

**REPÚBLICA BOLIVARIANA DE VENEZUELA**  
**MINISTERIO DEL PODER POPULAR PARA LA DEFENSA**  
**DESPACHO DE LA MINISTRA**

Caracas, 01 ABR 2014

203° y 155°

**RESOLUCIÓN 004263**

La Ministra del Poder Popular para la Defensa, ALMIRANTA EN JEFA CARMEN TERESA MELÉNDEZ RIVAS, nombrada mediante Decreto N° 214 de fecha 05 de julio de 2013, publicado en la Gaceta Oficial de la República Bolivariana de Venezuela N° 40.204 de fecha 10 de julio de 2013, en ejercicio de las atribuciones que le confiere el artículo 77 numeral 19 del Decreto N° 6.217 con Rango, Valor y Fuerza de Ley Orgánica de la Administración Pública de fecha 31 de julio de 2008, en concordancia con lo establecido en el artículo 11 del Decreto con Rango, Valor y Fuerza de Ley Orgánica de la Fuerza Armada Nacional Bolivariana de fecha 09 de marzo de 2011, publicado en la Gaceta Oficial de la República Bolivariana de Venezuela Extraordinaria N° 6.020 de fecha 21 de marzo de 2011, se dictan las siguientes,

**NORMAS DEL RÉGIMEN ESPECIAL DE SEGURIDAD DE LA FUERZA  
ARMADA NACIONAL BOLIVARIANA**

**CAPÍTULO I**  
**Disposiciones Generales**

**Objeto**

**Artículo 1.** Las presentes normas tienen por objeto establecer las directrices y procedimientos a seguir, para proteger las informaciones, documentos y materiales clasificados; así como, el régimen de seguridad de la Fuerza Armada Nacional Bolivariana.

**Régimen Especial de Seguridad**

**Artículo 2.** El régimen especial de seguridad es el sistema de regulaciones y medidas organizativas, educativas, de seguridad física, tecnológica y de control que se establecen e implantan para garantizar la seguridad, manejo y protección de la información oficial; así como, el régimen de seguridad de las unidades militares y dependencias administrativas de la Fuerza Armada Nacional Bolivariana, este incluye:

1. La seguridad, manejo y protección de la información oficial.
2. El régimen de seguridad.

CSBO/

/...

**La seguridad, manejo y protección de la  
Información oficial**

**Artículo 3.** La seguridad, manejo y protección de la información oficial comprende la clasificación y reclasificación de las informaciones escritas o electrónicas, las medidas de seguridad con las informaciones clasificadas en cualquier soporte, la seguridad informática, la protección electromagnética, la protección criptográfica, las instrucciones operativas de comunicaciones e instrucciones permanentes de comunicaciones, la compartimentación y el conjunto de regulaciones y medidas que evitan el conocimiento o divulgación no autorizada de la información oficial.

**El régimen de seguridad**

**Artículo 4.** El régimen de seguridad comprende el control de acceso, las medidas de seguridad física, tecnológica y el servicio de guardia de las unidades militares y dependencias administrativas de la Fuerza Armada Nacional Bolivariana.

**La información oficial**

**Artículo 5.** La información oficial es aquella que posee una unidad militar, dependencia administrativa, persona natural o jurídica residente en el territorio nacional o en representaciones diplomáticas en el exterior, capaz de proporcionar directa o indirectamente, datos o información que reflejen alguna actividad de la Fuerza Armada Nacional Bolivariana, o reconocida por ésta y que puedan darse a conocer de cualquier forma perceptible por la vista, el oído o el tacto. La información oficial constituye un bien de la Fuerza Armada Nacional Bolivariana y no un bien personal.

**Responsabilidad**

**Artículo 6.** Los Comandantes de unidades y jefes de dependencias administrativas a todos los niveles, tienen la responsabilidad de crear las condiciones que garanticen el cumplimiento de las medidas del régimen especial de seguridad en sus unidades militares y dependencias administrativas subordinadas.

El personal militar y civil autorizado para tener acceso a las informaciones y materiales clasificados, será individualmente responsable del cumplimiento de las medidas de seguridad, vigilancia, discreción y cuidado establecidas en las presentes normas.

**Estructura y atribuciones del Régimen  
Especial de Seguridad**

**Artículo 7.** La Dirección Conjunta del Régimen Especial de Seguridad en el Comando Estratégico Operacional, tendrá la responsabilidad de determinar las medidas generales de seguridad para las informaciones y materiales clasificados, establecer el régimen de seguridad de las unidades militares y dependencias administrativas, y representar a la Fuerza Armada Nacional Bolivariana ante las instituciones del Poder Público Nacional.



El régimen especial de seguridad en los Componentes Militares, la Milicia Bolivariana, las Regiones Estratégicas de Defensa Integral y dependencias administrativas a este nivel, se estructuran en Direcciones del Régimen Especial de Seguridad, y tienen la responsabilidad de aplicar los lineamientos generales emanados de la Dirección Conjunta del Régimen Especial de Seguridad del Comando Estratégico Operacional e instrumentar las específicas a su nivel en correspondencia con sus características propias.

La División del Régimen Especial de Seguridad en las Zonas Operativas de Defensa Integral y dependencias administrativas a este nivel, ejecutan las directrices establecidas en las presentes normas y las generadas por la Dirección del Régimen Especial de Seguridad del nivel superior.

El Jefe del Régimen Especial de Seguridad de las grandes unidades militares, dependencias administrativas a este nivel y de las Áreas de Defensa Integral, que por su composición y envergadura requieran del Órgano del Régimen Especial de Seguridad, responderá por la organización, el control y el cumplimiento de las normas y medidas establecidas para la seguridad, manejo y protección de la información oficial y el régimen de seguridad en sus unidades subordinadas.

Los Jefes de Estado Mayor, Plana Mayor y Segundo Comandante de las unidades militares y las Áreas de Defensa Integral o su equivalente en las dependencias administrativas, que no cuenten con estos órganos, responden por la organización y puesta en funcionamiento de las medidas del régimen especial de seguridad.

### **Funciones**

**Artículo 8.** La estructura del régimen especial de seguridad tiene las funciones siguientes:

1. Comprobar la correcta aplicación de las normas y procedimientos establecidos en la legislación vigente y lo dispuesto en los documentos rectores de la Fuerza Armada Nacional Bolivariana, para la seguridad y protección de la información oficial en el sector defensa.
2. Elaborar, proponer y supervisar el cumplimiento de las normas generales para la seguridad manejo y protección de la información oficial, en las unidades militares y dependencias administrativas.
3. Elaborar, proponer y controlar el cumplimiento de las normas generales sobre el régimen de seguridad de las unidades militares y dependencias administrativas de la Fuerza Armada Nacional Bolivariana a su nivel.
4. Elaborar y proponer las instrucciones particulares respecto al régimen especial de seguridad a su nivel y comprobar su cumplimiento.



5. Controlar en coordinación con el arma o servicio de comunicaciones, el cumplimiento e implementación de las medidas previstas para la seguridad tecnológica.
6. Establecer las regulaciones especiales de seguridad y control de acceso a las unidades militares y dependencias administrativas de la Fuerza Armada Nacional Bolivariana; así como, exigir y controlar su cumplimiento.
7. Planificar la adquisición de sellos húmedos, secos y metálicos, sistemas de control de acceso, libros, formatos y demás materiales y equipos necesarios para sus funciones.
8. Exigir el cumplimiento de las normas y procedimientos para la clasificación, reclasificación, registro, control, manipulación, archivo (activo y pasivo) y destrucción de la información.
9. Realizar las supervisiones planificadas al régimen especial de seguridad y participar en otras como parte de los planes aprobados por los Comandantes y jefes según sus facultades.
10. Mantener informado a su Comandante o jefe inmediato de aquellas deficiencias y situaciones que afectan el cumplimiento de las reglamentaciones establecidas, haciendo las propuestas de medidas que se adoptarán para corregirlas.
11. Organizar y asegurar el acceso del personal y otras medidas de compartimentación del secreto militar, en eventos relacionados con la seguridad y defensa, en los que participen los principales miembros de la Fuerza Armada Nacional Bolivariana, miembros de la Administración Pública y otras instituciones; así como, personalidades extranjeras.
12. Responder por el funcionamiento del Órgano de Protección y Control de la Información; así como, por la instrucción y capacitación del personal que labora en él.
13. Realizar periódicamente análisis sobre las vulnerabilidades del régimen especial de seguridad, identificando las causas y condiciones que las provocan; así como, proponer e implementar las medidas para erradicarlas y comprobar su cumplimiento.
14. Responder por la implementación y desarrollo de los sistemas tecnológicos de protección y control de acceso en las unidades militares y dependencias administrativas, controlar el cumplimiento de las normas para el diseño, prioridades y efectividad de la instalación del sistema de seguridad tecnológica.
15. Normar y regular los contenidos a publicar en los diferentes portales Web de la Fuerza Armada Nacional Bolivariana y velar por su cumplimiento.



**Deberes del personal de la Fuerza Armada  
Nacional Bolivariana**

**Artículo 9.** El personal de la Fuerza Armada Nacional Bolivariana con acceso a la información y material clasificado está obligado a:

1. Conocer los documentos rectores y las bases legales, que norman los aspectos relacionados con la seguridad, manejo y protección de la información.
2. Ser vigilantes ante aquellas conductas o acciones que puedan propiciar la fuga de información o violaciones al régimen especial de seguridad, informando oportunamente a su Comandante o jefe inmediato.
3. Determinar correctamente la clasificación de las informaciones, según la Lista Interna para la clasificación y reclasificación de la información oficial y elaborar los documentos clasificados solamente en soportes registrados por el Órgano de Protección y Control de la Información, tomando las medidas establecidas para asegurar su compartimentación y conservación.
4. Presentar durante las inspecciones y supervisiones que se realicen, las informaciones clasificadas que se encuentren en su poder.
5. Cumplir las medidas establecidas en las presentes normas.

**Prohibiciones al personal de la Fuerza Armada  
Nacional Bolivariana**

**Artículo 10.-** Al personal de la Fuerza Armada Nacional Bolivariana con acceso a información y material clasificado se le prohíbe:

1. Divulgar información clasificada o de asuntos del servicio a personas no autorizadas.
2. Escribir o almacenar información clasificada en documentos, soportes magnéticos o de cualquier otro tipo, sin certificación del Órgano de Protección y Control de la Información.
3. Destruir documentos con información clasificada sin cumplir el procedimiento establecido a través del Órgano de Protección y Control de la Información.
4. Poseer en las unidades militares y dependencias administrativas, dispositivos tecnológicos ajenos a la institución, que puedan almacenar y reproducir información de audio, vídeo e imágenes; sin la autorización de su comando natural.
5. Divulgar la denominación real de las unidades militares, sus áreas de ubicación y otras informaciones clasificadas, en conversaciones con personal ajeno a la Fuerza Armada Nacional Bolivariana, en el envío de correspondencia y en las publicaciones que se realicen.

6. Trabajar con documentos clasificados en locales que no cumplan con las medidas de seguridad establecidas.
7. Tener documentos clasificados en su poder cuando se ausente de la unidad por motivos de fuerza mayor (vacaciones, enfermedad, problemas personales y otros).

## **CAPÍTULO II ÓRGANO DE PROTECCIÓN Y CONTROL DE LA INFORMACIÓN**

### **Definición**

**Artículo 11.** El Órgano de Protección y Control de la Información es la dependencia subordinada directamente al Jefe del Régimen Especial de Seguridad, que responde por el registro, control, protección, tramitación, reproducción, almacenamiento y destrucción de las informaciones.

### **Deberes**

**Artículo 12.** El personal que pertenece al Órgano de Protección y Control de la Información tiene como deberes principales los siguientes:

1. Garantizar la seguridad y protección al elaborar, reproducir, manipular, almacenar y destruir la información oficial y participar en el cumplimiento de las medidas para mantener la compartimentación que éstas requieren.
2. Garantizar una correcta tramitación y organización de la información oficial por cualquier vía y en cualquier tipo de soporte, para asegurar un eficiente servicio y control.
3. Exigir a los responsables de la información el cumplimiento de las medidas establecidas para la elaboración, registro, control, manipulación y almacenamiento de la información oficial.
4. Revisar los sistemas de almacenamiento masivo de información para computadoras, con los detectores de programas malignos establecidos en la Fuerza Armada Nacional Bolivariana, cada vez que sean usados y le sean entregados para su custodia por los responsables de información; así como, los que se reciban de otras unidades militares o dependencias administrativas.
5. Borrar los sistemas de almacenamiento masivo de información para computadoras, cuando se transfieran a otro administrador de información, unidad militar o dependencia administrativa, a los cuales no les compete la información contenida en ellos.
6. Exigir que se determinen y cumplan los plazos de vigencia de las informaciones, para facilitar su depuración periódica, respondiendo por su destrucción.



7. Controlar los medios de reproducción y las cajas fuertes de la unidad militar o dependencia administrativa.
8. Ejecutar una permanente actualización y el control de la ubicación de los documentos que se encuentran en poder de los responsables de información, o pendientes por archivar en el Órgano de Protección y Control de la Información.
9. Mantener actualizado el listado de todo el personal de la unidad militar o dependencia administrativa con acceso a las informaciones clasificadas.
10. Recibir, registrar, entregar y controlar los sellos de la unidad militar o dependencia administrativa.
11. Enviar la información oficial a otras unidades militares o dependencias administrativas a través de los medios establecidos por el Sistema de Comunicaciones de la Fuerza Armada Nacional Bolivariana, asegurando su integridad y el cumplimiento de los procedimientos.

#### **Medidas de seguridad**

**Artículo 13.** El local donde se ubica el Órgano de Protección y Control de la Información debe cumplir un conjunto de medidas de seguridad física, tecnológica y organizativa por cuyo cumplimiento responde el Jefe de Estado Mayor y Segundo Comandante o su equivalente:

1. El Órgano de Protección y Control de la Información debe ubicarse en locales independientes dentro de la instalación principal del Estado Mayor y Plana Mayor de las unidades militares o su equivalente en las dependencias administrativas.
2. Las puertas deben ser resistentes, revestidas con láminas de metal o con rejas metálicas y cerradura de doble paso.
3. Las ventanas y orificios para los equipos de aire acondicionado estarán protegidos por rejas metálicas. Las rejas de las puertas, ventanas y orificios para los equipos de aire acondicionado deben ser empotradas en la pared, preferiblemente por la parte interior del local.
4. Las paredes deberán ser de concreto y llegar hasta el techo.
5. Las puertas y ventanas se habilitarán con medios tecnológicos de protección y control de acceso.
6. El local debe contar con medios de protección contra incendios.
7. La puerta de acceso será habilitada con dispositivos que permitan su sellado.
8. Los archivos y armarios deberán ser metálicos, de concreto o de madera con enchape metálico, con puertas, cerraduras seguras y con dispositivos que permitan su sellado.



9. Se habilitarán locales contiguos a éstas para que los administradores de información puedan trabajar con la información clasificada.
10. Tendrán acceso permanente al Órgano de Protección y Control de la Información, el personal que en ella labora, el Comandante, el Jefe de Estado Mayor y Segundo Comandante o su equivalente, el Jefe del Régimen Especial de Seguridad, el oficial de contrainteligencia militar y otro cargo que por sus funciones con relación al Órgano de Protección y Control de la Información, autorice el Comandante de la unidad o jefe de dependencia.
11. Las cerraduras de las puertas, archivos, cajas fuertes y armarios utilizados para la conservación de las informaciones clasificadas, deberán tener dos (02) copias de las llaves.
12. La limpieza y/o reparación de los locales y equipos instalados se realizará sólo en presencia del personal que labora en ella. En estos casos, todos los documentos y sistemas de almacenamiento masivo para computadoras, deben guardarse en los archivos y cajas fuertes.
13. Las combinaciones de las cajas fuertes se conservarán en el Órgano de Protección y Control de la Información, en sobres lacrados y sellados u otros medios de seguridad disponibles.
14. La apertura diaria del Órgano de Protección y Control de la Información la efectuará el personal que pertenece a este órgano, quien está en la obligación de comprobar la integridad de los sellos de las puertas, archivos y de sus cerraduras.
15. Al retirarse el personal del Órgano de Protección y Control de la Información, el Jefe del Servicio de Guardia recibirá las llaves del local, comprobando el correcto sellado y activará el sistema de alarma, respondiendo en lo adelante por su seguridad.
16. En los centros educativos de la Fuerza Armada Nacional Bolivariana en que existan bibliotecas, dentro de éstas se pueden destinar locales especiales para la conservación y utilización de las informaciones clasificadas; su control se realizará según las normas establecidas en las presentes normas.
17. Los Comandantes de las unidades militares o jefes de dependencias administrativas que no tienen Órgano de Protección y Control de la Información, deben designar mediante una orden interna, un responsable para esta tarea. El responsable debe cumplir con los requisitos de preparación y confiabilidad establecidos para el personal del Órgano de Protección y Control de la Información.

**Evacuación del Órgano de Protección y  
Control de la Información**

**Artículo 14.** En el Órgano de Protección y Control de la Información se elaborará el plan de evacuación y destrucción de las informaciones para las diferentes

**CSBO/**

.../...



situaciones del proceso de la puesta en completo apresto operacional y para casos de incendio o de desastre natural. Este plan lo aprobará el Jefe de Estado Mayor y Segundo Comandante o su equivalente, debiendo elaborarse y comprobarse su efectividad desde tiempo de paz.

**Trabajo del Órgano de Protección y Control de la Información en tiempo de guerra**

**Artículo 15.** El Órgano de Protección y Control de la Información en campaña debe ubicarse cerca de los locales que ocupan el Comando y el Estado Mayor en los Puestos de Comando:

1. El acondicionamiento del Órgano de Protección y Control de la Información en campaña se organizará de tal modo que facilite su maniobrabilidad junto con el Puesto de Comando, de tal manera que mantenga su funcionalidad y el control de las informaciones.
2. El registro, control, reproducción, manipulación y almacenamiento de los planes operacionales se realizará cumpliendo lo establecido en las presentes normas.
3. En caso de peligro inminente de captura de las informaciones clasificadas por parte del enemigo, éstas deben ser destruidas según las disposiciones del Comandante de la unidad o jefe de dependencia.
4. El personal militar cuando actúa aisladamente o como correo, ante la inminente captura por el enemigo, destruirá las informaciones clasificadas.
5. El Jefe de Estado Mayor y Segundo Comandante o su equivalente, debe asegurar desde tiempo de paz, un vehículo acondicionado para el trabajo del Órgano de Protección y Control de la Información en campaña.

**CAPÍTULO III**  
**CLASIFICACIÓN, SEGURIDAD Y MANEJO DE LAS INFORMACIONES Y MATERIALES CLASIFICADOS DE LA FUERZA ARMADA NACIONAL BOLIVARIANA**

**Definición**

**Artículo 16.** La clasificación, seguridad y manejo de las informaciones y materiales clasificados de la Fuerza Armada Nacional Bolivariana es el conjunto de medidas tecnológicas, organizativas, preventivas, educativas y de control, establecidas con el objetivo de detectar y prevenir las posibles vías de fuga de información y material clasificado; así como, las tendencias a eliminar las causas y condiciones que las propician e impedir su pérdida.

**Clasificación**

**Artículo 17.** La información oficial, atendiendo a su contenido y al nivel que la genere y con el fin de establecer las medidas para su seguridad y manejo se divide en las siguientes categorías:

**CSBO/**

/...

INFORMACIÓN OFICIAL CLASIFICADA {  
Secreto Priorizado  
Secreto  
Confidencial

INFORMACIÓN OFICIAL LIMITADA {  
Reservada  
Ordinaria

### Información oficial clasificada

**Artículo 18.** La información oficial clasificada es la que posee una unidad militar, dependencia administrativa o una persona natural o jurídica, y que requiere de medidas de protección definidas por la Ley, por contener datos o informaciones cuyo conocimiento o divulgación no autorizada puede ocasionar daños o entrañar riesgos para la Fuerza Armada Nacional Bolivariana y para la República. La misma se identificará con caratulas de color rojo.

De acuerdo con su importancia y contenido, la información oficial clasificada se divide en las siguientes categorías:

1. **Secreto Priorizado:** se le asigna a aquella información cuyo conocimiento o divulgación no autorizada pondría en peligro la soberanía, la seguridad, la defensa, la integridad, la estabilidad o el funcionamiento del Estado y además la sustentabilidad de la República.
2. **Secreto:** Se le asigna a aquella información cuyo conocimiento o divulgación no autorizada puede causar perjuicios o comprometer el desarrollo de planes o programas defensivos a nivel del País o de una parte de su territorio nacional, o que de algún modo pueda ocasionar daños a determinadas funciones o actividades fundamentales de la seguridad y defensa, tanto en el ámbito nacional como territorial.
3. **Confidencial:** Se le asignará a la información cuyo conocimiento o divulgación no autorizada pueda ocasionar daños o afectar a determinadas actividades o funciones de una unidad militar, dependencia administrativa, o de una especialidad en particular.

### Información oficial limitada

**Artículo 19.** La información oficial limitada es aquella que no compromete los intereses de la Fuerza Armada Nacional Bolivariana. La misma se identificará con caratulas de color azul. De acuerdo con su importancia y contenido, ésta se divide en las siguientes categorías:

1. **Reservada:** se asignará a las informaciones cuyo contenido sin llegar a ser conceptuada como clasificada, por su importancia o carácter sensible para el trabajo de la unidad militar, dependencia administrativa o de la persona natural o jurídica que la posee, no resulta conveniente su difusión pública y

CSBO/

.../...  
✓



debe limitarse su acceso a personas específicas, quienes no podrán divulgarla ni modificarla sin la correspondiente autorización.

2. **Ordinaria:** se la asignará a aquella información que posee una unidad militar, dependencia administrativa o persona natural o jurídica, cuyo conocimiento o divulgación no autorizada no produce daños o riesgos para su funcionamiento, de igual manera puede ser de conocimiento público.

#### **Clasificación**

**Artículo 20.** La clasificación es el proceso mediante el cual se determina la categoría correspondiente a una información oficial. La correcta clasificación de la información según lo establecido en la Lista Interna, es obligación del responsable de la información, y deberá revisarla el Comandante de la unidad militar o jefe de la dependencia administrativa que la aprueba.

#### **Reclasificación**

**Artículo 21.** La reclasificación es el proceso mediante el cual se le suprime la categoría de clasificación a una información al desaparecer los elementos que le dieron ese carácter.

#### **Lista Interna**

**Artículo 22.** La Lista Interna es una guía metodológica que permite la clasificación y reclasificación de la información oficial, se debe consultar de manera obligatoria para determinar la categoría de la información que se genera en cada unidad militar o dependencia administrativa a todos los niveles.

#### **Compartimentación de la información oficial clasificada**

**Artículo 23.** La compartimentación es un principio indispensable para asegurar la protección de la información oficial clasificada y es el procedimiento que deben organizar los Comandantes de unidades y jefes de dependencias, para garantizar que el personal subordinado tenga acceso sólo a la información que le compete para su trabajo. Esto se materializa en el conjunto de medidas de seguridad y protección que se cumplirán durante los procesos de elaboración, reproducción, manipulación y almacenamiento de los documentos e informaciones clasificadas.

#### **Medidas de compartimentación**

**Artículo 24.** Para garantizar la compartimentación de la información oficial clasificada se tomarán las siguientes medidas:

1. Determinar con antelación, qué personal debe tener acceso a determinada información y en qué volumen.
2. Se deberá emplear el mecanismo de envío de la información sólo a los jefes que les compete, manteniendo este procedimiento durante toda su manipulación en los diferentes niveles.



3. Elaborar extractos de la información oficial clasificada con la autorización del Comandante o jefe que la aprobó, para que cada nivel y cada jefe en el ámbito de sus atribuciones, conozca solamente la información que le compete para su trabajo.
4. Mantener el control del personal con acceso a la información oficial clasificada.
5. Informar sobre temas o asuntos clasificados en reuniones y otras actividades colectivas que se desarrollen, sólo los aspectos necesarios para alcanzar los objetivos propuestos.
6. Mantener protegidos del acceso visual, todos los documentos clasificados ubicados en los Puestos de Comando, salas situacionales, oficinas de los Jefes de Servicio de Guardia y otros locales donde se muestre información oficial clasificada.

#### **Elaboración de la información oficial clasificada**

**Artículo 25.** La información oficial clasificada se elaborará en cuadernos de trabajo, mapas, hojas de papel y otros soportes tecnológicos, debidamente certificados y controlados por el Órgano de Protección y Control de la Información, los cuales deben poseer la categoría que le corresponda a la información que se elabora.

#### **Reproducción de la información oficial clasificada**

**Artículo 26.** La información oficial clasificada se reproducirá sólo en el Órgano de Protección y Control de la Información de las unidades militares o dependencias administrativas de la Fuerza Armada Nacional Bolivariana o en las imprentas del Ministerio del Poder Popular para la Defensa, el Comando Estratégico Operacional, los Componentes Militares, la Milicia Bolivariana y las Regiones Estratégicas de Defensa Integral, en las cantidades necesarias para garantizar su entrega a los destinatarios establecidos en la lista de distribución, de tal manera que permita el cumplimiento de la misión y actividades de las unidades militares o dependencias administrativas.

En el caso de las informaciones con categoría Secreto Priorizado, se prohíbe su reproducción por otras unidades militares o dependencias administrativas que no sea la que las elaboró. La reproducción de estos documentos se hará en la cantidad de ejemplares imprescindibles. Este proceso se realizará en el mismo local y por el mismo personal que las elaboró.

#### **Medidas con los medios de reproducción de la información clasificada**

**Artículo 27.** Los medios de reproducción de información, como impresoras, grabadores de discos compactos, dispositivos para la protección de la información de computadoras, fotocopadoras, equipos de facsímil y otros, deben controlarse



mediante medidas organizativas, físicas y tecnológicas que aseguren el control de su empleo, tales como:

1. Ubicación en lugares seguros.
2. Limitación del personal con acceso a ellos.
3. Adecuada selección y adiestramiento del personal que los opera.
4. Las fotocopadoras deben instalarse fundamentalmente en el Órgano de Protección y Control de la Información. Los Comandantes de unidades militares o jefes dependencias administrativas podrán determinar que se instalen en otro local según las características de trabajo y del personal que en él labora, estableciendo las medidas de control para la reproducción de las informaciones clasificadas.
5. Los equipos de facsímil no asociados a dispositivos de cifrado se emplearán solamente para la transmisión de información limitada entre las unidades militares y dependencias administrativas de la Fuerza Armada Nacional Bolivariana.

#### **Dstrucción de la información oficial clasificada**

**Artículo 28.** La destrucción de la información oficial clasificada debe convertirse en una actividad sistemática de los responsables de la documentación oficial y del Órgano de Protección y Control de la Información, para mantener en los archivos sólo la información necesaria para el trabajo. La documentación y los dispositivos de almacenamiento masivo donde se archiva información oficial clasificada, se revisarán y depurarán al final de cada año.

Cada responsable de la documentación oficial al elaborar o recibir una información clasificada, está en la obligación de determinar y anotar en el documento el plazo de vigencia, con excepción de los documentos de la base legal. La destrucción física del documento la realizará el personal del Órgano de Protección y Control de la Información.

#### **Trabajo con los documentos operacionales**

**Artículo 29.** Los documentos operacionales requieren de elevadas medidas para su seguridad y protección, por ser portadores de informaciones que comprometen la seguridad y la defensa del Estado Venezolano y de su Fuerza Armada Nacional Bolivariana.

Estos documentos se elaborarán en computadoras por el personal con acceso a ellos, en el volumen que le corresponde hasta el nivel de Áreas de Defensa Integral y Brigadas o su equivalente. En los niveles inferiores se elaborarán en cuadernos de trabajo a mano, por los propios responsables de la información, observándose las normas establecidas en las presentes normas para el registro y control de las informaciones clasificadas.

La computadora para elaborar y reproducir documentos operacionales, se designará para este tipo de trabajo durante el tiempo que sea necesario y debe

**CSBO/**



ser certificada por el Órgano de Protección y Control de la Información, para tal fin no deberá estar conectada en red.

Una vez concluidos los trabajos de elaboración de la documentación operacional y antes de reintegrar la computadora a su trabajo habitual, se procederá al borrado del disco duro por parte del Órgano de Protección y Control de la Información.

Esta documentación se conservará en el Órgano de Protección y Control de la Información en bóvedas o en cajas fuertes, de manera independiente al resto de la información clasificada.

Los Comandantes de unidades militares y jefes de dependencias administrativas de la Fuerza Armada Nacional Bolivariana oficializarán mediante listado aprobado, el personal que tendrá acceso a la documentación operacional.

#### **CAPÍTULO IV**

### **SISTEMA DE SELLOS EN LA FUERZA ARMADA NACIONAL BOLIVARIANA**

#### **Definición**

**Artículo 30.** El sistema de sellos en la Fuerza Armada Nacional Bolivariana incluye las normas referentes a la tipificación y designación de estos medios, las facultades para su solicitud, confección, empleo y los procedimientos para su registro, control y almacenamiento. Estos medios forman parte de las normas para oficializar, autenticar y proteger la información, y para garantizar la integridad de las instalaciones, material y equipos de uso militar.

#### **Clasificación**

**Artículo 31.** El sistema de sellos de la Fuerza Armada Nacional Bolivariana por su designación tiene la siguiente clasificación:

1. **Sello seco:** troquel con el cual se sellan documentos de modo tal que los símbolos, letras y números quedan bajorrelieve en seco. Estos siempre son metálicos y están compuestos por una base, en la cual se encuentra un molde calado donde se introduce el troquel impreso con las letras, símbolos y números que quedan impresos, acto éste que se produce por la presión ejercida sobre una palanca que une el troquel con la base.
2. **Sello húmedo:** son sellos de goma que están constituidos por una base generalmente de madera, a la que se le fija una pieza de goma que tiene estampada al relieve la estructura de la impresión que se gravará en el papel, valiéndose de la tinta.
3. **Sello metálico:** están constituidos por una pieza de metal en la que aparece estampada la estructura que se imprimirá en lacre, plastilina u otro material similar. Los sellos se destinan para avalar la pertenencia y el carácter oficial de los documentos y para detectar el acceso no autorizado a



documentos, instalaciones, material y equipos de uso militar que se encuentren debidamente sellados. Este sello es de uso personal e intransferible.

4. **Sello adhesivo rotulado:** está constituido por una lámina de material adhesivo rotulado y seriado. Estos sellos se destinan fundamentalmente para detectar el acceso no autorizado al interior de los locales, materiales, equipos y sistemas de armas.

#### **Regulaciones para el control y empleo**

**Artículo 32.** Los Comandantes de las unidades militares y jefes de dependencias administrativas responden por la protección y el correcto empleo de los sellos.

Las autoridades militares facultadas para emplear el sello seco son las siguientes:

1. Ministro del Poder Popular para la Defensa.
2. Vice-Ministros del Ministerio del Poder Popular para la Defensa.
3. Contralor General de la Fuerza Armada Nacional Bolivariana.
4. Inspector General de la Fuerza Armada Nacional Bolivariana.
5. Comandante Estratégico Operacional de la Fuerza Armada Nacional Bolivariana.
6. Comandantes de las Regiones Estratégicas de Defensa Integral.
7. Comandantes de Componentes Militares y la Milicia Bolivariana.

Los Comandantes a los distintos niveles emitirán órdenes internas que regulen la utilización de los sellos, las medidas de seguridad para su control y asignarán las responsabilidades al personal militar y civil que por necesidades del servicio deben poseerlos.

Queda terminantemente prohibido emplear sellos de otra unidad militar o dependencia administrativa, para legalizar o avalar información o documentos por parte de cualquier integrante de la Fuerza Armada Nacional Bolivariana.

#### **Solicitud y confección**

**Artículo 33.** Las solicitudes para la confección de los sellos se presentarán al Jefe del Régimen Especial de Seguridad del comando superior, por los Comandantes de las unidades militares o jefes de dependencias administrativas de la Fuerza Armada Nacional Bolivariana, basándose en las órdenes y directivas que ponen en funcionamiento la estructura de sus propias unidades militares o dependencias administrativas o cuando cualquier otra situación así lo requiera.

Los sellos que se utilizan en la Fuerza Armada Nacional Bolivariana se confeccionarán en los lugares donde determinen los Jefes del Régimen Especial de Seguridad del Comando Estratégico Operacional, de las Regiones Estratégicas de Defensa Integral, de los Componentes Militares y la Milicia Bolivariana, quedando terminantemente prohibido su confección o duplicados en otros

**CSBO/**

W/...



lugares. Los sellos confeccionados se controlarán en el Libro de Registro de Sellos de cada unidad militar o dependencia administrativa de la Fuerza Armada Nacional Bolivariana; en él se plasmarán sus muestras, fechas de confección y cambios de custodios.

## **CAPÍTULO V**

### **SEGURIDAD Y PROTECCIÓN DE LA INFORMACIÓN OFICIAL EN EL TRABAJO CON LAS TECNOLOGÍAS DE LA INFORMACIÓN**

#### **Definición**

**Artículo 34.** La seguridad y protección de la información oficial en el trabajo con las tecnologías de la información, es el cumplimiento de un conjunto de medidas organizativas, físicas, técnicas, educativas y de control, dirigidas a detectar, prevenir e impedir acciones que faciliten el conocimiento o la divulgación no autorizada de la información oficial que se procesa, almacena e intercambia en los equipos informáticos y sus soportes.

#### **Clasificación de los equipos informáticos**

**Artículo 35.** Los equipos informáticos que se empleen en las unidades militares y dependencias administrativas de la Fuerza Armada Nacional Bolivariana, se clasificarán en correspondencia con la categoría que posea la información que se procese y almacene en ellos, estableciéndose las categorías siguientes:

1. **Categoría "A":** se designará con esta categoría a los equipos informáticos y soportes utilizados para el procesamiento y almacenamiento de información oficial clasificada con categoría hasta "Secreto Priorizado".
2. **Categoría "B":** se designará con esta categoría a los equipos informáticos y soportes utilizados para el procesamiento y almacenamiento de información oficial clasificada con categoría hasta "Secreto".
3. **Categoría "C":** se designará con esta categoría a los equipos informáticos y soportes utilizados para el procesamiento y almacenamiento de información oficial clasificada con categoría hasta "Confidencial".
4. **Categoría "D":** se designará con esta categoría a los equipos informáticos y soportes utilizados para el procesamiento y almacenamiento de información oficial limitada con categoría hasta "Reservada".
5. **Categoría "E":** se designará con esta categoría a los equipos informáticos y soportes utilizados para el procesamiento y almacenamiento de la información oficial "Ordinaria".

#### **Medidas para la seguridad de las instalaciones**

**Artículo 36.-** Las instalaciones donde se ubican los equipos informáticos que procesan información clasificada deben cumplir las siguientes medidas para la seguridad:

CSBO/

 /...



1.- Garantizar la seguridad de la instalación desde el punto de vista constructivo y de protección física de sus accesos, de forma tal que imposibilite la entrada de personal no autorizado.

2.- Asegurar el acondicionamiento con sistemas tecnológicos de protección y control de acceso, los que deberán complementarse con medidas organizativas para la compartimentación y protección de la información.

3.- Garantizar la protección electromagnética con el objetivo de disminuir la emisión de señales electromagnéticas comprometedoras de la información clasificada.

#### **Sellado de los equipos informáticos**

**Artículo 37.** A los equipos informáticos que contengan en su interior soportes de almacenamiento de información, se les aplicarán sistemas de cierres profesionales o sellados que permitan detectar la apertura no autorizada de estos.

#### **Certificación de los soportes de información**

**Artículo 38.** Los soportes de información para el trabajo con las tecnologías de información en las unidades militares y dependencias administrativas de la Fuerza Armada Nacional Bolivariana serán certificados, controlados y almacenados por el Órgano de Protección y Control de la Información y se les otorgará la categoría en correspondencia con la categoría de la información que procese.

#### **Medidas de seguridad tecnológica**

**Artículo 39.** Para el procesamiento de la información clasificada en los equipos informáticos, son de obligatorio cumplimiento las siguientes medidas de seguridad tecnológica:

1. El empleo de programas básicos y de aplicación, aprobados por la Dirección Conjunta de Comunicaciones de la Fuerza Armada Nacional Bolivariana.
2. La protección de acceso a los equipos informáticos y sus soportes.
3. El cifrado de los archivos que se almacenan y transmiten en los sistemas informáticos y redes.
4. La detección y eliminación de los programas malignos.
5. La implementación de las medidas de seguridad, sistemas de detección de intrusos y sistemas de firma digital.
6. La implementación de las herramientas de auditoría y control en los sistemas informáticos y redes que se desarrollan en la Fuerza Armada Nacional Bolivariana.
7. La organización y realización del respaldo de la información.



8. Las medidas para el borrado seguro de los archivos y soportes.

### **Seguridad de las aplicaciones**

**Artículo 40.** La Dirección Conjunta de Comunicaciones de la Fuerza Armada Nacional Bolivariana es la estructura organizacional responsable de organizar, supervisar y controlar la introducción de programas informáticos en la Fuerza Armada Nacional Bolivariana; para ello emitirá anualmente los estándares de programas, los cuales deben cumplir las exigencias de los productos de seguridad implantados.

### **Redes de computadoras y enlaces**

**Artículo 41.** Las redes de computadoras, servicios y enlaces, por su alcance y por el nivel de acceso que proveen a los responsables de la información, se clasifican en:

1. **Local:** se establecen entre oficinas o estructuras organizacionales, ubicadas dentro de una misma área geográfica o edificación.
2. **Internas:** se establecen entre unidades militares y/o dependencias administrativas de la Fuerza Armada Nacional Bolivariana o entre estructuras organizacionales de una misma unidad militar o dependencia administrativa de la Fuerza Armada Nacional Bolivariana separadas geográficamente dentro del territorio nacional.
3. **Nacionales:** las que se establecen entre unidades militares o dependencias administrativas de la Fuerza Armada Nacional Bolivariana y otros entes del país dentro del territorio nacional.
4. **Globales:** las que permiten la interconexión o el acceso de las unidades militares o dependencias administrativas de la Fuerza Armada Nacional Bolivariana a las redes de alcance internacional.

### **Medidas de seguridad en las redes**

**Artículo 42.** Para el trabajo con las redes de computadoras en la Fuerza Armada Nacional Bolivariana deben cumplirse las siguientes medidas de seguridad:

1. La red de comunicaciones de la Fuerza Armada Nacional Bolivariana tiene que ser físicamente independiente de cualquier red nacional o de alcance global.
2. En la red de comunicaciones de la Fuerza Armada Nacional Bolivariana se prohíbe la comunicación inalámbrica entre unidades militares y dependencias administrativas.
3. La sala de servidores debe tener medidas de seguridad física de acuerdo con su clasificación.

4. Todos los servidores tendrán implementados los sistemas de protección de acceso y las herramientas de auditoría propias de los sistemas operativos empleados.
5. El Comandante de la unidad o jefe de la dependencia administrativa aprobará los recursos informáticos que pueden ser compartidos.

#### **Empleo de la internet**

**Artículo 43.** Para el empleo de los servicios de Internet en las unidades militares y dependencias administrativas, se establecen las siguientes prohibiciones para el personal militar y civil de la Fuerza Armada Nacional Bolivariana:

1. El uso de servidores de correo público, privado o de otras dependencias del Estado, para tramitar información oficial clasificada relacionada con el servicio.
2. La publicación de cualquier información oficial clasificada, en las redes sociales, blogs, foros o sitios Web.
3. La publicación en las redes sociales, de datos relacionados con la vida y actividades profesionales dentro de la Fuerza Armada Nacional Bolivariana, del personal militar y civil.

#### **Implementación de los sitios web en la Fuerza Armada Nacional Bolivariana**

**Artículo 44.** La activación de portales o sitios Web en la Fuerza Armada Nacional Bolivariana se realizará con la autorización escrita del Ministro del Poder Popular para la Defensa y sus Viceministros, el Comandante Estratégico Operacional, los Comandantes de los Componentes Militares, el Comandante de la Milicia Bolivariana y los Comandantes de las Regiones Estratégicas de Defensa Integral, en las respectivas áreas de responsabilidad.

Se prohíbe la publicación en los portales o sitios Web de la Fuerza Armada Nacional Bolivariana de los siguientes aspectos:

1. Información oficial clasificada de cualquier tipo: documentos, bases de datos, imágenes, videos u otro material con formato digital.
2. Datos personales de los oficiales y personal de la Fuerza Armada Nacional Bolivariana.

#### **Filmaciones y publicaciones**

**Artículo 45.** La filmación y publicación a través de los medios de difusión públicos o privados de actividades protocolares, ejercicios o entrenamientos militares u otros eventos que se realicen en las unidades, polígonos, centros de entrenamiento o dependencias de la Fuerza Armada Nacional Bolivariana, se realizará por el personal debidamente acreditado por el Ministro del Poder Popular para la Defensa y sus Viceministros, el Comandante Estratégico Operacional, los Comandantes de los Componentes Militares, el Comandante de

**CSBO/**

 / ...



la Milicia Bolivariana y los Comandantes de las Regiones Estratégicas de Defensa Integral, en las respectivas áreas de responsabilidad.

#### **Empleo de medios tecnológicos particulares**

**Artículo 46.** El acceso de todo medio tecnológico particular a las unidades militares o dependencias administrativas, debe ser autorizado por el Comandante o Jefe de Estado Mayor y Segundo Comandante o su equivalente y quedará sujeto a la revisión o inspección por parte del Órgano del Régimen Especial de Seguridad. El empleo de estos medios se realizará sólo para actividades de carácter personal y se prohíbe su empleo para:

1. Elaborar, grabar, procesar, tramitar o almacenar cualquier información oficial clasificada, relacionada con el servicio en la Fuerza Armada Nacional Bolivariana.
2. Fotografiar, grabar o almacenar imágenes, videos o archivos de audio relacionados con información oficial clasificada y equipos o material de guerra de la Fuerza Armada Nacional Bolivariana.
3. Transmitir información, imágenes, videos o cualquier otra información oficial clasificada, relacionada con la Fuerza Armada Nacional Bolivariana.

### **CAPÍTULO VI SUPERVISIÓN AL ESTADO DE LA INFORMACIÓN OFICIAL**

#### **Definición**

**Artículo 47.** La supervisión consiste en comprobar el correcto registro, control, manipulación y almacenamiento de la información oficial; así como, las medidas de seguridad para su protección. En las unidades militares y dependencias administrativas de la Fuerza Armada Nacional Bolivariana, los Comandantes con el apoyo de la estructura organizacional del Régimen Especial de Seguridad, serán los encargados de dirigir dicha actividad en todos los niveles.

#### **Clasificación**

**Artículo 48.** En correspondencia con su periodicidad las supervisiones se clasifican en:

1. **Supervisión diaria:** es la comprobación que debe realizar el responsable de las informaciones a los documentos en su poder cada vez que trabaje con ellos.
2. **Supervisión mensual:** la ejecuta el personal del Órgano de Protección y Control de la Información, se realiza en los primeros cinco (05) días hábiles de cada mes y su objetivo es comprobar físicamente los documentos registrados y tramitados en el mes anterior.
3. **Supervisión semestral y anual:** se realizarán dos veces al año, al concluir cada semestre y tienen como finalidad fundamental la comprobación minuciosa de las informaciones clasificadas existentes; posibilitan además, detectar las

CSBO/

...  
✓

deficiencias en la elaboración, reproducción, manipulación, registro, control y almacenamiento de estas informaciones. Se exceptúan de ello las Áreas de Defensa Integral y los Órganos de Protección y Control de la Información que en su estructura cuenten con una sola persona, los cuales efectuarán solamente el control anual.

#### **Ejecución**

**Artículo 49.** Para la ejecución de las supervisiones se creará una comisión, originada por una orden del Jefe de Estado Mayor y Segundo Comandante de la unidad militar o su equivalente en la dependencia administrativa.

#### **Supervisión semestral**

**Artículo 50.** Durante la supervisión semestral se comprobarán los siguientes aspectos:

1. La solución de las deficiencias señaladas en la supervisión anterior.
2. El registro, control, manipulación, almacenamiento e incineración de las informaciones clasificadas durante el primer semestre del año, incluyendo los documentos operacionales. La manipulación incluye las informaciones elaboradas en años anteriores que hayan tenido movimiento.
3. Todas las informaciones clasificadas en poder de los administradores de información.
4. La orden de acceso a los documentos operacionales y otras tareas o planes especiales a los que se indique dar igual tratamiento, el estado del almacenamiento de los mismos y el control de su manipulación.
5. El cumplimiento de las supervisiones mensuales.
6. El cumplimiento de las medidas de seguridad establecidas para el Órgano de Protección y Control de la Información.
7. Mediante muestreo, comprobar la correcta clasificación de las informaciones según lo establecido en la Lista Interna, por parte de los responsables de la información.
8. Los aspectos organizativos o de otra índole que afecten el trabajo del Órgano de Protección y Control de la Información.

#### **Supervisión anual**

**Artículo 51.** Durante la supervisión anual se comprobará, además de lo indicado para la supervisión semestral, lo siguiente:

1. El registro, control, manipulación, almacenamiento e incineración de todas las informaciones clasificadas existentes en el Órgano de Protección y Control de la Información de años anteriores y del actual, incluyendo los documentos operacionales.
2. La existencia y objetividad del plan de evacuación y los medios necesarios para su cumplimiento.

CSBO/





3. La existencia de los sellos metálicos en poder de los responsables de la información clasificada; así como, de los sellos propiedad de la unidad militar o dependencia administrativa.
4. La existencia y conocimiento de los deberes funcionales del personal del Órgano de Protección y Control de la Información.
5. El cumplimiento de los procedimientos para la depuración de las informaciones clasificadas y el plazo de vigencia de las existentes.
6. Realizar una supervisión completa de todas las informaciones que existen en el Órgano de Protección y Control de la Información.

#### **Supervisiones no programadas**

**Artículo 52.** Los Comandantes o Jefes de Estado Mayor y Segundo Comandante o su equivalente, pueden decidir la realización de supervisiones no programadas al Órgano de Protección y Control de la Información subordinado. Las causas fundamentales que pueden motivar esta decisión pueden ser las siguientes:

1. Deficiencias detectadas que ponen en evidencia superficialidad en el trabajo de la comisión que realizó la supervisión.
2. Procedimientos incorrectos empleados por el personal del Órgano de Protección y Control de la Información que ponen en duda la confiabilidad del registro y control de las informaciones clasificadas o del propio personal.
3. Pérdida de informaciones clasificadas de forma reiterada o evidencias de descontrol en el trabajo con ellas.
4. Cambio del Jefe el Órgano de Protección y Control de la Información o unificación de dos o más de ellos.

### **CAPÍTULO VII RÉGIMEN DE SEGURIDAD**

#### **Definición**

**Artículo 53.** El régimen de seguridad es el conjunto de medidas organizativas, físicas, tecnológicas, preventivas y de control enfocadas a establecer un sistema de seguridad y protección; así como, un estricto control de acceso a las unidades militares y dependencias administrativas, con el propósito de evitar la acción del enemigo, la pérdida del armamento, el material de guerra y los medios materiales, y eliminar las causas y condiciones que posibiliten la ocurrencia de hechos extraordinarios.

#### **Medidas organizativas**

**Artículo 54.** Las medidas organizativas son todas aquellas actividades que se planifican y realizan con el objetivo de garantizar el régimen de seguridad en las unidades militares y dependencias administrativas; básicamente comprenden lo siguiente:

1. Medidas de control de acceso para el personal.

CSBO/

...



2. Organización de las medidas del régimen de seguridad en las reuniones y actividades de adiestramiento militar.
3. Medidas de seguridad durante las operaciones militares.
4. Medidas de seguridad, compartimentación y protección del secreto para las obras fortificadas en las etapas de preparación y ejecución.

#### **Acceso al personal extranjero**

**Artículo 55.** El acceso de personal extranjero a las unidades militares y dependencias administrativas de la Fuerza Armada Nacional Bolivariana por motivo de actividades diplomáticas o relaciones de trabajo, debe ser autorizado por el Ministro del Poder Popular para la Defensa, el Comandante Estratégico Operacional, los Comandantes de los Componentes Militares y la Milicia Bolivariana.

#### **Control de acceso**

**Artículo 56.** El control de acceso a todas las unidades militares y dependencias administrativas en la Fuerza Armada Nacional Bolivariana, se regula mediante la aplicación de un sistema de control de acceso que utiliza pases. Las solicitudes de pases de acceso se harán a los oficiales designados por el órgano del Régimen Especial de Seguridad y las aprobará el Comandante o el Jefe de Estado Mayor y Segundo Comandante o su equivalente; la elaboración, el registro y control será responsabilidad del órgano del Régimen Especial de Seguridad y se emitirán en los tipos siguientes:

1. **Pases permanentes:** se destinan para el personal orgánico de la unidad militar o dependencia administrativa.
2. **Pases provisionales:** se expiden al personal que se encuentra en proceso de nombramiento, en comisión de servicio y al que por otras razones de trabajo, deba visitar frecuentemente la unidad militar o dependencia administrativa en un período de tiempo determinado.
3. **Pases ordinarios:** se expiden en los puntos de expedición o de control de pases, al personal que visita la unidad militar o dependencia administrativa para reuniones, contactos personales, de trabajo, entrevistas, entre otros.
4. **Pases especiales:** se expiden con la finalidad de controlar la entrada y salida de equipos, documentos y otros soportes de información.

#### **Estados de excepción**

**Artículo 57.** En situaciones de estado de excepción deben organizarse sistemas de pases que respondan a las exigencias del Comando y las misiones asignadas. Estos deben almacenarse en los Puestos de Comando o en el Órgano de Protección y Control de la Información, empaquetados y sellados por el personal que integra el Régimen Especial de Seguridad.



### **Muestrario de pases**

**Artículo 58.** En los puntos de control de pases y acceso de las unidades y dependencias, se colocarán muestrarios, los cuales deben exhibir ejemplares de los diferentes tipos de pases; así como, de los pases de los niveles superiores que permiten el acceso a la unidad militar o dependencia administrativa, con los códigos, señales y firmas autorizadas, de tal manera que sirvan de referencia al controlador de acceso. La responsabilidad por la colocación y actualización de los muestrarios es del Órgano del Régimen Especial de Seguridad.

### **Operaciones Especiales**

**Artículo 59.** El Comandante de las Operaciones Especiales, a fin de asegurar la compartimentación, evitar la fuga de información clasificada y la seguridad del armamento, sistemas de armas, municiones y otros materiales de guerra durante su manipulación y transporte, establecerá mediante orden las medidas especiales de seguridad y enmascaramiento.

### **Seguridad de obras fortificadas**

**Artículo 60.** El Comandante de la unidad militar o jefe de la dependencia administrativa, asume la responsabilidad por la seguridad, protección y el control de acceso a la obra fortificada bajo su jurisdicción, desde la etapa de formulación de la propuesta de inversión y durante su ejecución. Para ello elaborará el plan de seguridad y control de acceso a la misma.

### **Acceso a obras fortificadas**

**Artículo 61.** El personal con acceso a las informaciones y a las obras fortificadas debe tener la aprobación del Comandante de la unidad militar o del jefe de la dependencia administrativa y de los órganos de la Contrainteligencia Militar, legalizándose esta autorización mediante un listado. Además debe establecerse un sistema de registro y control del personal que haya tenido acceso a las informaciones y a las obras por razones de cualquier índole y éstos se resguardarán en el Órgano del Régimen Especial de Seguridad que le compete.

### **Prohibiciones relativas a las obras fortificadas**

**Artículo 62.** Durante la construcción de obras fortificadas se prohíbe:

1. La utilización de personal en la obra para actividades de apoyo, sin la aprobación de los órganos de la Contrainteligencia Militar.
2. El acceso de personal administrativo que no tenga relación directa con la obra.
3. El almacenamiento de explosivos sin cumplir con las medidas y normas de seguridad establecidas.
4. Dibujar o copiar el esquema de la obra en hojas de papel, cartulina u otros soportes, sin registro y control, aunque en éste no se incluyan las coordenadas.



### **Medidas de seguridad física**

**Artículo 63.** Las medidas de seguridad física son aquellas que garantizan la protección de las unidades militares o dependencias administrativas, obstaculizando la acción del enemigo o de intrusos. Entre ellas se encuentran las siguientes:

1. El cercado perimetral de la unidad militar o dependencia administrativa.
2. La instalación de puertas y ventanas sólidas con láminas de metal, con rejas y cerraduras o candados de seguridad.
3. Las rejas a instalar deben ser resistentes, empotradas en la pared y colocadas por la parte interior de las puertas y ventanas.
4. La implementación de los dispositivos para el sellado que garanticen el control de acceso.
5. La existencia de los muestrarios de los sellos.
6. La prestación del servicio de guardia y la designación del personal de reacción ante una violación del régimen de seguridad establecido.
7. El sellado de los sistemas de armas en sus lugares más vulnerables (tanques de combustible, puertas de acceso, escotillas, sistemas de control, entre otros), las municiones, granadas, armamento y los materiales de guerra en general.

### **Sellado**

**Artículo 64.** El sellado es el procedimiento obligatorio que debe realizar todo responsable de la información oficial, el material de guerra, equipos tecnológicos e instalaciones en la Fuerza Armada Nacional Bolivariana, para detectar de forma oportuna el acceso y manipulación por parte de personal no autorizado.

Los locales y oficinas de trabajo de las unidades militares y dependencias administrativas serán siempre sellados al concluir la jornada laboral. El servicio de guardia deberá inspeccionar que los locales y oficinas estén sellados; las que no estén selladas, deberá sellarlas con su sello personal y registrarlo en el Libro del Servicio de Guardia.

### **Medidas de seguridad tecnológica**

**Artículo 65.** Las medidas de seguridad tecnológicas son aquellas acciones basadas en la utilización de equipos tecnológicos de protección y control de acceso, contraincendios, iluminación, comunicaciones y otras que se instalan como complemento al sistema de protección y seguridad de la unidad militar o dependencia administrativa. Entre ellas tenemos:

1. Instalación de medios tecnológicos de protección y control de acceso.
2. Establecimiento de una adecuada iluminación en las áreas exteriores de las edificaciones, galpones y locales aislados.



3. Ubicación de equipos contra incendios y la aplicación de las medidas para evitarlos.
4. Sistemas de alarmas acústicas y visuales.
5. Sistemas de video-vigilancia.
6. Sensores de detección de movimientos.
7. Instalación de cercas eléctricas.
8. Instalación de los equipos de comunicaciones.

#### **Régimen Estricto de Seguridad**

**Artículo 66.** El Régimen Estricto de Seguridad es el conjunto de medidas físicas, tecnológicas y organizativas que se incrementan a partir del régimen de seguridad, en aquellas unidades militares y dependencias administrativas que por su función, el grado de compartimentación de la actividad que realizan y las exigencias de protección que requieren, necesitan de un mayor nivel de seguridad.

Se establecerá el Régimen Estricto de Seguridad en los objetivos siguientes:

1. Puestos de comando, centros de comunicaciones y centros de datos del Ministerio del Poder Popular para la Defensa, Comando Estratégico Operacional, Componentes Militares, Milicia Bolivariana y Regiones Estratégicas de Defensa Integral.
2. Áreas especiales en industrias militares donde se construya o se almacene armamento, cohetes, municiones, explosivos u otro tipo de material que por su grado de compartimentación lo requiera.
3. Laboratorios o centros de investigaciones donde se estudien, proyecten y diseñen innovaciones constructivas del armamento, sistemas de armas u otro material de guerra.
4. Áreas de almacenes y obras donde se almacene armamento, cohetes, municiones, combustible, explosivos u otro tipo de equipos tecnológicos.
5. Las áreas donde se estén ejecutando las obras de construcción de los Puestos de Comando e instalaciones de alta protección y otras obras que por su importancia los Comandantes así lo determinen.

Es facultad del Comandante Estratégico Operacional, los Comandantes de los Componentes Militares, Milicia Bolivariana, Regiones Estratégicas de Defensa Integral y Zonas Operativas de Defensa Integral o equivalentes, la decisión de establecer en un objetivo subordinado el Régimen Estricto de Seguridad, emitiéndose la orden correspondiente.



**CAPÍTULO VIII**  
**VIOLACIONES AL RÉGIMEN ESPECIAL DE SEGURIDAD**

**Definición**

**Artículo 67.** Constituyen violaciones al Régimen Especial de Seguridad la inobservancia, omisión, negligencia o descuido, intencional o no, en el cumplimiento de las directrices y procedimientos establecidos en las presentes normas; estas violaciones serán sancionadas en correspondencia con las leyes y reglamentos vigentes en la República.

**Violaciones al Régimen Especial de Seguridad**

**Artículo 68.** Las violaciones al Régimen Especial de Seguridad son aquellas relacionadas con:

1. La pérdida de información oficial clasificada o los equipos tecnológicos usados en su elaboración; así como, la divulgación de datos relacionados con estos.
2. El robo o la extracción no autorizada de información oficial clasificada en cualquier soporte.
3. La apertura por parte de personal no autorizado, de información oficial clasificada cerrada y sellada.
4. La desactivación de los sistemas de protección informáticos o alteración de su funcionamiento de forma intencional.
5. La introducción de programas malignos u otras infracciones que pongan en peligro las informaciones almacenadas, las claves y los programas o productos de la seguridad informática.
6. El empleo por parte del personal no autorizado, de las máquinas y sus soportes, en redes de comunicaciones conectadas a Internet u otras redes de la Fuerza Armada Nacional Bolivariana, para el envío de información al extranjero o a otros organismos del Estado.
7. La falsificación de pases de acceso a una unidad militar o dependencia administrativa de la Fuerza Armada Nacional Bolivariana.
8. El ingreso a una unidad militar o dependencia administrativa de la Fuerza Armada Nacional Bolivariana por lugares no autorizados o de manera furtiva.
9. La utilización de sellos para falsificar un documento.
10. La desactivación de un sistema tecnológico de protección y control de acceso o la alteración de su funcionamiento de forma intencional.
11. La violación de las medidas de protección y de los sellos establecidos en los locales donde se conserva información o equipos clasificados.
12. Otras que por su connotación e importancia los Comandantes de unidades militares y jefes de dependencias administrativas consideren como violación al Régimen Especial de Seguridad.

**CAPÍTULO IX  
DISPOSICIONES FINALES**

**Derogación**

**Artículo 68.** Se deroga el Reglamento para Clasificación, Seguridad y Manejo de las Informaciones, Documentos y Materiales Clasificados de las Fuerzas Armadas, publicado mediante Resolución DG-4183 fecha 21 de Julio de 1986.

**Manual del Régimen Especial de Seguridad para la Fuerza Armada Nacional Bolivariana**

**Artículo 69.** El Comandante Estratégico Operacional promulgará el Manual del Régimen Especial de Seguridad, donde se establecerán de manera detallada, las normas y los procedimientos para proteger las informaciones, documentos y materiales clasificados, del conocimiento y difusión a personas no autorizadas y el régimen de seguridad aplicable a toda la Fuerza Armada Nacional Bolivariana.

Comuníquese y publíquese

Por el Ejecutivo Nacional



**CARMEN TERESA MELENDEZ RIVAS**

**Almiranta en Jefe**

**Ministra del Poder Popular  
para la Defensa**

CSBO/LCC/ZI.hhjd  
261456mar2014