiciones que le dieron origen.
- b) Estancado: cumplimiento entre el sesenta y el setenta y nueve por ciento de las medidas para resolver las infracciones que le fueron detectadas y las causas y condiciones que le dieron origen o cuando se han identificado nuevas infracciones.
- c) Retroceso: cumple menos del sesenta por ciento de las medidas dictadas para solucionar las infracciones detectadas y las causas y condiciones que le dieron origen o cuando se han identificado nuevas infracciones.

4. Cuando en un recontrol persistan infracciones no resueltas por causas ajenas a la voluntad del sujeto, previa evidencia demostrada, puede modificarse la evaluación a favor de este.

Artículo 149. En el caso del diagnóstico, control y recontrol se resume informe conclusivo que se entrega y despacha con el representante del órgano u organismo del Estado en la Comisión y se establece un plazo de treinta días para que el sujeto presente el plan de medidas resolutivo de las infracciones señaladas.

CAPÍTULO X DE LA CATEGORIZACIÓN DE LOS SUJETOS, SUS SISTEMAS DE TRABAJO Y ACTIVIDADES

Artículo 150. La propuesta de categorización de un sujeto responde a las complejidades de sus sistemas de trabajo y actividades, conforme a lo establecido en el Artículo 35 del Decreto-Ley 78 de 2023, y se presenta al órgano competente del MININT por los jefes facultados mediante un expediente que contiene los elementos siguientes:

- a) Nombre del sujeto;
- b) misión;
- c) ubicación geográfica y caracterización del entorno;
- d) identificación de la tecnología de la información, en lo adelante TI, para el procesamiento de información clasificada;
- e) identificación de TI y tecnologías operacionales, en lo adelante TO destinadas al procesamiento de información a proteger para garantizar la integridad y disponibilidad de la producción de bienes y servicios que asegura el sujeto;
- f) análisis de riesgos, amenazas y vulnerabilidades, internas y externas, que puedan propiciar la alteración de la confidencialidad, integridad y disponibilidad de la información a proteger;
- g) resultado de la última acción de control del órgano competente del MININT;
- h) nivel de categorización que se propone para el sujeto, sistema de trabajo o actividades;
- i) firma del jefe; y
- j) fecha de remisión.

Artículo 151. En aquellos sujetos categorizados de media o básica seguridad, se evalúa la conveniencia de categorizar de máxima un sistema de trabajo y actividades en las

que prevalezcan informaciones relacionadas con objetivos estratégicos de la defensa y la seguridad nacional, políticos, económicos, científicos-técnicos, culturales y sociales, cuya divulgación, conocimiento no autorizado, su alteración o no disponibilidad pueda causar daños o perjuicios al Estado cubano.

Artículo 152. Cuando se modifiquen los argumentos que dieron origen a una categoría, sobre la base de los elementos de los incisos d), e) y f) del Artículo 150, se presenta la propuesta de modificación con similar expediente, en un plazo que no exceda los noventa días de la causa que origina el cambio de categorización.

Artículo 153.1. El proceso de aprobación de la categorización por el órgano competente del MININT no excede los noventa días, contados a partir de la entrega de la documentación requerida.

2. En caso necesario, y durante ese período, el órgano competente del MININT puede solicitar requerimientos o convocar a quien considere para esclarecer elementos de interés sobre la propuesta que se presente.

3. El proceso concluye con el dictamen de aprobación de la categoría del sujeto, sus sistemas de trabajo y actividades.

CAPÍTULO XI DE LOS ESQUEMAS DE SEGURIDAD

SECCIÓN PRIMERA

Disposiciones generales

Artículo 154. El esquema de seguridad establece los lineamientos conceptuales para garantizar la seguridad y protección de la información clasificada y las entidades, sistemas de trabajo y actividades categorizados, y comprende tres dimensiones: medidas organizativas, físicas y tecnológicas.

Artículo 155. Las medidas organizativas se refieren a:

- a) La determinación de acciones de autocontrol que responden al sistema de control interno del sujeto en función de la supervisión de la seguridad y protección de la información clasificada y entidades, sistemas de trabajo y actividades categorizados;
- b) la proyección de la capacitación del personal implicado en la seguridad y protección de la información clasificada y entidades, sistemas de trabajo y actividades categorizados y de los portadores;
- c) la elaboración, desde tiempo de paz, del plan de evacuación, conservación y destrucción de la información clasificada y limitada ante situaciones excepcionales;
- d) la determinación de requerimientos de seguridad y protección de la información clasificada y sistemas de trabajo y actividades para el plan de ciberseguridad; y
- e) la certificación y compatibilización de sistemas de trabajo y actividades que soporten información clasificada con los intereses de la defensa, seguridad y orden interior.

Artículo 156. Las medidas físicas, además de lo establecido en la legislación vigente, contemplan:

- a) La identificación de muebles y locales donde exista información clasificada y limitada y sistemas de trabajo y actividades categorizados de máxima seguridad;
- b) garantizar sistemas constructivos robustos;
- c) las medidas de cierre, sellaje y sistemas automatizados de muebles y locales, según corresponda para garantizar seguridad y protección;
- d) establecer niveles de acceso y personal autorizado;
- e) control de llaves o contraseñas para acceder a muebles, locales y TO;

- f) equipar locales con medios de extinción de incendios; y
- g) mantener medidas de climatización, respaldo energético y salvas informativas que garanticen disponibilidad de los servicios.

Artículo 157. Las medidas tecnológicas contemplan:

1. El SPC para proteger la información clasificada y los sistemas de trabajo y actividades categorizadas de máxima seguridad.
2. La autenticación individual de usuarios o sujetos para el acceso a la infraestructura y a servicios suministrados por la entidad.
3. El control de acceso de dispositivos removibles a las TI y TO clasificadas;
4. La identificación y protección, con criptografía, los códigos fuentes de sistemas críticos, configuraciones y esquemas que detallen características que personalizan una infraestructura y sistemas tecnológicos.
5. La configuración con seguridad tecnológica y criptográfica de redes inalámbricas autorizadas, garantizan el control de accesos y la protección de la información, en dependencia de la tecnología a emplear.
6. La segmentación de las redes en zonas de seguridad que separan los servicios externos, internos, y las estaciones de trabajo en correspondencia con la actividad específica de las estructuras internas, a los fines de garantizar el flujo de la comunicación y la información entre ellas.
7. En caso de utilizarse tecnología de virtualización dirigida al alojamiento de los servicios dentro de zonas de seguridad, garantizar la configuración de un concentrador virtual independiente para la implementación de estos.
8. La asignación manual o automático y el control de manera centralizada del direccionamiento interno, así como asociar a este los identificadores de las interfaces de red.
9. Controlar que no exista acceso hacia redes públicas de alcance global o nacional desde la administración remota de la infraestructura tecnológica.
10. La evaluación por el sujeto de la pertinencia de establecer un centro de respaldo descentralizado geográficamente con capacidades de asumir las principales actividades, ante contingencias que puedan afectar la disponibilidad del principal.
11. Diseñar un proceso sistemático para la gestión de vulnerabilidades y actualizaciones de la infraestructura tecnológica, sobre la base de la publicación de las alertas y actualizaciones por los proveedores de tecnologías desplegadas, fuentes de confianzas, así como sistemas de seguridad desplegadas; y evaluar su aplicación de acuerdo con el nivel de criticidad y las implicaciones en los sistemas tecnológicos del sujeto.
12. Garantizar la protección contra programas malignos en toda la infraestructura tecnológica, realizar su actualización periódica y la administración centralizada.
13. Establecer el control del equipamiento, aplicaciones y servicios autorizados, así como que la instalación de nuevas aplicaciones o servicios solo se realice por el personal autorizado sobre la base de la política de seguridad aprobada en el sujeto.
14. Garantizar una correcta política de salva, con copias de respaldo verificadas y con protección criptográfica de la información, configuraciones, aplicaciones y servicios del sujeto.
15. La reparación o mantenimiento de los equipos destinados al procesamiento de información clasificada se realiza con garantías de extracción del soporte de almacenamiento del equipo, que se custodia en la OPCIC o Norma de Control.

16. Configurar con criterios de ciberseguridad y criptografía los servicios, plataformas, sistemas, aplicaciones, servidores y equipamiento de conectividad, que permita:
 - a) El bastionado de estos recursos y en especial los que brinden servicios expuestos a Internet;
 - b) revisar y corregir las opciones de las configuraciones por defecto;
 - c) eliminar o inhabilitar los servicios, protocolos, puertos y cuentas innecesarias para las funciones que está destinado y de la infraestructura donde se despliegue;
 - d) activar las opciones de seguridad que correspondan, según los requerimientos específicos de despliegue;
 - e) utilizar vías y protocolos con protección criptográfica aprobada para su gestión y administración; y
 - f) registrar la trazabilidad detallada de su operación.
17. Los responsables de ciberseguridad deben implementar y garantizar el registro de las trazas generadas por el equipamiento de seguridad, redes, servidores y servicios, las cuales tienen que contener los eventos que permitan la detección, caracterización e investigación de incidentes; para lo que deben cumplir los requisitos siguientes:
 - a) Personalizar las trazas y registrar los parámetros necesarios para la correcta comprensión e identificación de los eventos e incidentes;
 - b) garantizar el almacenamiento, integridad y accesibilidad de las trazas por un período indefinido en sujetos categorizados de máxima seguridad; no menor de cinco años para los de mediana seguridad y no menos de tres años en los de seguridad básica;
 - c) preferentemente implementar sistemas de almacenamiento centralizados de trazas que faciliten el análisis y la correlación de eventos, así como la descentralización geográfica de copias de respaldo; e
 - d) implementar un servicio centralizado de tiempo que permita la sincronización de la infraestructura y por consiguiente la data de las trazas que se registren.
18. Utilizar adecuadamente los privilegios de administración, así como garantizar su control mediante acciones de auditorías internas y externas, para lo que deben cumplir los requisitos siguientes:
 - a) Reservar las cuentas de administración para las acciones de gestión y configuración que lo requieran, por el personal facultado y con refuerzo del proceso de autenticación;
 - b) garantizar que los accesos para ejecutar las acciones de gestión y configuración de la infraestructura tecnológica, se realicen únicamente desde segmentos de red dedicados y con protección criptográfica para la administración, o en su defecto, de modo local en centros de datos, locales tecnológicos, gabinetes de comunicación y estaciones de trabajo;
 - c) como norma, instrumentar en los usuarios el empleo de cuentas sin privilegios de administración, y utilizar por parte de los administradores cuentas sin privilegios para tareas no administrativas, así como otras operaciones habituales de procesamiento de información; y
 - d) reforzar la protección del equipamiento utilizado y el canal de acceso con requerimientos criptográficos aprobados para realizar tareas de administración; preferentemente dedicar computadoras con este objetivo, las cuales solo pueden tener acceso a la gestión de la infraestructura.

19. Los sujetos deben organizar e implementar la supervisión de la disponibilidad y seguridad de la infraestructura tecnológica que soporta sus procesos de trabajo, así como priorizar el equipamiento de conectividad, procesamiento, aplicaciones y servicios críticos.
20. Los sujetos deben desplegar y aprovechar herramientas o mecanismos enfocados en el monitoreo de la disponibilidad del equipamiento principal de la infraestructura, así como la detección y obstaculización de ataques internos y externos, garantizar la configuración y actualización de los parámetros de detención en correspondencia con la infraestructura tecnológica y el análisis de riesgos, que incluye:
 - a) Conformar procedimientos que establezcan el modo de actuación ante la detección de incidentes de ciberseguridad y criptografía;
 - b) determinar el personal o estructura capacitada para asumir el proceso de supervisión y gestión de los incidentes de ciberseguridad con impacto en la infraestructura tecnológica del sujeto; y
 - c) mantener actualizado y certificado el grupo de trabajo de la criptografía, para asumir el proceso de supervisión y control ante incidentes con los SPC implementados en el sujeto.

Artículo 158. Cada sujeto personaliza el esquema de seguridad, conforme a las medidas organizativas, físicas y tecnológicas establecidas en los artículos de esta sección, en correspondencia con la categorización de media y básica aprobada, en un plazo de hasta sesenta días posteriores a notificarse la aprobación de esta.

Artículo 159. Los esquemas de seguridad, con la categorización de media y básica, se aprueban por el jefe facultado y se anexan a su expediente de categorización, actualizándolos anualmente.

SECCIÓN SEGUNDA

De los esquemas de seguridad de los sujetos, sus sistemas de trabajo y actividades categorizados de máxima seguridad

Artículo 160. En el caso de los esquemas de seguridad de los sujetos, y de sus sistemas de trabajo y actividades categorizados de máxima seguridad, además de las medidas genéricas de los artículos 155, 156 y 157, deben cumplir las siguientes:

1. Garantizar la alta disponibilidad de enlaces principales y equipamiento de procesamiento o producción mediante la redundancia activa según su encargo.
2. Establecer un centro de respaldo descentralizado geográficamente con capacidades de asumir las principales actividades, ante contingencias que puedan afectar la disponibilidad del principal.
3. Implementar un esquema de filtrado en el equipamiento de gestión y control de acceso en la infraestructura, configurando reglas que permitan solo los flujos de comunicación, como pueden ser direcciones, puertos y protocolos, autorizados entre zonas, subredes y hacia los servicios.
4. Diseñar e implementar un proceso sistemático para la gestión de vulnerabilidades y actualizaciones de la infraestructura tecnológica, sobre la base de la publicación de las alertas y actualizaciones por los proveedores de tecnologías desplegadas, fuentes de confianzas, así como sistemas de seguridad desplegados.
5. Diseñar el despliegue de las aplicaciones, plataformas y sistemas con las medidas de seguridad requeridas, el sistema de trabajo y actividades categorizados de máxima seguridad y que soporten servicios críticos, mediante tecnologías operacionales, así como con acceso a Internet; para lo que deben garantizar los requisitos siguientes:

- a) Aval de validación, certificación o compatibilización de ciberseguridad y criptografía, por una entidad autorizada y por la Dirección de Criptografía, respectivamente;
- b) diagnóstico periódico o cada vez que se realicen modificaciones y actualizaciones significativas, o se conozcan o detecten vulnerabilidades que afecten la confidencialidad, disponibilidad e integridad de las informaciones y datos que se procesen, almacenen o tramiten en su infraestructura tecnológica;
- c) las medidas de orden organizativo y tecnológico en la infraestructura que complementen la ciberseguridad de las aplicaciones, plataformas y sistemas;
- d) garantías de no acceso a redes de alcance global en aquellas estaciones con acceso a sistemas o plataformas críticas para el sujeto;
- e) identificación del personal o entidad calificada para brindar soporte técnico; y
- f) registro de las acciones relacionadas con la autenticación y autorización; la administración de cambios de configuración, gestión de roles, usuarios, privilegios, credenciales; infracciones graves, infracciones, errores y fallos, validación de datos; así como los inicios y cierres de equipos y sistemas.

Artículo 161.1. Para la aprobación de los esquemas de máxima seguridad, el jefe facultado presenta la propuesta personalizada al órgano competente del MININT en un plazo de hasta setenta y cinco días, posterior a la aprobación de la categorización.

2. El órgano competente del MININT dispone de hasta quince días para emitir conformidad de aprobación del esquema de seguridad en los categorizados de máxima.

Artículo 162.1. Ante intereses de contratación de esquemas de seguridad a un tercero, para sistemas de trabajo y actividades categorizadas de máxima seguridad, el jefe facultado presenta al órgano competente del MININT la propuesta, identificando la entidad a contratar, licencia para prestar el servicio y los argumentos de la tercerización de este servicio.

2. El órgano competente del MININT dispone de quince días para responder la propuesta.

Artículo 163. Las representaciones cubanas en el exterior cumplen el esquema de seguridad establecido para los sujetos categorizados de máxima, en materia de seguridad y protección de la información clasificada, y sus sistemas de trabajo y actividades, la cual se garantiza por el Servicio Central de Cifras del MININT.

SECCIÓN TERCERA

Del plan de evacuación para la conservación y destrucción de la información clasificada y limitada ante situaciones excepcionales y de desastre

Artículo 164. El plan de evacuación para la conservación y destrucción de la información clasificada y limitada ante situaciones excepcionales y de desastre, en lo adelante plan, se elabora por un grupo de trabajo presidido por el jefe del sujeto, e integrada por el jefe de seguridad y protección, especialista de defensa, jefe de OPCIC o Norma de Control y especialistas que se convoquen con acceso a información clasificada.

Artículo 165. Para la conformación del plan se define la información clasificada y limitada, en cualquier soporte, que:

- a) Se utiliza durante la situación excepcional y de desastre, y se entrega y custodia por el portador;
- b) se evacua por su valor estratégico, económico o patrimonial, así como el lugar a donde se traslada, previa coordinación con el responsable de la defensa del lugar de evacuación; y

- c) se destruye el resto de la información clasificada y limitada que no se utiliza, ni se evacua en la sede del sujeto o en el lugar declarado en el plan.

Artículo 166.1. El plan cuenta con la siguiente información y estructura:

- a) Título del plan;
- b) responsables de la ejecución de las acciones del plan designados por el grupo de trabajo, de los que se relaciona dirección, teléfono y función durante la ejecución;
- c) tecnologías de la información a utilizar, evacuar o destruir;
- d) medios y transporte destinados para la evacuación, destrucción y el borrado de información digital;
- e) lugar previsto para evacuar la información y contacto del responsable de la defensa del lugar de evacuación;
- f) lugar destinado para la destrucción de la información y responsable; y
- g) un gráfico que simbolice la ubicación de la OPCIC y Norma de Control, así como con color ROJO áreas contentivas de archivos y tecnologías de la información a incinerar y en color AZUL a evacuar; además del itinerario a ejecutar para la evacuación.

2. Los responsables de la ejecución de las acciones del plan deben tener acceso a la información clasificada y limitada, posibilidades de llegar al lugar cuando se activa el plan y preparación metodológica para su cumplimiento.

3. La copia de las llaves de los locales graficados en el plan deben conservarse en la OPCIC o Norma de Control, con normas de identificación y seguridad.

Artículo 167. Ante situaciones excepcionales y de desastre como primera medida del plan, se concentra en la OPCIC o Norma de Control, la información clasificada y limitada, en cualquier soporte, que se encuentre en otras áreas.

Artículo 168.1. Del plan se elabora un único ejemplar, que se clasifica según la lista interna del sujeto y debe permanecer en sobre cerrado y lacrado en la OPCIC o Norma de Control.

2. Los responsables de la ejecución del plan deben conocer el lugar donde se encuentra archivado.

Artículo 169. La persona facultada para dar la orden de ejecución de este plan es el jefe del sujeto.

Artículo 170. Los jefes facultados garantizan que los responsables de la ejecución del plan reciban preparación anual, en el contexto de ejercicios nacionales para la defensa, con el objetivo de garantizar la efectividad de este.

CAPÍTULO XII

DE LAS ATRIBUCIONES Y OBLIGACIONES DE LOS JEFES EN RELACIÓN CON LA INFORMACIÓN CLASIFICADA Y LIMITADA

Artículo 171. Los jefes de órganos, organismos y entidades del Estado, sistema empresarial y de las organizaciones políticas, sociales y de masas, además de lo establecido en el Decreto-Ley 78 de 2023, tienen respecto a la seguridad y protección de la información clasificada y limitada, las atribuciones y obligaciones siguientes:

- a) Crear las condiciones materiales y de organización que garanticen la aplicación y el cumplimiento de lo establecido en el Decreto-Ley 78 de 2023, este Reglamento y demás disposiciones complementarias;
- b) proponer la creación de la OPCIC o de una Norma de Control, al órgano competente del MININT;
- c) presentar el proyecto de lista interna anualmente al órgano competente del MININT, cuando esta tenga modificaciones, y aprobarla, por resolución, previo dictamen favorable de dicho órgano;
- d) aprobar por resolución la lista de información limitada;

- e) aprobar por resolución los procedimientos para la autorización temporal o definitiva de salida al exterior de un portador por asuntos personales;
- f) cumplir con lo establecido para la transmisión de la información clasificada y limitada por los medios de comunicación cuando sea necesario;
- g) garantizar que no se divulgue información clasificada y limitada, por los medios masivos de difusión;
- h) garantizar que se cumplan las medidas establecidas para la seguridad y protección de la información clasificada o limitada, en cualquier soporte;
- i) excepcionalmente, autorizar por escrito el empleo de tecnologías de la información de propiedad personal o de otro sujeto, para elaborar, registrar, reproducir, transmitir o conservar información clasificada y limitada;
- j) autorizar por escrito la extracción, dentro o fuera del territorio nacional, de tecnologías de la información con información clasificada o limitada, así como su empleo en eventos, siempre que cumplan las medidas de seguridad establecidas;
- k) aprobar cuáles de las informaciones que genera el sujeto debe identificarse como limitada y cuándo pierde esa condición;
- l) establecer los procedimientos internos para el ciclo de vida de la información limitada;
- m) otorgar acceso a la información limitada que genere el sujeto a personas nacionales y extranjeras y disponer las medidas de su seguridad y protección;
- n) autorizar, previa consulta con el destinatario, la desclasificación de un documento Secreto de Estado, cuyo período de permanencia no haya vencido o este sea hasta que se autorice su desclasificación;
- ñ) presentar para su aprobación, al órgano competente del MININT, los expedientes de categorización de entidades y sistemas de trabajo y actividades, bajo su radio de acción;
- o) presentar para su aprobación, al órgano competente del MININT, los esquemas de máxima seguridad;
- p) presentar para su aprobación, al órgano competente del MININT, los intereses de contratación de esquemas de seguridad a un tercero, para sistemas de trabajo y actividades categorizadas de máxima seguridad;
- q) aprobar los esquemas de seguridad para la categorización media y básica;
- r) determinar las medidas organizativas, físicas y tecnológicas para garantizar la seguridad y protección de la información limitada, en cualquier soporte que genere el sujeto;
- s) investigar las causas y condiciones, daños o perjuicios ocasionados al sujeto, responsables y medidas administrativas y disciplinarias que correspondan, ante la ocurrencia de hechos que constituyan infracciones graves de la seguridad y protección de la información clasificada;
- t) mantener actualizado el control de acceso a la información clasificada y limitada por portadores y definir su regulación migratoria;
- u) designar la persona encargada de instruir al portador ante la autorización de salida al exterior;
- v) supervisar el proceso de entrega de la información clasificada cuando ocurra un cambio o sustitución de un jefe de OPCIC o Norma de Control; y
- w) garantizar la preparación anual de los responsables de ejecutar plan de evacuación para la conservación y destrucción de la información clasificada y limitada ante situaciones excepcionales y de desastre.

Artículo 172. Los jefes en cualquier nivel tienen las atribuciones y obligaciones siguientes:

- a) Organizar, asesorar y controlar el cumplimiento del Decreto-Ley 78 de 2023, este Reglamento y demás disposiciones complementarias, así como las emanadas de la comisión estatal para la clasificación y desclasificación de la información clasificada;
- b) mantener actualizado el control de acceso a la información clasificada y limitada por portadores;
- c) mantener actualizada la lista de portadores de información clasificada y proponer su regulación migratoria;
- d) autorizar por escrito la reproducción de documentos clasificados;
- e) designar el personal que se responsabiliza con las medidas de seguridad de los documentos clasificados a imprimir o reproducir en imprenta;
- f) designar la persona responsable de la OPCIC o Norma de Control;
- g) designar quién asume la responsabilidad del personal de correo, cuando no exista;
- h) habilitar al personal implicado en la seguridad y protección de la información clasificada de los sujetos categorizados de media y básica seguridad;
- i) presentar al órgano competente del MININT la documentación requerida para la habilitación del personal implicado en la seguridad y protección de la información de los sujetos categorizados como máxima seguridad;
- j) asesorar, exigir y controlar el uso correcto de la lista interna para la clasificación y desclasificación de la información;
- k) participar y asesorar en la elaboración y actualización de la lista interna para la clasificación y desclasificación de la información;
- l) aprobar, a propuesta del ejecutor, la desclasificación de una parte del documento clasificado y limitado;
- m) asesorar y exigir el cumplimiento de las obligaciones comunes de todo el personal en cuanto a la seguridad y protección de la información clasificada y limitada;
- n) asesorar y supervisar el contenido de las cláusulas de confidencialidad de los convenios de colaboración con socios extranjeros, según corresponda;
- ñ) compatibilizar con el órgano competente del MININT el sistema informatizado para el registro y control de la información clasificada;
- o) establecer y supervisar los centros de datos, lugares y muebles donde se elabore, procese, tramite, trasmita reproduzca y conserve la información clasificada en los sujetos, con el fin de aplicar las medidas de seguridad y protección correspondientes y comprobar su cumplimiento;
- p) revisar y dictaminar, de conjunto con los responsables de ciberseguridad y criptografía, las tecnologías de la información que se trasladen al exterior, para comprobar que contengan las informaciones autorizadas y se apliquen las medidas de seguridad tecnológicas y criptográficas correspondientes;
- q) planificar y realizar el control al cumplimiento de lo establecido para la seguridad y protección de la información, en cualquier soporte;-
- r) informar de inmediato al órgano competente del MININT e investigar las causas y condiciones, daños o perjuicios que pueden ocasionar al Estado cubano y los responsables, así como aplicar las medidas administrativas y disciplinarias correspondientes, ante la ocurrencia de hechos que constituyan infracciones graves de la seguridad y protección de la información clasificada y limitada;
- s) planificar, elaborar y ejecutar planes de preparación de los portadores y del personal de seguridad y protección de la información clasificada y limitada, así como controlar su cumplimiento; y

- t) responder por la elaboración del plan de evacuación para la conservación y destrucción de información clasificada y limitada ante situaciones excepcionales y desastre, y presentar a la aprobación correspondiente.

Artículo 173. El jefe de la OPCIC y Norma de Control, tiene las atribuciones y obligaciones siguientes:

- a) Controlar el ciclo de vida de la información clasificada y limitada en cualquier soporte;
- b) asesorar y exigir el uso correcto de la lista interna para la clasificación y desclasificación de la información;
- c) planificar y efectuar controles para comprobar el estado de cumplimiento de las medidas de seguridad y protección de la información clasificada, en cualquier soporte;
- d) asesorar e instruir al personal con nivel de acceso a la información clasificada en lo relativo a la base jurídica para la seguridad y protección de la información clasificada;
- e) controlar la preparación del personal con acceso a información clasificada que viaja al exterior;
- f) conocer, cumplir y exigir los modelos establecidos en este Reglamento para el control de la información clasificada en cualquier soporte;
- g) realizar muestreos sistemáticos a la información limitada y al resto de la información que se genere en el sujeto en cualquier soporte, con el objetivo de detectar infracciones graves en el uso de la lista interna para la clasificación y desclasificación de la información;
- h) revisar los soportes removibles personales que se conecten a tecnologías de la información del sujeto donde se procese, almacene o transmita información clasificada, con el objetivo de detectar posibles infracciones;
- i) establecer coordinaciones de trabajo permanentes con los responsables de ciberseguridad y criptografía del sujeto, para ejercer el control de las medidas de seguridad tecnológica y criptográficas sobre la información clasificada en las tecnologías de la información y tecnologías operacionales;
- j) exigir que se determinen y cumplan los períodos de permanencia de las informaciones clasificada y limitada para facilitar su desclasificación;
- k) garantizar la destrucción de la información clasificada y limitada en cualquier soporte, cuando se autorice;
- l) informar oportunamente a la persona designada para atender la seguridad y protección de la información clasificada y limitada, las infracciones graves que se detecten en su actividad de control; y
- m) controlar el registro y existencia física de los medios vinculados a la seguridad y protección de la información clasificada y limitada, en su área de competencia.

Artículo 174. El personal de la OPCIC y de la Norma de Control, tiene las atribuciones y obligaciones siguientes:

- a) Controlar la entrada y salida de la información clasificada y limitada, en cualquier soporte;
- b) asignar un número de registro a todo documento clasificado y limitado, que se genere o reciba, en cualquier soporte;
- c) controlar la entrega y devolución de los documentos clasificados y limitados al personal con acceso, en cualquier soporte, en el territorio nacional y los que sean necesarios trasladar al exterior;

- d) controlar la elaboración, en cualquier soporte, de los documentos clasificados y limitados en el sujeto;
- e) cumplir con el nivel de acceso establecido en la entrega de los documentos clasificados y limitados;
- f) controlar la reproducción de la información clasificada y limitada, en cualquier soporte;
- g) aplicar las medidas de control para el oportuno retorno de los documentos clasificados y limitados a los archivos;
- h) informar oportunamente al jefe de la OPCIC o al especialista de seguridad y protección o persona designada para atender la seguridad y protección de la información clasificada y limitada, las infracciones graves que detecten en su actividad de control; y
- i) cumplir las orientaciones del jefe de la OPCIC y Norma de Control en cuanto al plan de evacuación para la conservación y destrucción de la información clasificada y limitada.

Artículo 175. El especialista o persona designada para atender la seguridad y protección de la información clasificada, subordinado a la dirección de seguridad y protección de los sujetos, tiene las atribuciones y obligaciones siguientes:

- a) Organizar, asesorar y controlar el cumplimiento del Decreto-Ley, este Reglamento y demás disposiciones complementarias;
- b) asesorar, exigir y controlar el uso correcto de la lista interna para la clasificación y desclasificación de la información;
- c) participar y asesorar en la elaboración y actualización de la lista interna para la clasificación y desclasificación de la información;
- d) participar en la confección del expediente de habilitación del personal implicado en la seguridad y protección de la información clasificada en el sujeto categorizado de máxima seguridad;
- e) participar en la habilitación del personal implicado en la seguridad y protección de la información clasificada de los sujetos categorizados de seguridad media y básica;
- f) planificar y efectuar controles para comprobar el estado de cumplimiento de las medidas de seguridad y protección de la información clasificada y limitada, en cualquier soporte;
- g) realizar muestreos sistemáticos a la información que se genere en el sujeto en cualquier soporte, con el objetivo de detectar infracciones graves en el uso de la lista interna para la clasificación y desclasificación de la información;
- h) controlar el cumplimiento de las atribuciones y obligaciones de los jefes y personal de la OPCIC y Norma de Control;
- i) asesorar y exigir el cumplimiento de las obligaciones de los portadores;
- j) comprobar que exista la compatibilización con el órgano competente del MININT del sistema informatizado para el registro y control de la información clasificada;
- k) participar en el grupo de trabajo para definir la información limitada y las medidas de su seguridad y protección;
- l) participar en la elaboración de los planes de evacuación para la conservación y destrucción de la información clasificada y limitada ante situaciones excepcionales y de desastre;
- m) trabajar coordinada y sistemáticamente con el responsable de la ciberseguridad, a fin de evitar hechos que atenten contra la integridad, confidencialidad y disponibilidad de la información en las tecnologías de la información y operacionales;

- n) asesorar y controlar el cumplimiento de las medidas de seguridad y protección de la información clasificada y limitada, en cualquier soporte, en eventos nacionales e internacionales que se organicen a su nivel o en los que participe;
- ñ) controlar que los centros de datos, lugares y muebles donde se elabore, procese, tramite, transmita, reproduzca y conserve la información clasificada y limitada en los sujetos, estén aplicadas las medidas de seguridad y protección correspondientes y comprobar su cumplimiento;
- o) revisar de conjunto con los responsables de ciberseguridad y criptografía, las tecnologías de la información que se trasladen al exterior, para comprobar que contienen las informaciones autorizadas y están aplicadas las medidas de seguridad tecnológicas y criptográficas correspondientes;
- p) controlar al cumplimiento de los planes de medidas para la solución de infracciones; y
- q) participar en el esclarecimiento de hechos que constituyan infracciones graves de la seguridad y protección de la información clasificada y limitada, si el jefe lo designa.

Artículo 176. Los administradores de red y responsables de ciberseguridad, en los sujetos categorizados de máxima y media seguridad tienen las atribuciones y obligaciones siguientes:

- a) Velar por la instrumentación, en el esquema de seguridad, de los requisitos establecidos en este Reglamento en la dimensión tecnológica;
- b) activar los mecanismos técnicos y organizativos de respuesta ante incidentes o eventos nocivos de ciberseguridad que se identifiquen;
- c) cumplir con el mecanismo de notificación ante incidentes o eventos nocivos;
- d) contribuir al esclarecimiento de hechos que comprometan la información, sistemas de trabajo y actividades clasificadas;
- e) participar en la elaboración e implementación del esquema de ciberseguridad;
- f) supervisar y evaluar la seguridad de las redes y los riesgos que podrían existir en la infraestructura tecnológica vinculada a la información clasificada, sistemas de trabajo y actividades categorizadas de máxima y media; y
- g) apoyar y asistir técnicamente al órgano competente del MININT en la investigación de infracciones.

Artículo 177. Los portadores de información clasificada y limitada tienen las atribuciones y obligaciones siguientes:

- a) Conocer y cumplir las normas establecidas para la seguridad y protección de la información clasificada y limitada, en cualquier soporte contenidas en el Decreto-Ley, este Reglamento y demás disposiciones complementarias;
- b) firmar la recepción de documentos clasificados y en las entregas y devoluciones exigir la firma de quien los recibe;
- c) clasificar y señalar la categoría de clasificación de la información cuando se elabore un documento o borrador con contenido clasificado, en cualquier soporte, de acuerdo con lo establecido en la lista interna;
- d) impedir que los documentos o borradores contentivos de información clasificada y limitada, en cualquier soporte, sean conocidos por personas no autorizadas;
- e) guardar los documentos clasificados y limitados con las medidas de seguridad requeridas, en cualquier soporte;
- f) elaborar, transmitir y almacenar información clasificada solo en tecnologías de la información con los SPC aprobados y materiales de trabajo autorizados y debidamente controlados;

- g) entregar a la OPCIC o Norma de Control cualquier soporte utilizado como borrador y notificarle las versiones digitales que se conserven en las tecnologías de la información;
- h) velar porque las tecnologías de la información empleadas para elaborar, transmitir y almacenar información clasificada y limitada tengan implementadas las medidas de seguridad criptográficas y protección requeridas;
- i) solicitar a la OPCIC el borrado seguro de la información clasificada y limitada almacenada en las tecnologías de la información;
- j) custodiar documentos clasificados y limitados, medios y materiales que les hayan sido entregados para el trabajo con información clasificada y limitada;
- k) comprobar, antes de transmitir una información clasificada y limitada de forma oral, escrita o automatizada, que el destinatario esté autorizado a tener acceso a ella, las condiciones de privacidad del lugar donde se realice la transmisión y la utilización del medio de protección establecido para ello;
- l) cumplir las medidas de cierre, sellaje y contraseña donde exista información clasificada y limitada, en cualquier soporte;
- m) comprobar que en los locales con sistema automatizado para la detección de intrusos, este activado al concluir el horario de trabajo;
- n) comprobar la integridad en los sistemas de cierre y sellaje;
- ñ) entregar en la OPCIC o Norma de Control los documentos clasificados y limitados, en cualquier soporte, que obren en su poder, antes de salir de vacaciones, por traslado u otros motivos de ausencia temporal o definitiva del puesto de trabajo, y en el caso de viajar al exterior o a su retorno;
- o) entregar de inmediato en la OPCIC o Norma de Control documentos clasificados que haya recibido en otro lugar, en cualquier soporte para su registro y control;
- p) anotar en cada documento clasificado o limitado con carácter personal el número de registro y fecha reflejados en el sobre que lo contengan;
- q) comunicar al jefe inmediato, jefe de OPCIC y jefe de seguridad y protección las personas que no tienen acceso a una información clasificada o limitada y muestren interés en conocerla, así como cuando cometa o conozca de cualquier infracción;
- r) informar al jefe de la OPCIC la pérdida, extravío o destrucción indebida de información clasificada y limitada; y
- s) facilitar la información que se solicite en la ejecución de controles que se realicen por el personal facultado para ello.

Artículo 178. El personal vinculado a las tecnologías operacionales tiene las atribuciones y obligaciones siguientes:

- a) Conocer y cumplir los esquemas de seguridad de las tecnologías que operan;
- b) cumplir las medidas de cierre, sellaje y contraseña de tecnologías clasificadas;
- c) comprobar que en los locales con sistema automatizado para la detección de intrusos, este activado al concluir el horario de trabajo;
- d) comprobar la integridad en los sistemas de cierre y sellaje;
- e) comunicar al jefe de seguridad y protección las personas que no tienen acceso a la tecnología operacional y muestren interés en conocerla, así como cuando cometa o conozca cualquier infracción; y

- f) apoyar y asistir técnicamente al órgano competente del MININT en la investigación de infracciones graves.

Artículo 179. Las personas que cometan o conozcan de infracciones graves de las medidas establecidas para la seguridad y protección de la información clasificada y limitada, están en la obligación de comunicarlo a su jefe inmediato, así como preservar el lugar del hecho si es necesario, hasta tanto se presenten las autoridades competentes.

CAPÍTULO XIII

DE LAS INFRACCIONES QUE AFECTAN LA SEGURIDAD Y PROTECCIÓN DE LA INFORMACIÓN CLASIFICADA Y LIMITADA, LOS SISTEMAS DE TRABAJO Y ACTIVIDADES CATEGORIZADOS DE MÁXIMA SEGURIDAD Y SU INVESTIGACIÓN

SECCIÓN PRIMERA

Disposiciones generales

Artículo 180.1. Constituyen infracciones de la seguridad y protección de la información clasificada y limitada, el incumplimiento de lo dispuesto en el Decreto-Ley 78 de 2023 y en el presente Decreto.

2. Las infracciones conllevan acciones administrativas para su solución en un plazo que no exceda los treinta días.

Artículo 181. Constituyen infracciones graves las que afectan la confidencialidad de la información clasificada, en cualquier soporte, o conducen a la pérdida de su integridad o disponibilidad, siempre que no tipifiquen un delito; estas son:

- a) Pérdida y extravío de información clasificada;
- b) generar documentos contentivos de información clasificada sin identificar como tal;
- c) desclasificar informaciones sin estar facultado para ello;
- d) entregar o divulgar información clasificada a personas que no tengan acceso autorizado a esta;
- e) reproducir o extraer información clasificada, sin autorización, ni control;
- f) dañar o modificar la confidencialidad, integridad y disponibilidad de información clasificada y sistemas de trabajo y actividades categorizadas de máxima;
- g) usar medios abiertos para la transmisión de información clasificada sin las medidas de protección criptográficas exigidas por el MININT y sin la autorización correspondiente;
- h) tramitar información clasificada por plataformas digitales no autorizadas por el MININT;
- i) conectar tecnologías de la información controladas para el trabajo con la información clasificada, con o sin información clasificada, a redes de datos con alcance global;
- j) procesar, reproducir y conservar información clasificada en las tecnologías de la información no autorizadas y en las autorizadas que no tengan la protección criptográfica;
- k) trasladar dentro del país o hacia el extranjero documentos clasificados en cualquier soporte, sin autorización o sin las medidas de protección establecidas;
- l) destruir y borrar información clasificada sin la autorización correspondiente y el debido control;
- m) no tener implementado el sistema de registro, tramitación y control de la información clasificada en cualquier soporte o teniéndolo, existir información clasificada sin encontrarse debidamente registrada;

- n) entregar o recibir información clasificada sin mediar firma;
- ñ) no definir el acceso a la información clasificada, o definirlo sin precisar las informaciones a las que se autoriza a cada persona;
- o) incumplir las medidas de sellaje en muebles y locales contentivos de información clasificada y en sistemas de trabajo y actividades categorizadas de máxima;
- p) conservar información clasificada sin las medidas de protección establecidas;
- q) no aplicar los procedimientos establecidos para la investigación de infracciones graves, que afectan la seguridad y protección de la información clasificada y en sistemas de trabajo y actividades categorizados de máxima; y
- r) no realizar las correspondientes acciones administrativas en el plazo establecido para solucionar las infracciones.

SECCIÓN SEGUNDA

Sobre la investigación de infracciones graves

Artículo 182.1. Al conocer la ocurrencia de una infracción grave, el personal que lo detecte o tenga conocimiento de esta, informa de inmediato al jefe de seguridad y protección, jefe de OPCIC o Norma de Control o jefe del sujeto.

2. De ser posible, se preserva el lugar del hecho hasta que se presenten las autoridades estatales y del MININT competentes.

Artículo 183.1. El jefe de seguridad y protección analiza la información primaria, retroalimenta al jefe del sujeto e informa al órgano competente del MININT, salvo en los casos de los incisos m), n), ñ), o), p), q) y r), definidos en el Artículo 181, las cuales son reportadas a consideración del jefe, según la afectación ocasionada.

2. Las infracciones graves recogidas en los incisos m), n), ñ), o), p), q) y r) del citado Artículo 181, no informadas al órgano competente del MININT, por ser mínima la afectación producida, deben corregirse por el jefe del sujeto en un plazo que no exceda los treinta días.

Artículo 184. El jefe de seguridad y protección garantiza que el contenido de la información primaria contemple infracción: títulos o asuntos, registros, número de ejemplares y clasificación de la información, sistema de trabajo y actividades que contiene afectación, soporte en que se encuentra y si estaba con la protección criptográfica aprobada; lugar de ocurrencia; fecha en que se detectó; forma de detección; nombre, cargo y fecha de la persona que informa para la toma de decisiones y facilitar la investigación.

Artículo 185.1. El jefe del sujeto, al conocer la infracción grave, procede a constituir la comisión para la investigación y esclarecimiento, en lo adelante, comisión investigadora, y designa quien la preside a la brevedad posible.

2. La comisión investigadora se integra por al menos tres personas designadas por el jefe del sujeto, que tienen acceso a la información clasificada y limitada y sus sistemas de trabajo y actividades, donde se incluye al jefe de OPCIC o Norma de Control; en ningún caso pueden estar vinculadas con el hecho.

Artículo 186. La comisión investigadora tiene la responsabilidad de comprobar lo siguiente:

- a) Fecha en que se detectó y lugar de ocurrencia;
- b) infracciones graves cometidas;
- c) títulos o asuntos, registro, número de ejemplares y categoría de clasificación de la información, sistema de trabajo y actividades que contiene afectación, soporte en que se encuentra, protección criptográfica y forma de detección;

- d) daño ocasionado por la infracción, en caso de información clasificada determinar la correcta clasificación y su vigencia;
- e) amenazas y riesgos que dieron origen a la infracción; definir autores y responsables;
- f) antecedentes de infracciones graves similares, de los autores y responsables, del soporte o lugar; y
- g) otros elementos que aprecie conveniente esclarecer o definir para arribar a conclusiones y propuestas concretas.

Artículo 187.1. La comisión investigadora está facultada para entrevistarse con cada una de las personas que puedan aportar informaciones esclarecedoras sobre la infracción, y puede realizar la revisión de registros, controles, expedientes, soportes digitales, archivos, muebles, locales que resulten necesarios en el esclarecimiento de la infracción.

2. De no poder determinar con exactitud cómo se produjo la infracción, debe elaborar una versión de los hechos con los elementos recogidos en la investigación.

Artículo 188.1. La comisión investigadora dispone de hasta quince días para la investigación, que concluye con la presentación al jefe del sujeto de un informe final con el resultado de los aspectos trabajados en el proceso investigativo, conclusiones y propuesta de medidas disciplinarias a aplicar a los responsables directos y colaterales de las infracciones graves.

2. Cuando la comisión investigadora determina la posible existencia de delito, propone la ejecución de la denuncia ante el órgano fiscal por la administración.

Artículo 189. Una copia de este informe se envía al órgano competente del MININT, firmado por el jefe del sujeto, en un término que no exceda los treinta días de creada la comisión.

Artículo 190.1. El órgano competente del MININT tiene la facultad de proponer la modificación de las medidas disciplinarias a aplicar a los responsables directos de infracciones graves, en un plazo de hasta cinco días de recibida la copia del informe.

2. De no responder el órgano competente del MININT en dicho plazo, se entiende que está conforme con la propuesta de medida disciplinaria.

SECCIÓN TERCERA

De la aplicación de medidas disciplinarias

Artículo 191. Las propuestas de medidas disciplinarias a aplicar a los trabajadores y cuadros que se identifiquen responsables de infracciones graves, deben estar en correspondencia con la categorización del sujeto, el valor de la información, sistema de trabajo, actividad comprometida y el daño ocasionado.

Artículo 192. Ante las infracciones graves detectadas, las medidas disciplinarias a aplicar se corresponden con la legislación vigente en esta materia, y son las siguientes:

- a) De la Ley 116, “Código de Trabajo”, de 20 de diciembre de 2013, las previstas en el Artículo 149, incisos a), c), d), e) y f).
- b) Del Decreto-Ley 67 sobre las relaciones de trabajo de los funcionarios y otros trabajadores designados, de 22 de noviembre de 2022, las previstas en el Artículo 20.1, incisos a), c), d), e) y f).
- c) Del Decreto-Ley 13, “Sistema de trabajo con los Cuadros del Estado y del Gobierno y sus reservas”, de 18 de junio de 2020, las previstas en el Artículo 30.1, incisos a), c), d), e) y f).

Artículo 193. En los casos en que se aplica la medida disciplinaria de separación definitiva de la entidad, se le apercibe al infractor que la revelación adicional de la

información clasificada que hasta ese momento conozca, puede ser objeto de sanción penal.

Artículo 194.1. La notificación de la medida disciplinaria al responsable se ejecuta por el jefe del sujeto en un plazo de hasta cinco días posteriores a la conformidad del MININT.

2. En los casos de los sujetos categorizados de máxima seguridad la notificación se realiza en presencia de especialista del órgano competente del MININT.

DISPOSICIONES TRANSITORIAS

PRIMERA: La capacitación del personal que participa en la implementación de este Reglamento se realiza por el órgano competente del MININT, en los noventa días posteriores a la aprobación de la norma

SEGUNDA: El proceso de categorización de los sujetos, sistemas de trabajo y actividades comienza a partir de la capacitación en cada uno de ellos y se extiende hasta un año.

TERCERA: Una vez aprobada la categorización, los jefes facultados, en un plazo de hasta cuarenta y cinco días, proceden con la presentación y aprobación de esquemas de seguridad y habilitación del personal implicado en la seguridad y protección de la información clasificada, según lo establecido en este Reglamento.

DISPOSICIONES FINALES

PRIMERA: Se facultan a los ministros de las Fuerzas Armadas Revolucionarias y del Interior, según corresponda, para adecuar en lo que resulte necesario, las disposiciones establecidas en el presente Decreto, en correspondencia con las particularidades de las funciones, misiones y características de la información clasificada y limitada de dichos organismos.

SEGUNDA: Derogar las disposiciones normativas siguientes:

1. Acuerdo 6221 del Comité Ejecutivo del Consejo de Ministros, que aprueba y dispone la entrada en vigor del “Reglamento de la Comisión Estatal para la Clasificación y Desclasificación de la Información Oficial”, de 11 de enero de 2008.
2. Resolución 6 del ministro del Interior, que pone en vigor el “Reglamento sobre la Seguridad Informática”, de 18 de noviembre de 1996.
3. Resolución 1 del ministro del Interior, que pone en vigor el “Reglamento sobre la seguridad y protección de la información oficial”, de 26 de diciembre de 2000.
4. Instrucción 2 del viceministro del Interior, “Que establece las normas y procedimientos para el registro, tramitación y control de la Información Clasificada”, de 26 de enero de 2001.
5. Instrucción 1 del viceministro del Interior, “Que define las infracciones graves que afectan la seguridad y protección de la Información Oficial Clasificada y establece los procedimientos para su investigación por los órganos, organismos, entidades y sus dependencias”, de 6 de febrero de 2007.
6. Instrucción 4 del viceministro del Interior, “Que establece la metodología para el trabajo con las Listas General e Interna para la Clasificación y Desclasificación de la Información Oficial y la elaboración o actualización de las Listas Internas en los órganos, organismos y entidades nacionales”, de 16 de junio de 2012.

TERCERA: El presente Decreto entra en vigor a los noventa días posteriores a su publicación en la Gaceta Oficial de la República de Cuba.

PUBLÍQUESE en la Gaceta Oficial de la República de Cuba.

DADO en el Palacio de la Revolución, en La Habana, a los 12 días del mes de julio de 2024.

Manuel Marrero Cruz

LIBRO DE REGISTRO

LIBRO DE REGISTRO

[illegible]

Indicadores:

1. Número de registro que le corresponde al documento, de forma única y consecutiva, tanto para los generados como recibidos.
2. Lugar de procedencia del documento, sea del sujeto (viceministerio, departamento) o de otro.
3. Número de registro de procedencia.
4. Título o asunto de los documentos que se reciban o generen. Esta columna también se utiliza para reflejar la fecha en que se registran, lo que hace una sola vez al día y se sitúa en el centro de la columna.
5. Categoría de clasificación del documento; se ponen las iniciales SE, S, C, SP.
6. Número de control del material utilizado, como son cuadernos de trabajo, libreta taquigráfica, computadora, memoria flash.
7. Número de los folios del material utilizado para la elaboración del borrador o versión.
8. Cantidad de ejemplares que se reciben o generan.
9. Número del ejemplar que se recibe o genera.
10. Número de hojas o páginas del documento. Cuando es página se especifica: pág.
11. Firma de la persona que se responsabiliza con la destrucción del borrador o versión digital y la fecha en que se realiza.
12. Cargo y lugar a donde se envía cada ejemplar; en el particular de más de cinco ejemplares, se plasma SLD y cuando los ejemplares se reproducen o imprimen en imprenta se plasma OT (Orden de Trabajo)
13. Número del comprobante o folio donde se entrega el documento.
- 14 al 16. Firma y fecha como constancia de entrega de los documentos impresos o digitales los destinatarios internos que se agrupan por áreas.
17. Cantidad de ejemplares a reproducir. Se efectúa la anotación en la línea correspondiente al ejemplar que se utiliza para realizar la reproducción, de no estar desglosados como ocurre en los casos de las listas de destinatarios, se hace en la línea donde se registró el documento.
18. Cantidad de hojas o páginas que se reproducen.
19. Firma de la persona que autoriza la reproducción.
20. Número de la lista de destinatarios o comprobante de entrega de documentos, cuando no supera los dos ejemplares, donde se señala la distribución de la reproducción realizada.
21. Número del expediente, depósito o material donde se conserva el ejemplar del documento en el archivo o computadora y la fecha en que se realiza.
22. Firma de la persona que autoriza la desclasificación y fecha en que se desclasifica el documento.
23. Número del acta por la cual se destruyen los ejemplares.
24. Cualquier otra anotación o aclaración que se entienda necesaria referente a cada ejemplar.

Al comenzar a hacerse las anotaciones, se pasa una raya debajo del último registro y se sitúa en el centro la fecha para diferenciar cada día.

ANEXO II

CONTROL DE LOS MATERIALES DE TRABAJO

Control de los materiales de trabajo: Este modelo sirve para controlar todos los materiales utilizados en el trabajo con la información clasificada tales como: cuadernos de trabajo, libros de registro o control, hojas foliadas, sellos personales, casetes, memorias flash, discos externos, tablets, laptop, computadoras, impresoras y otros. En todos los casos se lleva por la OPCIC o Norma de Control.

CONTROL DE LOS MATERIALES DE TRABAJO

Datos del material (1)			Lugar y persona a quien se entrega (2)		Recibido por: (3)		Devuelto a: (4)		Destino (5)		Observaciones (6)
Tipo	No.	Folios			Firma	Fecha	Nombre Apellidos y Firma	Fecha	Lugar	Fecha	

Indicadores:

1. Se anota el tipo de material, el número que le corresponde y número del primer y último folio que contiene de acuerdo con el material que se controle.
2. Nombre y apellidos de la persona a quien se entrega el material y lugar donde labora.
3. Firma de la persona a quien se entrega el material y fecha en que se efectúa la entrega.
4. Nombre, apellidos y firma de la persona que en la OPCIC recibe el material cuando es devuelto y fecha en que se efectúa la devolución.
5. Se anota el destino posterior del material devuelto, y la fecha en que se realiza el envío.
6. Se anota cualquier aclaración que resulte necesaria, en el particular de las tecnologías de la información, esta casilla es utilizada para plasmar el número de serie de fabricación, como identificador único del medio.

ANEXO III

ORDEN DE TRABAJO

Orden de trabajo: Sirve de solicitud y control de los documentos y materiales que se envían a imprenta para su reproducción.

Modelo No. 9

ORDEN DE TRABAJO											
(1) ASUNTO:			(3) CLASIFICACION			(4) GRADO DE URGENCIA					
(2) UNIDAD EJECUTORA			(6) NUMERO DE HOJAS O PAGINAS			(7) FECHA					
(5) CANTIDAD			(6) NUMERO DE HOJAS O PAGINAS			DIA		MES		ANO	
(8) TIPO DE TRABAJO QUE SE SOLICITA											
(9) BORRADORES Y MATERIALES QUE SE ENTREGAN					(10) CUSTODIO DESIGNADO						
					NOMBRE Y APELLIDOS		CARGO				
					(11) MATERIALES DE DESECHOS						
(12) Ejecutor		(13) Autorizado		(14) Recibido en Unidad ejecutora			(15) Registro		(16) Trabajo terminado recibido por:		
				Nombre y apellidos			Fecha		Nombre y apellidos		Fecha
				Cargo			D M A		Cargo		D M A
				Firma					Firma		

Indicadores:

1. Título o asunto de que se trate el material que se solicite.
2. Nombre de la unidad ejecutora que efectúa el trabajo de impresión o reproducción.
3. Categoría de clasificación que posee el documento o material.
4. Grado de urgencia que requiere.
5. Cantidad de ejemplares que se solicitan
6. Número de hojas o páginas de cada ejemplar.
7. Día, mes y año en que se emite la orden.
8. Breve descripción del tipo de trabajo que solicita.
9. Descripción de los borradores, documentos y materiales, así como prototipos que se entregan a la unidad ejecutora, señala número y folios de estos.
10. Nombre, apellidos y cargo de la persona que se designe como custodio durante el proceso de impresión o reproducción.
11. Descripción de los documentos y materiales, desechos durante el proceso de impresión o reproducción.
12. Firma del ejecutor del trabajo.
13. Firma del funcionario responsable que autoriza la orden de trabajo.
14. Firma de la persona autorizada en la unidad ejecutora que recepciona la orden de trabajo, así como cuño gomígrafo que certifica dicha unidad.
15. Número de registro que se le otorgó al documento.
16. Nombre y apellidos, cargo y firma del custodio designado en conformidad con la ejecución del trabajo y los desechos señalados y fecha de recibido.

ENTREGA DE CORRESPONDENCIA INTERNA

En el área el modelo de entrega de correspondencia interna consigna los documentos impresos o digitales que se generen o reciban en el área y se señala dónde se encuentra el ejemplar digital o de archivo.

[illegible]

1. Número de registro del documento.
2. Categoría de clasificación del documento.
3. Número del o los ejemplares.
4. Cantidad de hojas o páginas de cada ejemplar.
5. Título o asunto del documento que recibe o envía; en este último caso el área a la que se remite el documento para su distribución.
6. Nombre, apellidos y firma de la persona que recibe y fecha en que recepciona, donde dice: archivo se pone el número del expediente, depósito, tecnología de la información o cualquier otro dato que exprese dónde está el documento físico o digital.
7. Se anotan las aclaraciones que resulten necesarias.

Cuando el área entregue a la OPCIC o Norma de Control, los documentos generados, hace constar la entrega de borradores y lista de destinatarios en la columna de “Observaciones”.

- Puede utilizarse un mismo folio para la entrega de distintos documentos a uno o varios destinatarios, siempre que estos respondan al control de la propia OPCIC o Norma de Control.

En todos los casos se especifican en “Observaciones” las causas por las que subrayan los datos.

1. Número de registro del documento, expediente, depósito o material de trabajo.
2. Número del primer y último folio que le corresponde al documento en su orden consecutivo en el expediente; cuando se preste el expediente, depósito, o material se deja en su lugar la relación interior, velando por su actualización una vez entregado.

- 3. Nombre y apellidos, firma y fecha de la persona con acceso a la cual se le entrega el documento, expediente, depósito o material de trabajo.
- 4. Fecha convenida con el portador para la devolución del documento, expediente, depósito o material; si el usuario solicita prórroga se sitúa la nueva fecha en el renglón a continuación o en el que se encuentre vacío señala en “Observaciones” que es una prórroga.
- 5. Nombre y apellidos, firma y fecha de la persona que en archivo recepciona el documento, expediente, depósito o material.
- 6. Cualquier aclaración que resulte necesario realizar.

ANEXO VIII

NIVEL PERSONAL DE ACCESO Y ACTA DE RESPONSABILIDAD

Nivel personal de acceso y acta de responsabilidad: Se confecciona a cada persona con acceso autorizado a la información clasificada con el objetivo de controlar y conocer a la que tiene acceso, así como su compromiso de no divulgarla.

NIVEL PERSONAL DE ACCESO Y ACTA DE RESPONSABILIDAD

(1) Organismo					
(2) Área o Dependencia					
(3) Nombre y apellidos				(4) Ciudadanía	
(5) Cargo		Con acceso hasta categoría (6)		Fecha (7)	
				Desde	Hasta
(8) Propuesto por:					
Nombre y apellidos		Cargo	Firma	Fecha	
(9) Autorizado por:					
Nombre y apellidos		Cargo	Firma	Fecha	
Acceso a:					
Información (10)	No. (11)	Cat (12)	Fecha (13)		Observaciones (14)
			Desde	Hasta	

(15) OBSERVACIONES:

(16) ACTA DE RESPONSABILIDAD

El que suscribe _____

trabajador de _____ me comprometo a no divulgar la información clasificada que sea de mi conocimiento, así como cumplir todo lo establecido para su seguridad y protección, por lo cual firmo la presente.

Firma _____ Fecha _____

Indicadores:

- 1. Nombre del sujeto.
- 2. Área o dependencia donde trabaja la persona.
- 3. Nombre y apellidos de la persona.
- 4. Ciudadanía de la persona.

- 5. Cargo que ocupa.
- 6. Categoría más alta a la que tiene acceso.
- 7. Fecha desde y hasta que cese el acceso a la categoría de clasificación que se le otorgue, considerando que puede variar o no.
- 8. Nombre y apellidos, cargo y firma del funcionario que propone otorgar el acceso y fecha en que realiza la propuesta.
- 9. Nombre y apellidos, cargo y firma del funcionario que otorga el acceso y fecha en que lo realiza.
- 10. Se detallan todas las informaciones que se generan y reciben en el área, o que por su cargo tenga acceso.
- 11. Número que le corresponde a la información en la lista interna para la clasificación y desclasificación de la información.
- 12. Categoría de clasificación de la información.
- 13. Fecha desde que comienza el acceso hasta que cesa. Debe tenerse en cuenta que la información puede variar de acuerdo con el cargo que ocupa la persona.
- 14. Observaciones que resulten necesarias hacer sobre el motivo por el cual se cancela el acceso a una información o categoría de clasificación.
- 15. Cualquier aclaración que se necesite realizar.
- 16. Se refleja el nombre, apellidos y centro de trabajo del funcionario al que se le otorga el acceso, así como la firma de este y la fecha.

ANEXO IX
PROPUESTA DE CLASIFICACIÓN, MODIFICACIÓN
O DESCLASIFICACIÓN DE LA INFORMACIÓN

Propuesta de clasificación, modificación o desclasificación de la información: Se utiliza para realizar las propuestas de clasificación, modificación o desclasificación de la información.

+

CLASIFICACIÓN _____		Referida a:	
Modificación _____		Denominación Lista General _____	
Desclasificación _____		Información Lista Interna _____	
(1)		Anexo _____	
		Categoría de clasificación _____	
		Período de Permanencia _____	
(2)			
Organismo: _____		Fecha: _____	
Dependencia: _____		(4)	
No. (5)	Denominación, Información o Indicador (6)	Categoría (7)	
		Período de Permanencia	
Fundamentación de la Propuesta (8)			
Propuesto por: (9) _____		Firma	
Visto bueno: (10) _____		Firma	
Aprobado por: (11) _____		Firma	
Nombre, apellidos y cargo			
Nombre, apellidos y cargo			
Nombre, apellidos y cargo			

Indicadores:

1. Marcar con una (x) a cuál de los casos indicados se refiere la propuesta.
2. Marcar con una (x) a cuál de los aspectos indicados se refiere la propuesta.
3. Reflejar el nombre del sujeto y la dependencia que realiza la propuesta.
4. Fecha en que se realiza la propuesta.
5. Número de la denominación, información o indicador a que se refiere la propuesta; cuando se trate de una inclusión este espacio se deja en blanco.
6. Enunciado de la denominación, información o indicador que se propone clasificar, modificar o desclasificar.
7. Cuando se trate de una propuesta de clasificación o modificación, se refleja en la forma que debe redactarse la denominación, información y categoría que se propone; cuando se refiere a una desclasificación, se pone la palabra “desclasificar”.
8. Reflejar los elementos de juicio y criterios que motivan la propuesta.
9. Nombre, apellidos, cargo y firma del funcionario que propone.
10. Nombre, apellidos, cargo y firma del representante de la comisión estatal para la clasificación y desclasificación de la información clasificada.
11. Nombre, apellidos, cargo y firma del jefe del sujeto.

ANEXO X**ORDEN Y CONTENIDO DEL EXPEDIENTE DE HABILITACIÓN
DEL PERSONAL DE PROTECCIÓN DE LA INFORMACIÓN**

- Tres (3) fotos 1x1 actualizadas. Una foto ubicada en el lateral derecho superior de la carátula del expediente; una foto en la planilla de entrevista inicial; una foto para el carné o solapín de identificación como personal de seguridad en los sujetos que lo tengan instituido.
- Remisión del expediente. Firmada por el jefe del sujeto.
- Formulación de la propuesta. Debe estar firmada y acuñada por el jefe del órgano de seguridad y protección, dirigida al jefe del órgano competente del MININT en La Habana o a los jefes de la Contrainteligencia en el caso de las provincias. En la propuesta se debe especificar si el cargo es de nueva creación o si estaba ocupado por otro compañero; en este caso, si estaba aprobado por el MININT, poner nombres y apellidos, número de aprobado y año, así como las causas por lo que ya no ocupa el cargo, lo cual permite la actualización sistemática de los cargos aprobados y pendientes a aprobar.
- Informe conclusivo o resumen del caso. Constituye uno de los documentos principales del expediente, por lo que debe estar debidamente firmado y acuñado por el jefe del sujeto. En el informe conclusivo o resumen del caso, se exponen los resultados de la entrevista inicial del personal que se propone, significándose aquellas cuestiones que a juicio del jefe, o persona designada de seguridad y protección que se ocupa de este proceso en cada sujeto, constituyen posibles invalidantes, que solo puede decidir el órgano rector.

Considerar en el análisis de cada caso, posibles indicios o manifestación de nepotismo en las futuras relaciones laborales del candidato con familiares, parientes o allegados que ocupen cargos de dirección en el mismo sistema, haciendo referencia sobre el particular en el contenido del informe resumen conclusivo.

Tener en cuenta que este informe debe ser un reflejo de la personalidad del sujeto, ya que para ser aprobado a este nivel se requiere disponer de la mayor cantidad posible de

información sobre la persona, por ser esta la alternativa más viable para ser justos a la hora de decidir su aprobación a ocupar los cargos para los que se proponen; y en él debe reflejarse de forma sintetizada la valoración objetiva de las conductas en los momentos siguientes:

Datos generales del candidato

- Resultados de la entrevista inicial, significar si la persona ha sido detenida, investigada o sancionada por la comisión de algún delito; si ha solicitado visa para abandonar legalmente el país. Exponer los criterios al respecto.
- Si posee el nivel requerido para el cargo y de no poseerlo, las razones que, a juicio del promovente, le permiten ocupar el cargo.
- Trayectoria estudiantil.
- Trayectoria laboral.
- Trayectoria política revolucionaria.
- Resultado del chequeo pre-empleo.
- Resultado de Antecedentes Penales.

Nota: Los jefes, especialistas o técnicos de seguridad y protección, en sus diferentes niveles, tienen la obligación de intervenir, controlar y supervisar los procesos de habilitación del personal que se proponga a la aprobación del MININT y debe estar, a su vez, aprobados por este órgano (debiendo identificarse con su número de orden de aprobación incluyendo el año).

De no cumplirse con esta indicación y no exista razón justificada, el MININT no tramita los expedientes presentados.

Esta medida se establece para garantizar la adecuada confiabilidad y calidad de los procesos de habilitación del personal de protección de la información clasificada y sus niveles de competencia.

- **Planilla de solicitud de empleo.** Debe incluir una foto actualizada de la persona. En la entrevista inicial a los candidatos se deben conocer y documentar las motivaciones e intereses de ingresar al cargo, obteniendo la mayor cantidad de información del entrevistado a través de sus respuestas y el lenguaje corporal, a fin de lograr una imagen primaria del candidato durante la entrevista, tanto por su presencia física, como por el perfil de su personalidad, buscando conocer su forma y manera de pensar.

Deben obtenerse evidencias e información que permitan complementar la obtenida por otras vías o documentos; aplicación de procesos, sanciones judiciales o administrativas, medidas de detención o investigación por parte de la PNR y elementos que puedan arrojar más información sobre el candidato, recogiendo los datos siguientes:

1er apellido		2do apellido		Nombres			
Natural de:		Ciudadanía:		No. CI.			
Padre:		Madre:		Edad:		Sexo:	
Estado civil	Soltero:	Casado:	Concubinato:		Viudo:		
Piel:	Ojos:	Peso:	Pelo:	Estatura:			
Jubilado (fecha):		FAR		MININT		Grado militar:	
Desmovilizado (fecha):		FAR		MININT		Grado militar:	
Pasó el Servicio Militar: Sí		fecha		No		Motivos:	
Integración a Organizaciones		PCC	UJC	ACRC	CDR	FMC	MTT BPD
Misiones internacionalistas: País		Fecha		País		Fecha	
Dirección particular:							
Municipio:				Teléfono para localizarlo:			
Personas que conviven con Ud. (de no tener señalar no)							
Nombres y apellidos	Filiación	Edad	Trabaja/Estudia		Integración social/política		
Centros educacionales donde ha cursado estudios							
Años							
Nombre del centro		Dirección			Desde:		Hasta:
Centros de trabajo donde ha laborado							
Años							
Nombre del centro		Dirección			Desde:		Hasta:
Ha sido detenido o sujeto a proceso investigativo por la PNR:							
Ha sido procesado o sancionado por Tribunales Militares, Judiciales o Laborales:							
Familiares en el exterior		No	Sí	Filiación:		País:	
Ha solicitado la salida temporal o permanente del país:							
Ha prestado servicios en la actividad con anteriormente: Sí No							
Cargo que ocupaba:				Dónde:			
Por qué lo dejó:							
Certifico que las afirmaciones hechas en esta solicitud son ciertas:							
Firma del candidato:				Entrevistador:			

(Cualquier otro dato de interés al dorso)

- **Autobiografía del candidato.** Elaborada por el candidato, debe contener la mayor información posible, caracterizar la vida estudiantil, laboral, política, social y económica de la persona que se propone.
 - Debe comenzar su autobiografía indicando fecha y lugar de nacimiento, nombre de los padres, procedencia social, fechas cronológicas de su trayectoria escolar indicando nombre y ubicación de los centros de enseñanza donde ha cursado estudios, participación en actividades socioculturales, deportivas o políticas durante ese período; integración, distinciones o estímulos recibidos.
 - Cumplimiento del servicio militar, lugar y fecha; de no haberlo pasado indicar motivo.
 - Trayectoria laboral o militar, indicando en orden cronológico fechas de inicio y terminación en cada lugar, nombre del centro o institución militar, cargos ocupados, causas de la baja.
 - En los casos de haberse dedicado al trabajo por cuenta propia, especificar la actividad a que se dedicó y su autorización por la ONAT; integración política y social durante ese período.
 - Integración a organizaciones políticas, sociales y de masas a las que pertenece, actividades sociopolíticas del candidato y de los familiares que conviven con este.
 - Argumentar motivaciones por las cuales interesa incorporarse al cargo.
 - Firma del candidato.

- **Certificación del nivel educacional del candidato.** Debe responder a los requisitos del cargo a ocupar, según lo establecido por el MTSS y el MININT, para los casos que no posean el nivel requerido, se dispondrá una excepcionalidad.

La certificación de estudios terminados puede ser presentada en documento original para una mejor comprobación, en caso de fotocopia, tiene que aparecer nombre completo y la firma de la persona que tuvo acceso al certificado original, así como el cuño de la entidad interesada y fecha en que fue realizada la comprobación.

En los casos de estudios en el extranjero, la certificación debe ser homologada por el MES o MINED que atiende estos casos, según corresponda, lo cual es aplicable a los cursos militares en los que no se especifique el nivel educacional alcanzado.

- **Certificación de antecedentes penales.** Solo es válido si no ha excedido el año de expedición; no presentar fotocopia.

- **Chequeo médico pre-empleo.** Acreditando el estado de salud del interesado, indicando si el candidato está apto físicamente para ocupar el cargo; puede adjuntarse resultado de test psicométricos, para tener mayor información sobre el candidato. No presentar fotocopia.

- **Verificaciones en el lugar de residencia del interesado y en el centro de trabajo o estudio de donde procede.** Con tres personas como mínimo en cada caso; debe reflejarse nombre y apellidos, cargo, militancia si la tiene y dirección de los informantes, así como número de teléfono si lo posee.

En las verificaciones en el lugar de residencia debe profundizarse en aspectos como integración familiar, participación en actividades sociales y políticas, modo de vida, características de las personas con las que se reúne, etcétera.

En el centro de trabajo anterior, debe ser verificado con los factores administración, PCC y sección sindical, firmado y acunado; en los casos en que el candidato ocupó con anterioridad, algún cargo vinculado a la actividad de seguridad y protección, debe aparecer en el expediente una evaluación del período en que desempeñó estas funciones y los motivos por los cuales dejó de hacerlo, firmada por la administración, sindicato y PCC de la entidad donde trabajó y el cuño correspondiente.

En los casos en que el candidato alega haber trabajado por cuenta propia, debe solicitarse, entre otras acciones de comprobación, la documentación que establece la ONAT para el desempeño de esta modalidad laboral.

De proceder de un centro de estudios, se verifica con la dirección de la institución, de donde procede; tener en cuenta no exista relación de parentesco del verificador con el candidato.

Con relación a las verificaciones realizadas por detectives o verificadores de SEPSA, se aceptan sin informar las fuentes de información, siempre que se cumplan los demás requerimientos, estén acreditadas con el cuño o logotipo de la entidad, en fecha acorde a la propuesta y no ser fotocopiadas.

En los casos para los cuales se determinan cambios de cargos dentro del sistema de seguridad y protección o traslados de instalación u objetivo, pero dentro del ámbito de la empresa o grupo empresarial, solo se necesita actualizar el informe resumen conclusivo, la verificación o evaluación de su desempeño en el cargo anterior y la remisión correspondiente.

Si el cambio de cargo o traslado se realiza posterior a un año de su aprobación en el cargo anterior, debe incluir certificación de antecedentes penales.

ANEXO XI
PLAN DE MEDIDAS
PLAN DE MEDIDAS PARA LA SOLUCIÓN DE INFRACCIONES

Nombre del sujeto					
No. (1)	Infracción (2)	Medidas (3)	Fecha de Cumplimiento (4)	Ejecuta (5)	Controla (6)

Fecha del documento (7)

Nombre, apellidos, cargo y firma del jefe del sujeto (8)

Indicadores:

1. Número de la infracción.
2. Descripción de la infracción.
3. Medidas a aplicar y definir el área afectada.
4. Fecha de cumplimiento de la medida.
5. Nombre y cargo del que ejecuta la medida.
6. Nombre y cargo del que controla el cumplimiento de la medida.
7. Fecha de elaboración del documento.
8. Nombre, apellidos, cargo y firma del jefe del sujeto.