

EJÉRCITO ARGENTINO

ROP – 11 – 06

Reservado

EJEMPLAR Nro:

MEDIDAS DE SEGURIDAD DE CONTRAINTELIGENCIA



REPÚBLICA ARGENTINA
Editado en el Departamento Doctrina
AÑO 2014



Ejército Argentino
Dir Grl Org Doct



*"2014 – Año del Homenaje al Almirante Guillermo Brown,
en el Bicentenario del Combate Naval de Montevideo"*

C A de BUENOS AIRES, 16 de diciembre de 2014.

Visto el expediente Letra D6 14 Nro 1231/5, lo Dictaminado por la Dirección General de Asuntos Jurídicos, lo informado por el Director General de Organización y Doctrina y lo establecido en el Art 2, Decreto 1759/12 (T O 1991).

EL SUBJEFE DEL ESTADO MAYOR GENERAL DEL EJÉRCITO

DISPONE:

ARTÍCULO 1º.- Apruébase el Reglamento propuesto - el que será inscripto en el "Registro de Publicaciones Militares" de la Fuerza - de acuerdo con los datos que se consignan a continuación:

1. Identificación:

a. Título: "MEDIDAS DE SEGURIDAD DE CONTRAINTELIGENCIA".

b. Signatura: ROP – 11 – 06.

2. Carácter del reglamento: RESERVADO.

3. Elemento responsable de su elaboración: Dirección de Inteligencia Funcional.

ARTÍCULO 2º.- Imprímanse, a través de la Dirección de General de Organización y Doctrina (Departamento Doctrina), SEIS (6) ejemplares de la publicación aprobada, e inscribase dicha publicación en el "Registro de Publicaciones Impresas". Una vez





realizado tal trámite, distribúyase la publicación impresa con cargo, a los efectos de su preservación histórica, entre los siguientes Elementos:

- a) Servicio Histórico del Ejército / DAHE..... 1 ejemplar.
- b) Archivo General del Ejército / DAHE..... 1 ejemplar.
- c) Biblioteca Central del Ejército / Secr Grl Ej..... 1 ejemplar.
- d) DGOD (DPTO DOCT)..... 1 ejemplar.
- e) Ministerio de Defensa..... 1 ejemplar.
- f) DINIEM..... 1 ejemplar

ARTÍCULO 3º - Realícese, por parte de todos los Elementos no consignados en el Artículo 2º, la impresión establecida en el artículo 6.037 del reglamento "La Doctrina en el Ejército Argentino" (RFD – 50 – 01).

ARTÍCULO 4º.- Elabórese la versión digitalizada e informatizada del reglamento aprobado, e inscribirlo en el "Registro de Publicaciones Digitalizadas".

ARTÍCULO 5º - Autorízase la instalación de la versión informatizada de la publicación aprobada, en cualquier tipo de soporte digital. Dicha autorización tiende al objetivo de facilitar su difusión de manera aislada, o bien reunida en compilaciones y compendios que se elaboren a tal efecto.

ARTÍCULO 6º.- Difúndase la versión digitalizada del reglamento, a través de soportes digitales y redes informáticas, administrados por la Fuerza, atendiendo los requisitos de seguridad y de acceso a la información, consignados en las leyes y reglamentos vigentes.

EMGE
DISPOSICION N° 331/14



ARTÍCULO 7º.- Practíquese la actualización de la publicación, en cualquiera de sus versiones – impresa y/o digital – de manera simultánea a la aprobación, registro y difusión de las eventuales rectificaciones de sus contenidos.

ARTÍCULO 8º.- Pónese en vigencia las versiones impresas y digitalizadas del reglamento, a partir de la difusión del aviso de su aprobación.

ARTÍCULO 9º.- Derógase en cualquiera de sus versiones – impresa y/o digital – a partir de la entrada en vigencia de la publicación aprobada por la presente Disposición, el reglamento "MEDIDAS DE SEGURIDAD DE CONTRAINTELIGENCIA (ROP – 11 – 06), Edición 2008, y, consecuentemente, instrúmentese lo establecido en los artículos 6.053, 6.054, 6.055 y, cuando corresponda, 6.056 del reglamento "La Doctrina en el Ejército Argentino" (RFD – 50 – 01).

ARTÍCULO 10º.- Regístrese en el Libro "Resoluciones y Disposiciones del EMGE", de acuerdo a lo determinado en el Artículo 5.006 del reglamento "Documentación" (RFP-70-05), y archívese en el Cuartel General del EMGE, como antecedente.

ARTÍCULO 11º.- Comuníquese y publíquese en el Boletín Público del Ejército.

DGOD
Dpto Doct
<i>[Signature]</i>
<i>[Signature]</i>
<i>[Signature]</i>
<i>[Signature]</i>

EMGE
DISPOSICION Nº 331 /14



[Signature]
General de División RUBEN OSCAR FERRARI
SUBJEFE DEL ESTADO MAYOR GENERAL DEL EJERCITO

ÍNDICE GENERAL

Página

INTRODUCCIÓN.....	I
CAPÍTULO	SEGURIDAD
Sección I	Conceptos generales..... Cap I – 1 Consideraciones básicas..... Cap I – 1
Sección II	Definiciones y conceptos asociados a la seguridad..... Cap I – 1 Seguridad..... Cap I – 1 La seguridad como principio de la conducción..... Cap I – 2 La relación entre inteligencia y seguridad..... Cap I – 2 Riesgos aplicativos a la seguridad..... Cap I – 2
CAPÍTULO II	CONTRAİNTELIGENCIA
Sección I	Conceptos generales..... Cap II – 1 Conceptos generales..... Cap II – 1 Contraİnteligencia. Definición..... Cap II – 1 Finalidad..... Cap II – 2 La contraİnteligencia y las bases jurídicos – legales..... Cap II – 2 Vigencia y alcance de la contraİnteligencia..... Cap II – 2 Conciencia de contraİnteligencia..... Cap II – 3
Sección II	Responsabilidad de contraİnteligencia..... Cap II – 3 Conceptos generales..... Cap II – 3 Responsabilidad el comandante..... Cap II – 3 Responsabilidad del jefe de inteligencia del estado mayor / plana mayor..... Cap II – 4 Responsabilidad de otros miembros del estado mayor / plana mayor..... Cap II – 4 Responsabilidad del jefe de la unidad de inteligencia..... Cap II – 4 Responsabilidad de las tropas..... Cap II – 4
CAPÍTULO III	MEDIDAS DE SEGURIDAD DE CONTRAİNTELIGENCIA
Sección I	Conceptos generales..... Cap III – 1 Definición..... Cap III – 1 Aspectos que abarcan las medidas de seguridad de contraİnteligencia.... Cap III – 1 Alcance..... Cap III – 1 Consideraciones orientadoras de las MSCİ..... Cap III – 1 Características de las MSCİ..... Cap III – 2 Fundamento de la implementación de las MSCİ..... Cap III – 3
Sección II	Definiciones y conceptos asociados a las medidas de seguridad de con- traİnteligencia..... Cap III – 3 Información del instrumento militar propio (IIMP)..... Cap III – 3 Información en el ámbito de la inteligencia militar..... Cap III – 3 Medios..... Cap III – 3 Material..... Cap III – 4 Material bélico..... Cap III – 4 Material bélico crítico..... Cap III – 4 Material clasificado..... Cap III – 4 Espionaje..... Cap III – 4 Sabotaje..... Cap III – 4 Protección de la información y medios del instrumento militar..... Cap III – 4 Seguridad de la información..... Cap III – 5 Gestión de la información..... Cap III – 5 Secreto militar..... Cap III – 5 Documento..... Cap III – 5 Las MSCİ y la guerra de la información..... Cap III – 6 Las MSCİ y las agresiones en el ciberespacio..... Cap III – 6 Los elementos de inteligencia militar y las MSCİ..... Cap III – 7 Criterios de eficiencia/medidas de seguridad de contraİnteligencia..... Cap III – 7

		Página
Sección III	Terminología e uso frecuente asociada a las MSCl.....	Cap III – 7
	Acción.....	Cap III – 7
	Actor.....	Cap III – 7
	Administración de riesgo.....	Cap III – 8
	Ámbito militar.....	Cap III – 8
	Amenazas.....	Cap III – 8
	Área.....	Cap III – 8
	Área de seguridad.....	Cap III – 8
	Área restringida.....	Cap III – 8
	Área excluida.....	Cap III – 8
	Área controlada.....	Cap III – 8
	Conocimiento.....	Cap III – 8
	Contrainteligencia.....	Cap III – 8
	Contraespionaje.....	Cap III – 8
	Contrasabotaje.....	Cap III – 8
	Evaluación del riesgo.....	Cap III – 8
	Incidente de seguridad.....	Cap III – 8
	Información.....	Cap III – 9
	Instalación militar.....	Cap III – 9
	Inteligencia.....	Cap III – 9
	Jurisdicción.....	Cap III – 9
	Jurisdicción militar.....	Cap III – 9
	Medidas.....	Cap III – 9
	Medios.....	Cap III – 9
	Operaciones de inteligencia militar.....	Cap III – 9
	Riesgo.....	Cap III – 9
	Zona de responsabilidad.....	Cap III – 9
Sección IV	Clasificación de la información.....	Cap III – 10
	Información clasificada.....	Cap III – 10
	Clasificación de seguridad (Decreto 950/02).....	Cap III – 10
	Público – Militar.....	Cap III – 10
Sección V	Barreras.....	Cap III – 10
	Barreras. Definición del concepto desde el punto de vista de las MSCl...	Cap III – 10
Sección VI	Aplicación de las medidas de seguridad de contrainteligencia.....	Cap III – 11
	Aplicación de las MSCl durante períodos de paz y durante las operaciones.....	Cap III – 11
CAPÍTULO IV	MEDIDAS DE SEGURIDAD DE CONTRAINTELIGENCIA REFERIDAS A LA SEGURIDAD FÍSICA DE LAS INSTALACIONES	
Sección I	Conceptos generales.....	Cap IV – 1
	Definición.....	Cap IV – 1
	Conceptos generales.....	Cap IV – 1
	Instalaciones militares.....	Cap IV – 1
	Personal.....	Cap IV – 1
	Particularidades de la seguridad física de las instalaciones.....	Cap IV – 2
	Identificación de las áreas de seguridad.....	Cap IV – 3
	Área de seguridad.....	Cap IV – 3
	Área controlada.....	Cap IV – 3
	Área restringida.....	Cap IV – 3
	Área excluida.....	Cap IV – 4
	El entorno y las áreas de seguridad.....	Cap IV – 5
Sección II	Barreras.....	Cap IV – 5
	Barrera.....	Cap IV – 5
	Barrera – MSCl. Definición del concepto desde el punto de vista de las MSCl.....	Cap IV – 5
	Finalidad.....	Cap IV – 5
	Clasificación de las barreras.....	Cap IV – 6
Sección III	Barreras naturales.....	Cap IV – 8
	Definición.....	Cap IV – 8
	Conceptos básicos.....	Cap IV – 8
	Terrenos accidentados.....	Cap IV – 8

	Terrenos con vegetación.....	Cap IV – 8
	Terrenos con obstáculos constituidos por espejos de agua.....	Cap IV – 8
Sección IV	Barreras humanas.....	Cap IV – 9
	Definición.....	Cap IV – 9
	Características de las barreras humanas.....	Cap IV – 9
	Guardia de prevención.....	Cap IV – 9
	Personal de vigilancia en las instalaciones.....	Cap IV – 10
	Recepcionistas y secretarios.....	Cap IV – 10
	Individuos integrantes de la organización.....	Cap IV – 10
	Fracción de seguridad de personal muy importante.....	Cap IV – 10
Sección V	Barreras animales.....	Cap IV – 10
	Definición.....	Cap IV – 10
	Características.....	Cap IV – 10
Sección VI	Barreras artificiales.....	Cap IV – 11
	Definición.....	Cap IV – 11
	Tipos de barreras artificiales.....	Cap IV – 11
Sección VII	Recursos accesorios complementarios.....	Cap IV – 16
	Definición.....	Cap IV – 16
	Consideraciones básicas.....	Cap IV – 16
	Sistema de iluminación.....	Cap IV – 17
	Método e cálculo de “fuente puntual”.....	Cap IV – 17
	Conceptos influyentes en la iluminación.....	Cap IV – 17
	Características de la iluminación.....	Cap IV – 17
	Clasificación general de los equipos de iluminación por considerar.....	Cap IV – 18
	Instalación de los sistemas de iluminación.....	Cap IV – 18
	Empleo de los sistemas de iluminación.....	Cap IV – 18
CAPÍTULO V	MEDIDAS DE SEGURIDAD DE CONTRAINTELIGENCIA REFERIDAS A LA SEGURIDAD DEL PERSONAL	
Sección I	Conceptos generales.....	Cap V – 1
	Definición.....	Cap V – 1
	Conceptos generales.....	Cap V – 1
	Personal muy importante (PMI).....	Cap V – 2
	Personal del instrumento militar con funciones críticas (PFC).....	Cap V – 2
	Personal del instrumento militar.....	Cap V – 2
	Aspectos generales que abarcan las medidas de seguridad de contrainte- ligencia referidas al personal.....	Cap V – 2
Sección II	Seguridad en relación con el conocimiento que posee.....	Cap V – 2
	Seguridad de las personas relacionada con el conocimiento que posee..	Cap V – 2
	Características propias de los individuos.....	Cap V – 3
	Proceder con el personal que se separa o se retira del servicio.....	Cap V – 5
Sección III	Seguridad física de las personas.....	Cap V – 5
	Seguridad física de las personas.....	Cap V – 5
CAPÍTULO VI	PROCEDIMIENTOS DE SEGURIDAD REFERIDOS A LA IDENTIFICA- CIÓN Y CONTROL DE PERSONAL Y MATERIALES	
Sección I	Identificación y control de personas y vehículos.....	Cap VI – 1
	Conceptos generales.....	Cap VI – 1
	Identificación de personal militar y civil del elemento.....	Cap VI – 1
	Identificación del personal ajeno al elemento.....	Cap VI – 1
	Procedimientos de control.....	Cap VI – 2
	Control de acceso y salida de personal militar y civil.....	Cap VI – 2
	Control de acceso y salida de vehículos.....	Cap VI – 3
	Control de circulación interna de personas.....	Cap VI – 3
	Áreas de estacionamiento.....	Cap VI – 4
	Control de proveedores, cantineros y contratistas.....	Cap VI – 5
	Personas o entes civiles alojados en instalaciones militares.....	Cap VI – 6
	Personal militar o autoridades extranjeras.....	Cap VI – 6

	Visita de funcionarios del propio país.....	Cap VI – 6
	Personal designado ayudante de oficiales superiores extranjeros.....	Cap VI – 7
	Estudiantes militares o civiles extranjeros que realizan cursos en institutos militares argentinos.....	Cap VI – 7
	Visitantes a fábricas y establecimientos militares que trabajan con proyectos o producen material clasificado.....	Cap VI – 8
	Proceder con periodistas.....	Cap VI – 8
Sección II	Control de instalaciones y efectos.....	Cap VI – 9
	Control en edificios, pisos y sectores.....	Cap VI – 9
	Control en locales y depósitos para la guarda de documentación, materiales y otros efectos.....	Cap VI – 9
	Control en muebles, armarios, cajas de seguridad y otros.....	Cap VI – 10
	Control en aulas, salas cinematográficas y otros.....	Cap VI – 10
	Control de talleres, depósitos, laboratorios y surtidores.....	Cap VI – 10
	Control sobre evacuación y destrucción de documentos y materiales....	Cap VI – 11
CAPÍTULO VII	MEDIDAS DE SEGURIDAD REFERIDAS A LA DOCUMENTACIÓN Y MATERIAL CLASIFICADO	
Sección I	Conceptos generales.....	Cap VII – 1
	Definición.....	Cap VII – 1
	Consideraciones básicas.....	Cap VII – 1
	Seguridad de la información documentada.....	Cap VII – 1
	Información documentada.....	Cap VII – 1
	Información oficial.....	Cap VII – 1
Sección II	Normas de seguridad de contrainteligencia que rigen la confección y el tratamiento de la documentación.....	Cap VII – 1
	Normas de seguridad a aplicar sobre la información documentada.....	Cap VII – 1
	Clasificación. Determinación de la clasificación de seguridad de la información documentada.....	Cap VII – 2
	Escala de clasificación de la información.....	Cap VII – 2
	Imposición de la clasificación de seguridad.....	Cap VII – 3
	Identificación de documentos.....	Cap VII – 5
	Vicios de identificación.....	Cap VII – 6
	Reclasificación.....	Cap VII – 6
	Elaboración y tramitación.....	Cap VII – 7
	Determinación del distribuidor.....	Cap VII – 8
	Reproducción.....	Cap VII – 8
	Registro.....	Cap VII – 9
	Usuario de documentación clasificada.....	Cap VII – 9
	Archivo, custodia y guarda.....	Cap VII – 9
	Entrega y recepción de la información documentada.....	Cap VII – 10
	Control de entrada y salida de documentación.....	Cap VII – 10
	Transmisión de la información.....	Cap VII – 11
	Destrucción de documentación clasificada.....	Cap VII – 11
	Evacuación de la información documentada.....	Cap VII – 12
	Responsabilidades en el control de la información.....	Cap VII – 12
	Transgresiones a las normas de seguridad.....	Cap VII – 13
Sección III	Medidas de seguridad referidas al material.....	Cap VII – 13
	Consideraciones básicas.....	Cap VII – 13
	Material clasificado.....	Cap VII – 13
	Criterios de clasificación de material clasificado.....	Cap VII – 13
	Criterios de responsabilidad del material clasificado.....	Cap VII – 13
	Responsabilidades sobre material clasificado.....	Cap VII – 13
	Seguridad del material criptográfico.....	Cap VII – 13
	Transporte y guarda del material.....	Cap VII – 13
	Transgresiones a las normas de seguridad.....	Cap VII – 14
CAPÍTULO VIII	MEDIDAS DE SEGURIDAD REFERIDAS A LAS COMUNICACIONES	
Sección I	Conceptos generales.....	Cap VIII – 1
	Definición.....	Cap VIII – 1
	Consideraciones básicas.....	Cap VIII – 1

	Factores que influyen en la seguridad de las comunicaciones.....	Cap VIII – 1
	Conceptos asociados por tener en cuenta.....	Cap VIII – 2
	Responsabilidades y misiones.....	Cap VIII – 2
	Responsabilidades del oficial de inteligencia.....	Cap VIII – 3
	Responsabilidades del oficial de operaciones.....	Cap VIII – 3
Sección II	Estudio de seguridad de comunicaciones.....	Cap VIII – 3
	Evaluación de las vulnerabilidades de los sistema de comunicaciones.....	Cap VIII – 3
Sección III	Protección en las transmisiones.....	Cap VIII – 6
	Definición.....	Cap VIII – 6
	Procedimientos para la protección de las transmisiones.....	Cap VIII – 6
CAPÍTULO IX	MEDIDAS DE SEGURIDAD REFERIDAS A LA CRIPTOLOGÍA	
Sección I	Conceptos generales.....	Cap IX – 1
	Definición.....	Cap IX – 1
	Glosario de términos.....	Cap IX – 1
	Consideraciones básicas.....	Cap IX – 1
	Capacidades atribuidas al enemigo u oponente.....	Cap IX – 1
	Debilidades el sistema.....	Cap IX – 2
	El material criptográfico y su clasificación de seguridad.....	Cap IX – 2
Sección II	Responsabilidades.....	Cap IX – 2
	Responsabilidades del jefe de elemento.....	Cap IX – 2
	Responsabilidades del oficial de claves.....	Cap IX – 3
	Responsabilidades de los usuarios.....	Cap IX – 3
	Vigencia de la responsabilidad en caso de relevo.....	Cap IX – 3
Sección III	Seguridad física del material.....	Cap IX – 3
	Seguridad física.....	Cap IX – 3
	Cajas fuertes, cofres y armarios metálicos.....	Cap IX – 4
	Cifrarios.....	Cap IX – 5
	Almacenamiento, manipulación y custodia del material clasificado.....	Cap IX – 5
	Lugar de instalación de los equipos criptológicos.....	Cap IX – 6
	Transporte del material criptográfico.....	Cap IX – 6
	Remisión del material criptográfico.....	Cap IX – 7
	Mantenimiento de equipos criptológicos.....	Cap IX – 7
Sección IV	Destrucción del material criptográfico.....	Cap IX – 7
	Consideraciones básicas.....	Cap IX – 7
	Procedimiento para la destrucción de rutina.....	Cap IX – 7
	Destrucción de emergencia.....	Cap IX – 7
CAPÍTULO X	MEDIDAS DE SEGURIDAD REFERIDAS A INFORMÁTICA	
Sección I	Conceptos generales.....	Cap X – 1
	Definición.....	Cap X – 1
	Glosario de términos informáticos.....	Cap X – 1
	Consideraciones básicas.....	Cap X – 2
	Criterios de uso.....	Cap X – 2
	Vulnerabilidad e los sistemas informáticos.....	Cap X – 2
	Dispositivos informáticos.....	Cap X – 3
	Incidentes de seguridad informática.....	Cap X – 4
Sección II	Seguridad física.....	Cap X – 5
	Conceptos generales.....	Cap X – 5
	Provisión de energía.....	Cap X – 5
	Consideraciones en los cableados.....	Cap X – 5
	Sistemas de refrigeración.....	Cap X – 6
	Prevención contra incendios.....	Cap X – 6
Sección III	Seguridad de los sistemas operativos.....	Cap X – 6
	Planificación y aprobación de sistemas.....	Cap X – 6
	Intercambios o cesión de sistemas de información y software.....	Cap X – 6
	Los programas informáticos.....	Cap X – 7

	Sistema de transmisión de datos.....	Cap X – 7
Sección IV	Seguridad de la información.....	Cap X – 8
	Seguridad de la información documentada bajo formato digital.....	Cap X – 8
	Mantenimiento. Copia de resguardo de la información.....	Cap X – 8
Sección V	Seguridad de los dispositivos informáticos.....	Cap X – 8
	Clasificación general.....	Cap X – 8
	Protección del equipamiento físico.....	Cap X – 8
	Seguridad de terminales.....	Cap X – 9
	Accesos desde equipos terminales a un equipo central.....	Cap X – 10
	Centros de cómputos.....	Cap X – 10
	Seguridad en computadoras personales. Conceptos generales.....	Cap X – 11
	Protección de la computadora.....	Cap X – 11
	Dispositivos de almacenamiento removible. Medidas de protección.....	Cap X – 13
	Destrucción y/o eliminación de información bajo formato digital.....	Cap X – 14
	Destrucción y/o eliminación de dispositivos de almacenamiento en desuso.....	Cap X – 14
Sección VI	Seguridad de usuarios.....	Cap X – 15
	Conceptos generales.....	Cap X – 15
	Registro de usuarios.....	Cap X – 15
	Administración de contraseñas de usuarios.....	Cap X – 16
	Administración de contraseñas críticas.....	Cap X – 16
	Revisión de derechos de accesos de usuarios.....	Cap X – 17
	Responsabilidades del usuario. Contraseñas.....	Cap X – 17
	Equipos desatendidos en áreas de usuarios.....	Cap X – 17
Sección VII	Seguridad de redes informáticas.....	Cap X – 18
	Conceptos generales.....	Cap X – 18
	Control de acceso a la red.....	Cap X – 18
	Camino forzado.....	Cap X – 18
	Autenticación de usuarios para conexiones externas.....	Cap X – 19
	Autenticación de nodos.....	Cap X – 19
	Protección de los puertos (ports) de diagnóstico remoto.....	Cap X – 19
	Subdivisión de redes.....	Cap X – 19
	Control de ruteo de red.....	Cap X – 19
	Redes inalámbricas.....	Cap X – 19
	Seguridad de los servicios de red.....	Cap X – 19
Sección VIII	Seguridad en internet.....	Cap X – 20
	Conceptos generales.....	Cap X – 20
	Sistemas de acceso público. Protección de la información publicada electrónicamente.....	Cap X – 21
	Control de software malicioso.....	Cap X – 21
CAPÍTULO XI	MEDIDAS DE SEGURIDAD EN APOYO A LAS OPERACIONES	
Sección I	Conceptos generales.....	Cap XI – 1
	Conceptos generales.....	Cap XI – 1
	Seguridad de las operaciones.....	Cap XI – 1
	Alcance de la aplicación de las medidas de seguridad de contrainteligencia.....	Cap XI – 1
	Responsabilidades.....	Cap XI – 2
Sección II	Planeamiento.....	Cap XI – 2
	Conceptos básicos.....	Cap XI – 2
	Fase preliminar.....	Cap XI – 3
	Primera etapa del PPC “Determinación del plan general” (dentro de la Fase preliminar).....	Cap XI – 3
	Segunda etapa del PPC “Desarrollo del plan general”.....	Cap XI – 5
	Tercera etapa del PPC “Elaboración de la orden”.....	Cap XI – 6
	Cuarta etapa del PPC “Supervisión de la acción”.....	Cap XI – 6
	Dirección.....	Cap XI – 6
	Secuencia para la determinación y aplicación de las medidas de seguridad en las operaciones.....	Cap XI – 7

Sección III	Evaluaciones de seguridad en actividades de campaña.....	Cap XI – 11
	Conceptos básicos.....	Cap XI – 11
	Objeto de las evaluaciones.....	Cap XI – 11
	Fases de la evaluación.....	Cap XI – 12
	Planeamiento.....	Cap XI – 12
	Evaluación en el terreno.....	Cap XI – 13
	Informe final.....	Cap XI – 15
CAPÍTULO XII	PLANEAMIENTO, SUPERVISIÓN Y CONTROL DE LAS MEDIDAS DE SEGURIDAD DE CONTRAINTELIGENCIA	
Sección I	Planeamiento de las MSCI.....	Cap XII – 1
	Aspectos generales.....	Cap XII – 1
	Planeamiento estratégico militar conjunto y específico.....	Cap XII – 1
	Planeamiento a nivel operacional y táctico.....	Cap XII – 1
	Recurrencia de los planes.....	Cap XII – 1
	Responsabilidades.....	Cap XII – 1
Sección II	Información documentada de contrainteligencia.....	Cap XII – 2
	Conceptos generales.....	Cap XII – 2
	Apreciación de situación de contrainteligencia.....	Cap XII – 2
	Bases de trabajo para el desarrollo de la apreciación de situación de contrainteligencia.....	Cap XII – 2
	Plan de obtención de contrainteligencia.....	Cap XII – 3
	Plan de medidas de seguridad de contrainteligencia.....	Cap XII – 3
	Carta de hechos que afectan a la fuerza (desde el punto de vista de las medidas de seguridad de contrainteligencia).....	Cap XII – 3
	Carta de situación de ataques cibernéticos.....	Cap XII – 3
Sección III	Supervisión de las medidas de seguridad de contrainteligencia.....	Cap XII – 4
	Conceptos generales. Definición.....	Cap XII – 4
	Control de las medidas de seguridad de contrainteligencia.....	Cap XII – 4
CAPÍTULO XIII	ESTUDIOS E INSPECCIONES DE SEGURIDAD	
Sección I	Conceptos generales.....	Cap XIII – 1
	Conceptos generales.....	Cap XIII – 1
	El estudio de seguridad. Definición.....	Cap XIII – 1
	La inspección de seguridad. Definición.....	Cap XIII – 1
	Responsabilidades. Alcance.....	Cap XIII – 1
Sección II	Estudios de seguridad.....	Cap XIII – 2
	La oportunidad de ejecución.....	Cap XIII – 2
	Planeamiento.....	Cap XIII – 2
	Estudios de seguridad especiales.....	Cap XIII – 4
Sección III	Inspecciones de seguridad.....	Cap XIII – 5
	Consideraciones básicas.....	Cap XIII – 5
	Responsabilidades.....	Cap XIII – 5
	Ejecución de la inspección de seguridad.....	Cap XIII – 5
CAPÍTULO XIV	EDUCACIÓN E INSTRUCCIÓN DE MEDIDAS DE SEGURIDAD DE CONTRAINTELIGENCIA	
Sección I	Conceptos generales.....	Cap XIV – 1
	Conceptos generales.....	Cap XIV – 1
	Definiciones de interés.....	Cap XIV – 1
Sección II	Planeamiento.....	Cap XIV – 2
	El planeamiento de educación e instrucción de las medidas de seguridad de contrainteligencia.....	Cap XIV – 2
Sección III	Responsabilidades.....	Cap XIV – 2
	Responsabilidad en la educación e instrucción del personal.....	Cap XIV – 2

Sección IV	Objetivos educativos.....	Cap XIV – 3
	Objetivo de la educación e instrucción.....	Cap XIV – 3
	Consideraciones generales.....	Cap XIV – 3

ANEXOS

Anexo 1	Legislación vinculada al secreto militar.....	Anexo 1 – 1
Anexo 2	Modelo de carteles para la identificación de áreas de seguridad.....	Anexo 2 – 1
Anexo 3	Modelo de credencial del organismo.....	Anexo 3 – 1
Anexo 4	Modelo de ficha de control de tránsito de personal en instalaciones militares.....	Anexo 4 – 1
Anexo 5	Modelo de tarjeta de circulación.....	Anexo 5 – 1
Anexo 6	Modelo de ficha de control de circulación de personal en instalaciones militares con mucha circulación.....	Anexo 6 – 1
Anexo 7	Modelo de ficha índice de documentos en custodia.....	Anexo 7 – 1
Anexo 8	Modelo de registro de seguridad de manipulación de información documentada clasificada.....	Anexo 8 – 1
Anexo 9	Modelo de recibo de autorización de ingreso o egreso de documentación y material clasificado del elemento u organismo.....	Anexo 9 – 1
Anexo 10	Acta de eliminación de documentos (Boletines, documentos de todo tipo clasificados o sin clasificar, etc.).....	Anexo 10 – 1
Anexo 11	Graficación de los emisores desplegados en el terreno.....	Anexo 11 – 1
Anexo 12	Graficación de los lóbulos de emisión.....	Anexo 12 – 1
Anexo 13	Graficación del PEEM del elemento en consideración.....	Anexo 13 – 1
Anexo 14	Cartel de advertencia sobre la vulnerabilidad de los sistemas de comunicaciones.....	Anexo 14 – 1
Anexo 15	Modelo de apreciación de situación de medidas de seguridad de contrainteligencia.....	Anexo 15 – 1
Anexo 16	Guía para la confeccionar un informe sobre un estudio o inspección de seguridad.....	Anexo 16 – 1
Anexo 17	Modelo de informe e un estudio de seguridad.....	Anexo 17 – 1
Anexo 18	Formato del plan de medidas de seguridad de contrainteligencia	Anexo 18 – 1

INTRODUCCIÓN

I. FINALIDAD

Fijar las bases que orienten las actividades vinculadas a la aplicación de Medidas de Seguridad de Contrainteligencia y establecer normas comunes que permitan satisfacer las exigencias del Planeamiento y el Accionar Militar Conjunto, y de la conducción específica, cualquiera fuere el nivel que se trate, para otorgar el carácter sistémico que impone su aplicación eficaz en el marco del Instrumento Militar.

II. CARÁCTER

Tendrá carácter rector para todas las actividades y documentos vinculados a las temáticas que involucren la aplicación de las Medidas de Seguridad de Contrainteligencia que se produzcan en el ámbito específico de la Fuerza.

La clasificación de seguridad “RESERVADO”, otorgada a la publicación, permitirá su difusión amplia en el ámbito del Ejército Argentino, de manera que se facilite el acceso a todos los responsables involucrados en la concepción, determinación, implementación y control de las Medidas de Seguridad de Contrainteligencia, y a la vez se preserve lo que su contenido pudiera significar en términos de facilidades para la determinación de debilidades propias.

III. ALCANCE

De acuerdo con su finalidad y carácter, contiene los conceptos que hacen al planeamiento, ejecución, supervisión y control de Medidas de Seguridad de Contrainteligencia, para todos los niveles de conducción dentro del ámbito militar, cualesquiera fueren su situación, en términos de localización (jurisdicción nacional o exterior), magnitud y/o marco de conflictividad en que deba desempeñarse.

IV. BASES

- A. PC-00-02 “GLOSARIO DE TÉRMINOS DE EMPLEO MILITAR PARA LA ACCIÓN MILITAR CONJUNTA”.
- B. PC-00-01 “DOCTRINA BASICA PARA LA ACCIÓN MILITAR CONJUNTA”.
- C. PC-12-04 “MEDIDAS DE SEGURIDAD DE CONTRAINTELIGENCIA PARA LA ACCIÓN MILITAR CONJUNTA”.
- D. PC-12-01 “INTELIGENCIA PARA LA ACCIÓN MILITAR CONJUNTA”.
- E. ROB-00-01 “REGLAMENTO DE CONDUCCIÓN PARA EL IMT” Edición 2001.
- F. ROP-11-06 “MEDIDAS DE SEGURIDAD DE CONTRAINTELIGENCIA” Edición 2008.
- G. RFD-50-01 “LA DOCTRINA EN EL EJÉRCITO ARGENTINO”.
- H. ROD-11-01 “INTELIGENCIA TÁCTICA”.
- I. RFD-99-01 “TERMINOLOGÍA CASTRENSE DE USO EN EL EA” Edición 2001.
- J. Ley 25.520, de Inteligencia Nacional.
- K. Decreto 950/2002 de la Ley de Inteligencia Militar 25.520.

L. Ley 24.059 de Seguridad Interior.

M. Decreto 1273/92 de la Ley 24.059 de Seguridad Interior.

N. Ley 23.554 de Defensa Nacional.

O. Decreto 727/06 de la Ley de Defensa Nacional.

P. Resolución Ministerial 381/06 (Ministerio de Defensa).

Q. Resolución Ministerial 386/06 (Ministerio de Defensa).

R. Resolución Ministerial 699/06 (Ministerio de Defensa).

S. Resolución Ministerial 1233/09 (Ministerio de Defensa).

V. NECESIDADES QUE SATISFACE

Actualizar las prescripciones reglamentarias vinculadas a las Medidas de Seguridad de Contrainteligencia en el ámbito del Ejército Argentino y, simultáneamente, adecuarlas a las prescripciones que rigen el planeamiento y accionar del Instrumento Militar para la Acción Militar Conjunta.

Expresar la normativa general para la aplicación de las Medidas de Seguridad de Contrainteligencia en el ámbito del Ejército Argentino, en todos los niveles de comando, y su aplicación en cualquier situación o lugar en que se encuentre la Fuerza.

Determinar procedimientos para la instrumentación de las Medidas de Seguridad de Contrainteligencia.

Establecer las bases para la instrucción de seguridad del personal de la Fuerza.

CAPÍTULO I

SEGURIDAD

SECCIÓN I

CONCEPTOS GENERALES

1.001. Consideraciones básicas. La protección de la información y medios del Instrumento Militar (IM) de la acción de los sistemas de Inteligencia de aquellos actores que representen amenazas o riesgos para la seguridad del Estado Nacional constituye uno de los problemas más complejos que este afronta, por la cantidad y variedad de situaciones en que sus elementos se encuentran o pueden encontrarse involucrados, que propician la generación de oportunidades para que esos sistemas hostiles intenten llegar a ellos y así poder usufructuar en beneficio propio el acceso a información o causar daño inmediato o mediato a los sistemas militares.

Los sistemas de Inteligencia desarrollan actividades en forma constante y encuentran, en los períodos de paz, múltiples oportunidades para lograr su cometido, por la menor atención que pareciera otorgarse a la protección de la información y materiales clasificados, cuando la acción de esos sistemas no es percibida por la distensión que caracteriza a dichos períodos.

Durante momentos de tensión, crisis y, fundamentalmente, de guerra, la propia dinámica que adquiere el Instrumento Militar multiplica su nivel de exposición a la acción de la Inteligencia extranjera, aun cuando naturalmente se adopten con mayor intensidad acciones de protección.

Tres situaciones incrementan complejidad a lo planteado:

- a. La constante aparición y renovación de tecnologías que se presentan como opciones para cumplir con el cometido de los sistemas de Inteligencia de los diferentes actores.
- b. La creciente tendencia de las sociedades, en las que se insertan los integrantes del IM, a compartir sin discreción una cantidad significativa de los actos de sus vidas, tanto personales como laborales y sociales.
- c. La integración sistémica del IM, que presenta a toda debilidad existente en la protección de información y materiales clasificados como una puerta de acceso para el accionar no deseado, con el consecuente riesgo para todo el IM.

En orden a lo expresado, la transversalidad del ciberespacio en las actividades del IM conforma un nuevo desafío para la protección de su información y medios clasificados.

En este escenario, las medidas de seguridad de contrainteligencia (MSCI) constituyen el primer escalón para alcanzar la protección de personal, información y materiales clasificados, y por ello todos los integrantes del IM están involucrados, ciertamente con diferentes responsabilidades, pero todos ineludiblemente con alguna.

La naturaleza pasiva adjudicada a las medidas de seguridad de contrainteligencia no debe llevar a error y resignar una actitud proactiva en la implementación y perfeccionamiento de ellas, ya que esa condición solo indica que no se orientan a la búsqueda del enemigo que potencialmente pretenda vulnerar la seguridad informativa propia, sino a disuadir, impedir y/o rechazar su posible iniciativa, mediante obstáculos de diversa naturaleza contra ese accionar no deseado, en el ámbito de la propia Jurisdicción Militar.

SECCIÓN II

DEFINICIONES Y CONCEPTOS ASOCIADOS A LA SEGURIDAD

1.002. Seguridad. Es el conjunto de recaudos para limitar o anular los riesgos y efectos de una amenaza. Se materializa en la adopción de medidas y procedimientos destinados a evitar en lo posible la materialización de los eventos mencionados, y las consecuencias que de ellos pudieran derivarse (PC -0-02).

Conceptualmente, el término engloba las diferentes situaciones que pueden significar la materialización de riesgos o amenazas para el Instrumento Militar. En tal sentido, puede distinguirse una Seguridad Operacional, cuando se focalice la protección de porciones del IM en el desarrollo de operaciones militares, una Seguridad de Instalaciones, cuando el foco sea la protección de los emplazamientos militares, una Seguridad Sanitaria, cuando la atención se centre en el cuidado del personal frente a ciertas características o condiciones del ambiente geográfico, hostiles para la salud humana, entre otras.

1.003. Se identifica a la Seguridad de la Información cuando el interés se concentra en la protección de aquella información clasificada que nutre al Sistema Militar y es necesario evitar que pueda ser conocida por terceros actores, porque ello expondría al IM a que sus capacidades sean anuladas, reducidas u orientadas a producir efectos no deseados.

1.004. La seguridad como principio de la conducción. Se define como el resultado de la adopción de un conjunto de medidas destinadas a prevenir la sorpresa, preservar la libertad de acción y negar al enemigo información sobre las propias fuerzas (ROB-00-01 Reglamento de Conducción para el Instrumento Militar Terrestre).

1.005. La Relación entre inteligencia y seguridad. La inteligencia constituye el conocimiento, basado en la experiencia, indispensable para el desarrollo del planeamiento y la ejecución de operaciones o actividades en apoyo de los elementos de la fuerza, en todos los niveles de conducción.

En todo sentido, la inteligencia es contribuyente a la implementación de las medidas, procedimientos y acciones destinadas a proporcionar alertas con los lapsos temporales rentables, ante la existencia real de amenazas o riesgos que afecten instalaciones y recursos (humanos y materiales) de la Fuerza.

Aplicados estos conceptos al entorno operacional, a la luz de principios lógicos de la conducción, serán esenciales para la preservación del poder de combate y se plasman en medidas y procedimientos adoptados para prevenir sorpresas, preservar la libertad de acción y negar información al oponente sobre las propias tropas.

Alguno de los conceptos que rigen el funcionamiento de la seguridad se caracterizan principalmente por su adaptación a cualquier situación o contexto, proporcionando a los responsables de la conducción una base para la planificación de actividades de seguridad y la previsión para la asignación de recursos.

- a. Amplitud Dimensional: La seguridad debe orientarse SIEMPRE a ser continua, asimétrica, considerar amenazas, riesgos y peligros en todas direcciones, en todo momento y en diferentes escenarios.
- b. Multiplicidad: El análisis de inteligencia aplicado a las capacidades de la seguridad debe considerarse en barreras simultáneas que proporcionen fuerza y profundidad al conjunto.
- c. Superposición de medios: La integración de subsistemas específicos de inteligencia facilita el logro del efecto de potenciar el concepto de seguridad, a través de la redundancia de los distintos medios.
- d. Integración: El concepto de seguridad permite combinar las acciones de inteligencia, subsistemas, capacidades y esfuerzos propios de los Elementos, estén asociados o no a las operaciones militares, otorgando resistencia y estructura en su conjunto.
- e. Confiabilidad del hombre: El grado de idoneidad e identificación con los objetivos de la fuerza será determinante en la estructura de la seguridad. En función de sus actitudes y acciones, ante una situación en particular, será capaz de alcanzar una opinión favorable basada en la confianza.

A lo largo del tiempo, la seguridad, como principio de la conducción, ha influido en el planeamiento y la ejecución de las operaciones militares, y, actualmente, se mantiene e incrementa su importancia, constituyéndose en una premisa que no debe dejar de observarse.

1.006. Riesgos aplicativos a la seguridad. El régimen funcional de la Fuerza en todos sus niveles impone confeccionar, tramitar y difundir directivas, planes, órdenes y comunicaciones, así como material de distinto carácter según su contenido. Esa Información, desde el momento que se la comienza a tramitar hasta que llega al último destinatario previsto, podrá pasar por intermediarios que, en una u otra forma, constituyen una cadena de enlaces.

Esto constituirá diversos puntos que, en mayor o menor medida, facilitarán la difusión indebida de Información. El hombre es siempre el eslabón más débil de la citada cadena de enlaces y será el responsable de permitir que ese conocimiento llegue a determinados actores, más, por las facilidades que se le presentan para su obtención que por un gran despliegue de medios de ejecución.

En consecuencia, surge la necesidad de mantener la más absoluta reserva de todo aquello que es visto o contemplado dentro del ámbito militar. La correcta aplicación de la “disciplina del secreto” será el método que habrá de ejercitarse, con mayor severidad, para garantizar al máximo su efectividad.

Ello se logrará mediante la adecuada educación e instrucción del personal en los siguientes aspectos:

- a. El afianzamiento del concepto de discreción en toda circunstancia por parte del personal.
- b. La determinación de las responsabilidades en la ejecución de las tareas.
- c. El cuidado de la información y limitación en el conocimiento de esta.
- d. El estricto cumplimiento de las órdenes que se hayan impartido a tal efecto.
- e. La sanción de quienes violen las órdenes, normas y disposiciones que lo preservan.

Aunque el riesgo principal de la seguridad se materialice por las fallas de las medidas de seguridad de contrainteligencia adoptadas, existen otros riesgos configurados por las características propias de todo individuo y por la violación consciente del secreto.

- a. Características propias del individuo. Son precisamente las peculiaridades de las personas (el exceso de confianza, la vanidad, el entusiasmo y el orgullo, la ignorancia y el encono) las que pueden llegar a poner en peligro el éxito de las medidas adoptadas. Cobra especial relevancia conocer estas características del individuo de acuerdo con las responsabilidades y tareas por desarrollar dentro de una organización militar.
- b. Exceso de confianza. Generalmente, es el factor de riesgo más común. La creencia de poseer una verdadera y real conciencia de contrainteligencia, aun sobre el resto de sus pares, lleva habitualmente a cometer errores. Resulta muy difícil al hombre poder determinar en oportunidad el grado de discreción que puede tener otra persona, fundamentalmente cuando esta no está debidamente adecuada e instruida en la disciplina del secreto o cuando no pertenece a la Fuerza. El núcleo familiar y los círculos de amistades constituirán una fuente de información abundante para personal ajeno a los objetivos de la institución.

Una de las lecciones más difíciles de aprender es que la información no deberá divulgarse, aun cuando en apariencia sea insignificante o fragmentaria.

- c. Vanidad. Esta vulnerabilidad es muy fácil de explotar y constituye el factor con mejores probabilidades de llegar a la fuente de información. La exposición de sus conocimientos y/o puntos de vista, mediante la adulación o persuasión, será el procedimiento más común para aprovechar esta debilidad.
- d. Entusiasmo y orgullo. Estos factores propios del ser humano son causas comunes de indiscreción. El individuo identificado con la organización, con sus tareas diarias y responsabilidades, más si su servicio se traduce en éxitos, encuentra difícil no hablar o escribir sobre las ellas. El principal equilibrio consiste en que el entusiasmo y el orgullo, como virtud, no sobrepasen los límites de la seguridad, materializados por la imposición de no revelar información clasificada a personas no autorizadas.
- e. Ignorancia. Generalmente, información vital se disemina indebidamente por no comprender su valor y no conocer los procedimientos y medidas más adecuadas para su resguardo. La educación del sentido común de todo el personal será de vital importancia para la seguridad en su conjunto. El error más usual es interpretar que una pequeña y aislada parte de una información es demasiado insignificante para ser de algún uso para otra persona ajena a los intereses de la Fuerza.
- f. El encono. El cansancio, situaciones de estrés y resultados no esperados podrán ejercer presiones anímicas manifestadas en expresiones de encono o enojo. En ocasiones, a modo de descarga emocional, se vierten conceptos inherentes a sus actividades o tareas, que vulneran el marco de seguridad impuesto.

La educación e la instrucción en materia de Contrainteligencia serán los métodos más adecuados para combatir los errores que se han consignado.

CAPÍTULO II

CONTRAINTELIGENCIA

SECCIÓN I

CONCEPTOS GENERALES

2.001. Conceptos generales. Constituye una parte importante e inseparable de la inteligencia. La contrainteligencia es la actividad de inteligencia destinada a negar información, para proteger al personal, documentación, material, instalaciones y sistemas de comunicaciones, mediante los procedimientos tendientes a descubrir y anular o neutralizar las actividades de inteligencia de aquellos actores que representen riesgos o amenazas para la seguridad del Estado Nacional.

Inteligencia implica contrainteligencia; en tal sentido, referirse a inteligencia es referirse también a Contrainteligencia.

La contrainteligencia requerirá información de las actividades de inteligencia del enemigo que tiendan a tomar conocimiento sobre las propias fuerzas; comprende a la actividad de reunión de información, ejecutada por medio de procedimientos que realizan las unidades de las armas, tropas técnicas y servicios del enemigo u oponente, y el elemento humano considerado individualmente en su condición de medio de reunión de información.

La contrainteligencia también requerirá información sobre aquellas actividades de inteligencia que buscan disminuir o neutralizar el propio poder de combate.

La contrainteligencia requerirá toda esa información a fin de prever y adoptar las medidas pertinentes que le permitirán lograr la necesaria seguridad.

Las actividades de inteligencia, en general, estarán íntimamente relacionadas entre sí. Algunos medios y fuentes de información, empleados por inteligencia para satisfacer necesidades del conocimiento sobre el poder de combate del enemigo u adversario, servirán también a la contrainteligencia.

Se deberá tener siempre presente que la inteligencia será indispensable al enemigo en igual medida que para propias fuerzas; toda actividad de inteligencia que aquel realice deberá tener una réplica prevista. Estas medidas servirán para anularla o, por lo menos, neutralizarla. Su importancia radicarán en que los éxitos de dichas medidas facilitarán la propia conducción, que posibilitara el logro de la sorpresa, y neutralizarán o dificultarán el accionar del enemigo.

Dentro del concepto señalado, la contrainteligencia tratará permanentemente de proteger a los propios medios contra las actividades de inteligencia del enemigo mediante la localización, identificación, investigación, etc., de cualquier tipo de amenaza.

Si en su ejecución se tomara conocimiento de información que materialice un riesgo y este sobrepasare o no fuere competencia específica del organismo, dicho conocimiento se difundirá al nivel de conducción que correspondiere.

2.002. Contrainteligencia. Definición. Se define a la contrainteligencia como aquella “actividad propia del campo de la inteligencia que se realiza con el propósito de evitar actividades de inteligencia de actores que representen amenazas o riesgos para la seguridad del Estado Nacional” (Ley de Inteligencia Nacional Nro 25.520 – Art. 2º).

Los niveles superiores de conducción estratégica procurarán establecer aquellas amenazas que afecten la protección de la información clasificada del instrumento militar. En tiempo de paz, a medida que se alcance su determinación, el nivel estratégico militar difundirá la inteligencia relativa a las amenazas definidas para la seguridad de la información en jurisdicción militar, que contribuirá a la formulación de las bases de los análisis pertinentes que fundamentarán la aplicación de las medidas de seguridad de contrainteligencia (MSCI) adicionales en las distintas organizaciones que integran el instrumento militar.

En tiempo de guerra, la inteligencia se complementará con lo pertinente a la jurisdicción de cada uno de los comandos estratégicos operacionales que se determinen. Sin embargo, la ausencia de ese presupuesto (definición de amenazas) no invalida la ejecución de la actividad de contrainteligencia, dentro de la jurisdicción militar, para determinar debilidades respecto de la protección de la información sensible (clasificada) del instrumento militar. Consecuentemente, cada responsable de una organización militar fundamentará, inicialmente, la adopción de las MSCI en las debilidades para la protección de la información clasificada que presente el elemento u organismo puesto bajo su mando.

2.003. Finalidad. En los niveles estratégico militar, operacional y táctico, la finalidad de la contrainteligencia militar será la de proteger el poder militar de las actividades de inteligencia del oponente o enemigo real/potencial, para proporcionar libertad de acción a la propia conducción, siendo contribuyente al logro de la sorpresa en el empleo del propio poder militar.

2.004. La contrainteligencia y las bases jurídico-legales. Las actividades de contrainteligencia, que son de carácter permanente, deben desarrollarse en el marco que brindan la Constitución Nacional, el Código Penal de la Nación, las leyes de Defensa, Inteligencia y Seguridad Interior con sus respectivas reglamentaciones y las leyes o normas que se sancionen específicamente.

2.005. Vigencia y alcance de la contrainteligencia

a. Vigencia.

La contrainteligencia, dentro de la zona de responsabilidad, será de permanente aplicación, ya que la ejecución de las actividades de inteligencia de aquellos actores que representen amenazas o riesgos para la seguridad del Estado Nacional, no se limitarán a situaciones de conflicto violento.

El enemigo real o potencial buscará permanentemente obtener información sobre el instrumento militar para conocer nuestro poder de combate.

Siendo la inteligencia una actividad permanente, lo será también la contrainteligencia, como una consecuencia de la también permanente actividad de inteligencia del enemigo u oponente potencial o real.

b. Alcance.

La contrainteligencia será indispensable en todos los niveles de la conducción militar contribuirá para proporcionar libertad de acción a las propias tropas y para la aplicación exitosa de dos de los principios de la guerra: la seguridad y la sorpresa.

El alcance de la contrainteligencia se extenderá en relación con el nivel de comando, pero deberá abarcar a toda la Fuerza, desde el soldado, considerado individualmente.

El soldado, considerado individualmente, es un medio de ejecución, ya que puede proporcionar información sobre actividades que realice el enemigo u oponente en función de la reunión de información y otras actividades.

En gran parte, el éxito de las medidas tomadas en materia de contrainteligencia dependerán de la habilidad del soldado y de todo el personal militar para cumplirlas adecuadamente.

Como prisionero de guerra, es una valiosa fuente para los sistemas de inteligencia del enemigo u oponente. Por eso deberá también recibir instrucción sobre procedimientos de evasión y forma de proceder ante interrogatorios.

Todos los organismos son fuentes de información; ello los obliga a tomar las medidas de contrainteligencia que su situación exija, acorde con el grado de seguridad necesario, para negarle al enemigo u oponente información sobre sus propias actividades.

Algunos elementos de la fuerza, concretamente las unidades de inteligencia, tienen funciones técnicas de contrainteligencia debido a la naturaleza de las misiones que tienen asignadas.

El personal de estas unidades, en su zona de responsabilidad, brindará apoyo de combate de inteligencia (contrainteligencia) a las operaciones militares y/o actividades de los organismos.

A nivel gran unidad de combate, la contrainteligencia llevará su esfuerzo principal sobre la base de las medidas de seguridad de contrainteligencia.

A nivel gran unidad de batalla, la contrainteligencia llevará su esfuerzo principal sobre la base de la aplicación de las medidas de seguridad de contrainteligencia.

A nivel comando del componente terrestre, la contrainteligencia tendrá similares responsabilidades que para las grandes unidades de batalla, pero incrementadas en relación con la amplitud de la zona de responsabilidad y la disponibilidad de medios técnicos de inteligencia. Su acción se llevará a cabo, fundamentalmente, en la zona de comunicaciones.

El comando del componente de las fuerzas terrestres, sobre la base de las directivas y coordinación del comando del teatro de operaciones o zona de emergencia, impartirá a su vez sus directivas a fin de obtener un grado de seguridad eficaz, coordinado y cubriendo todo el ámbito de su zona de responsabilidad.

Un concepto similar se aplicará para la zona de emergencia, teniendo en cuenta que la acción de la contrainteligencia se llevará a cabo sobre todo su ámbito en forma similar.

2.006. Conciencia de contrainteligencia. Para lograr la complementación y coordinación de todos los medios y medidas que en su conjunto proporcionarán un adecuado grado de seguridad, será necesario que se inculque en todo el personal una severa “**conciencia de contrainteligencia**”. Ello implica el conocimiento exacto y reflexivo de lo que representa lograr un grado conveniente de seguridad y de los peligros que entraña la no observancia de las medidas de contrainteligencia.

En cada elemento de la fuerza se aprovechará toda oportunidad para fomentar el “**hábito de la seguridad**”, se arbitrarán los máximos recursos para mantenerlo latente. Este hábito, por su constante repetición, llegará a constituirse en costumbre, que redituará grandes beneficios, no solo para el afianzamiento de una adecuada “conciencia de contrainteligencia”, sino también para limitar los riesgos emergentes de la inobservancia de las medidas que se hubieren adoptado.

Los permanentes controles al régimen funcional, las investigaciones, las periódicas inspecciones y la educación e instrucción contribuirán a afianzar el mecanismo integral montado para brindar protección, y constituirán valiosos aportes para el mantenimiento de la “conciencia de contrainteligencia”.

SECCIÓN II

RESPONSABILIDAD DE CONTRAINTELIGENCIA

2.007. Conceptos generales. Todo el personal militar tendrá, en mayor o menor grado, responsabilidad de inteligencia, en su carácter de “elemento de Inteligencia”. De acuerdo con lo expresado en el artículo 2.001, esa responsabilidad involucra a la contrainteligencia, la que aumenta acorde con el grado y cargo que desempeñe en la fuerza. Según las funciones que se realicen, se distinguirá:

- a. La responsabilidad de los órganos de dirección de inteligencia; estrechamente relacionada con el cargo, propia del comandante, del oficial de inteligencia y de los miembros que integran el campo de inteligencia.
- b. La responsabilidad de los medios de ejecución; relacionada con el solo hecho de ser integrante de la fuerza, como individuo, o integrando un elemento.

Básicamente, en el ámbito militar existe la responsabilidad de comando la que, como tal, no podrá ser compartida ni delegada; es decir que todo comandante será responsable del logro y mantenimiento de la necesaria seguridad. Sin embargo, esta responsabilidad recaerá también, individualmente, en cada uno de los integrantes de la Fuerza a fin de alcanzar, con la complementación y cooperación de todos, la máxima eficacia.

La ausencia de una actividad operacional en la tropa no significará que el campo de inteligencia no esté en operaciones, pues las actividades de inteligencia son permanentes. El enemigo potencial o real no esperará la iniciación de posibles operaciones para recién iniciar la reunión de información o tratar de disminuir el poder de combate de propia tropa mediante la ejecución de actos de sabotaje; su acción será permanente, como lo deben ser las propias actividades de contrainteligencia.

2.008. Responsabilidad del comandante. El comandante, director o jefe será el responsable del planeamiento y ejecución de los procedimientos de contrainteligencia.

El interés y el apoyo que el comandante le preste a esta actividad y a la educación e instrucción del personal serán decisivos en la capacitación de los elementos y en la eficacia de la tarea por cumplir.

2.009. Responsabilidad del jefe de inteligencia del estado mayor/plana mayor. La responsabilidad sobre la dirección y supervisión de los procedimientos de contrainteligencia recaerá en el órgano de dirección de inteligencia del estado mayor / plana mayor.

El jefe del órgano de contrainteligencia será el principal asesor y auxiliar del oficial de inteligencia en el ejercicio de sus responsabilidades de contrainteligencia.

Sus funciones específicas se relacionarán con el planeamiento integral de contrainteligencia (para el logro y mantenimiento de la seguridad) sobre la base del conocimiento de las actividades de la propia fuerza y de las capacidades y debilidades del enemigo u oponente. Además, supervisará el cumplimiento de las medidas ordenadas.

El asesoramiento por prestar en materia de contrainteligencia se hará extensivo a todos los miembros del estado mayor.

Asimismo, propondrá al oficial de inteligencia los aspectos "de contrainteligencia que se deberán incluir en las directivas de educación e instrucción de las tropas de la gran unidad".

2.010. Responsabilidad de otros miembros del estado mayor/plana mayor. Todos los miembros del estado mayor tendrán responsabilidad en materia de contrainteligencia.

Tal responsabilidad consistirá fundamentalmente en:

- a. Asesorar sobre aspectos de su incumbencia y necesidades particulares en materia de contrainteligencia.
- b. Apoyar, con todos los medios a su alcance, la ejecución de los procedimientos de contrainteligencia.
- c. Formular requerimientos al órgano de dirección de inteligencia en función de sus propias necesidades y satisfacer los requerimientos que le sean formulados.
- d. Colaborar con el jefe de inteligencia en la supervisión del cumplimiento de las medidas ordenadas.

2.011. Responsabilidad del jefe de la unidad de inteligencia. La unidad de inteligencia que forme parte, asignada, agregada o en apoyo de una gran unidad, será el único medio técnico de inteligencia de que dispondrá el comando. El jefe de esta unidad tendrá la responsabilidad del planeamiento de detalle, ejecución y supervisión de la actividad de contrainteligencia, en cumplimiento de las órdenes y los pedidos que reciba.

En materia de contrainteligencia, sus responsabilidades serán las de proporcionar seguridad a la propia unidad y asesoramiento acerca de las medidas de seguridad de contrainteligencia a las unidades que integran la gran unidad apoyada.

2.012. Responsabilidad de las tropas. La contribución de las tropas será fundamental para el logro y mantenimiento de la seguridad, especialmente por su contacto con el enemigo u oponente durante el desarrollo de las operaciones.

La responsabilidad básica y común a todas las tropas consistirá en la estricta observancia de las medidas de contrainteligencia que se hayan ordenado.

El soldado individual, que constituirá por sí mismo una valiosa fuente de información para el enemigo, será también un eslabón muy valioso en el accionar de la contrainteligencia de toda la fuerza.

El control permanente, el grado de educación e instrucción alcanzado y el cumplimiento de las órdenes recibidas serán el método que, en su conjunto, mejor satisfará las exigencias de contrainteligencia y contribuirá a cimentar una verdadera "**conciencia de contrainteligencia**", posibilitando el logro del adecuado grado de seguridad impuesto por el comandante respectivo.

Cada soldado deberá estar convencido de que constituye un elemento necesario, básico y fundamental de todo el sistema de inteligencia de la fuerza, por su condición de medio de reunión de información y por el cumplimiento y observancia permanente de las medidas de seguridad de contrainteligencia que se dispongan.

CAPÍTULO III

MEDIDAS DE SEGURIDAD DE CONTRAINTELIGENCIA

SECCIÓN I

CONCEPTOS GENERALES

3.001. Definición. Las medidas de seguridad de contrainteligencia constituyen un procedimiento de contrainteligencia. Son las disposiciones que se adoptan para proteger el propio instrumento militar contra las actividades de inteligencia de aquellos actores que representen amenazas o riesgos a la seguridad, tendientes a negar el acceso a la información, evitando o restringiendo su difusión y protegiendo al personal, documentación, material, instalaciones y sistemas de comunicaciones que las poseen, mediante una serie de acciones tendientes a descubrir y anular o neutralizar esas actividades.

3.002. Aspectos que abarcan las medidas de seguridad de contrainteligencia

- a. Seguridad física de instalaciones.
- b. Seguridad del personal.
- c. Seguridad de documentos y material clasificado.
- d. Seguridad de las comunicaciones.
- e. Seguridad de material criptográfico.
- f. Seguridad informática.

3.003. Alcance. Las medidas de seguridad de contrainteligencia, en general, serán comunes en todos los niveles de comando y serán de aplicación en todo lugar o situación donde el instrumento militar se desenvuelva.

3.004. Consideraciones orientadoras de las MSCI. Son medidas de carácter pasivo/defensivo que se adoptan en el ámbito militar en forma permanente, bajo el presupuesto de que siempre existirá una acción enemiga, oponente o adversaria, en general, interesada en afectar la información clasificada contenida en los medios materiales y/o humanos del instrumento militar propio, u obtener información que ponga en riesgo su seguridad.

Su carácter pasivo está dado por no concentrarse en un quién y una oportunidad definidos, sino por su condición de preventivas y permanentes ante la posibilidad de iniciativas de origen externo, o eventualmente internas (integrante deshonesto o negligente de la propia organización militar).

Procuran evitar el conocimiento indebido de la propia situación y crear las condiciones de seguridad informativa (protección) más favorables frente a las operaciones ofensivas de inteligencia, operaciones psicológicas y operaciones especiales del adversario.

Las medidas de seguridad de contrainteligencia, por su carácter permanente y naturaleza preventiva, además de su articulación sistémica, constituyen el mínimo de providencias que toda organización militar debe aplicar para preservar la confidencialidad, integridad y disponibilidad de la información o elementos críticos clasificados, bajo su responsabilidad, a través de criterios normalizados que faciliten su control y permitan detectar oportunamente todo intento de vulnerar la protección de los medios propios, para impedir o reducir los efectos de la acción detectada.

Estas medidas son aplicadas sobre la base de abarcar todos los aspectos que se vinculan en la dinámica de la gestión de la información clasificada por ello se prescriben como criterios rectores y presuponen la adaptación a cada situación particular y su permanente actualización.

Las medidas de seguridad de contrainteligencia se encuadran en las operaciones de inteligencia, aún cuando constituyen una responsabilidad de comando y son ejecutadas por todo el personal de las organizaciones militares, los especialistas de inteligencia tienen un rol técnico en los estudios para la implementación y las acciones de supervisión y/o control, dado que tienen por objeto contrarrestar la acción de sistemas de inteligencia de una voluntad opuesta, explícita o no, en términos de amenaza, que al menos potencialmente procurará acceder a información protegida en todo tiempo y/o buscará incidir negativamente sobre los medios clasificados del instrumento militar.

3.005. Características de las medidas de seguridad de contrainteligencia. Las medidas de seguridad de contrainteligencia se caracterizarán, porque:

- a. Requerirán una permanente actualización.

El escenario global, con sus mutaciones permanentes y constante evolución tecnológica, impone que el proceso de adecuación para la protección de la información y los medios clasificados sostenga por lo menos igual ritmo que las principales tendencias, a fin de no constituir o mantener modelos perimidos o ineficientes de seguridad frente a la necesidad de proteger.

- b. Son de naturaleza pasiva.

La naturaleza pasiva de las medidas de seguridad de contrainteligencia debe entenderse en cuanto que no se dirigen, por propia iniciativa, hacia un actor o acciones determinadas, sino que operan ante la posibilidad de que alguna situación pueda significar una vulnerabilidad del propio instrumento militar, que resulte aprovechable para la acción de la Inteligencia del enemigo u oponente, real o potencial.

- c. Son una actividad dinámica con eminente sentido de previsión.

En cuanto que deben atender a las causas que motivan las vulnerabilidades o debilidades del sistema necesario para proteger la información.

- d. Son carácter preventivo.

Implican considerar cada amenaza o riesgo, adoptar medidas para evitar las violaciones de lo establecido y en caso de concretarse, reducir el riesgo de los efectos de su acción a través de respuestas.

- e. Existirá una estrecha relación entre lo que se debe proteger y las características particulares del ambiente operacional.

Las características del objetivo por proteger, ya sea información, personal, material o sistemas de comunicaciones, el grado de seguridad que se desee y los distintos factores que componen el ambiente operacional condicionarán las medidas de seguridad que se implementarán.

- f. Exigirán una completa integración y coordinación con los distintos planes.

Exigen una completa integración y coordinación entre sí, a fin de conformar un sistema; este aspecto incluye las medidas generales, comunes a todo el IM, y las particulares de la organización militar que se trate. Esta integración y coordinación también debe verificarse respecto de elementos superiores, dependientes y del mismo nivel del referenciado, siendo el superior el responsable de alcanzar la integración requerida.

La integración y coordinación posibilita aplicar las medidas de seguridad sobre el objetivo a partir de previsiones (causas) y de la prevención (efectos y respuestas).

- g. Se aplican en el ámbito militar.

- h. Son una responsabilidad de todo nivel de Comando.

- i. Demandan medidas de supervisión y control que contribuyan a su constante evaluación.

- j. Demandan mantener conciencia sobre que, detrás de cada hecho que afecte o pueda afectar a los elementos a proteger, es posible encontrar la acción de un enemigo, aun cuando no se haya definido su existencia como tal (actividad de Inteligencia adversaria).

3.006. Fundamento de la implementación de las MSCl. La información que se requiera proteger puede encontrarse almacenada en soportes de diversa naturaleza, bajo una multiplicidad de formatos, en objetos de diferentes dimensiones y características, y también en el conocimiento de determinadas personas, lo que genera una muy amplia gama de situaciones por resolver para alcanzar un adecuado nivel de seguridad, en orden a evitar el acceso indebido.

De la misma manera, los elementos críticos del instrumento militar, que materialicen información clasificada, pasibles de ser objeto de daño por la acción de la inteligencia del adversario, representan, también, una multiplicidad de situaciones por resolver para su preservación, conforme a su diversa naturaleza y situación.

Frente a esto, las medidas de seguridad de contrainteligencia constituyen una respuesta básica preventiva, de naturaleza pasiva/defensiva que no agota el esfuerzo de protección, pero que sí asegura un mínimo razonable de condiciones aceptables de seguridad formulado a partir de un núcleo normativo mandatorio, que opera, fundamentalmente, como un disparador para alcanzar soluciones eficaces ante la ecuación amenazas – recursos disponibles.

Es de destacar que en un mundo caracterizado por los efectos de la comunicación globalizada, con fuerte influencia de redes informáticas, cada vez más amigables con las conductas cotidianas de las personas, la condición humana continúa siendo el elemento más sensible de todo sistema de protección de la información y o materiales clasificados, sin que ello suponga subestimar el constante avance tecnológico, que otorga nuevas y mejores herramientas a quienes procuran acceder a la información.

SECCIÓN II

DEFINICIONES Y CONCEPTOS ASOCIADOS A LAS MEDIDAS DE SEGURIDAD DE CONTRAINTELIGENCIA

3.007. Información del instrumento militar propio (IIMP)

Definición: expresión mínima de contenido, respecto de un tema inherente o vinculado al Instrumento Militar Nacional (IMN) en un contexto determinado (dato contextualizado).

Por extensión también se entenderá por información a un conjunto de dichas expresiones.

La información constituye un mensaje (bajo cualquier formato adoptado) que cambia el estado de conocimiento del sujeto o sistema que la recibe.

Sobre la base de la definición expresada y considerando que el Instrumento Militar de la Nación se conforma básicamente por medios humanos y materiales, puede advertirse que la vinculación de estos medios en sus diversos niveles y circunstancias está dada por el flujo de información que circula entre ellos, y que expresa el sustento de la dinámica del sistema militar.

Un pulso radar registrado en una oportunidad dada, bases de datos logísticos, un parte de novedades de personal o material, órdenes, planes, registros de un legajo personal, un documento de doctrina, un plano, una fotografía de materiales provistos, el conocimiento alcanzado por el personal propio en el desarrollo de su función dentro del instrumento militar, archivos de Inteligencia, cuadros de organización, características de los propios sistemas de comunicaciones, estados de abastecimientos de efectos, etc., son ejemplos de lo que genéricamente se incluye bajo el concepto de información del propio instrumento militar.

Muchas veces, determinados materiales de uso militar pueden, en sí mismos, contener información, sin que ésta pueda separarse del elemento que la contiene o representa, materializando situaciones especiales al momento de evitar que pueda haber un conocimiento no deseado de ellos (identificación contenido – continente).

3.008. +Información en el ámbito de la inteligencia militar. La publicación conjunta "Diccionario para la Acción Militar Conjunta (PC-00-02) define Información como el "conocimiento específico sobre datos de la realidad que no habiendo sido sometidos a ningún proceso intelectual, salvo el requerido para su obtención, se constituyen en elementos esenciales para la producción de inteligencia".

Esta información, que es la que el propio sistema de inteligencia necesita para elaborar productos de asesoramiento para la toma de decisiones y asistencia a la conducción es originada fuera del propio instrumento militar, ya que las fuentes de información son ajenas al control de este.

La información obtenida por la inteligencia militar se transforma en información del propio instrumento militar a partir de incorporarse en los procesos que caracterizan la función de inteligencia.

3.009. Medios. Elementos con la aptitud adecuada para el logro de un determinado fin pueden ser clasificados en tres categorías:

a. Medios humanos: personal.

Constituyen el más valioso de los elementos, entre otras consideraciones, por el costo de adquisición en términos de inversión y tiempos de formación adecuados y necesarios, por lo que requieren una especial y específica administración.

b. Medios físicos: material.

Conjunto de elementos que comprenden a los bienes muebles, inmuebles (infraestructura y/o instalaciones) y semovientes, perecederos o durables, de consumo o de uso, naturales o artificiales, desde el más simple hasta el más complejo, así como de sus partes integrantes.

c. Medios orgánicos: servicios.

Conjunto de elementos que se instrumentan a través de la organización del personal, del material y de la infraestructura, para ejecutar una función básica que cubra un campo específico de la logística.

3.010. Material. Comprende todos los efectos necesarios para el equipamiento, mantenimiento, operaciones y apoyo de las actividades militares, sin distinción del propósito de su aplicación.

3.011. Material bélico. Es el material (efectos finales, partes, componentes y repuestos) correspondiente a un sistema de armas, para el combate por el fuego del instrumento militar, que comprende: las armas y los proyectiles, sus plataformas y subsistemas de apoyo: efectos de apoyo logístico (de material y personal) y de apoyo de combate (ingenieros, comunicaciones, de comando y control, informática y guerra electrónica, y de inteligencia), así como el vestuario, armamento, munición, medicamentos, equipo y raciones alimenticias de combate del individuo.

3.012. Material bélico crítico. Partes, conjuntos, componentes y efectos finales necesarios para el equipamiento, abastecimiento, mantenimiento, operaciones y apoyo a las actividades militares para garantizar la Defensa y Seguridad Nacional, que por su carácter e importancia requieren un tratamiento especial de seguridad en sus proyectos, adquisición, uso y conservación, ya que su divulgación indebida causaría un perjuicio a la Nación o interferiría la ejecución de los planes del Estado.

3.013. Material clasificado. Todo material bélico crítico, sin distinción del propósito de su aplicación, que en sí mismo constituye información y cuyo conocimiento no debe ser accesible para sistemas de inteligencia de terceros estados y consecuentemente se le ha asignado una clasificación de seguridad conforme a la información que contiene o importa.

3.014. Espionaje. Operación de inteligencia militar ofensiva, planificada y técnicamente ejecutada con el objeto de acceder al conocimiento de información no pública de un oponente, documentos y/o materiales de alta clasificación de seguridad de este.

3.015. Sabotaje. Operación de inteligencia militar ofensiva, planificada y técnicamente ejecutada con el objeto de perturbar, dañar o destruir, directa o indirectamente, los medios materiales de que dispone un oponente.

3.016. Protección de la información y medios del instrumento militar. La búsqueda de la información protegida es el núcleo central de las actividades de los sistemas de inteligencia de todos y cada uno de los instrumentos militares de los actores estatales de la comunidad internacional y, consecuentemente para ello, éstos generan sus capacidades a fin de penetrar y explotar informativamente o dañar los sistemas militares y otros asociados, que les permitan obtener ventajas respecto de adversarios, mediante operaciones que, ordinariamente, serán solo percibidas a partir de que se cancelen sus efectos.

Aun cuando la actual expansión de los flujos de comunicaciones, especialmente por medio de redes informáticas, haya puesto al alcance de la masa de la población un volumen extraordinario de información, de variada calidad, y relacionada a muchos de los temas vinculados al objeto del trabajo de los sistemas de inteligencia militar, los contenidos de máximo interés continúan fuera de estos flujos masivos, incentivando una cada vez más perfeccionada actividad de inteligencia para obtener información protegida o dañar y/o afectar su disponibilidad para los procesos de decisión y empleo militar, o la de determinados materiales o infraestructuras ligadas a las capacidades del instrumento Militar de la Nación.

Los esfuerzos del adversario para la obtención de información protegida y dañar y/o afectar elementos críticos alcanzados por el “secreto militar” imponen al instrumento militar, para impedir, limitar o atenuar sus efectos, entre otras, el desarrollo de acciones caracterizadas por exhaustivos análisis sobre lo que se debe proteger y su entorno, soluciones ingeniosas, diseño de medios adecuados, capacitación de todo el personal con mínimos básicos y segmentos de especialistas, y la adaptación de los elementos militares, en términos de cultura organizacional, a criterios que aseguren niveles aceptables de protección de la información y medios clasificados del instrumento militar.

Esas acciones desarrolladas en la propia jurisdicción militar se concretarán en medidas tendientes a negar el acceso a la información y medios clasificados, restringiendo su difusión y protegiendo documentos, materiales, instalaciones, actividades, comunicaciones y personas, de las operaciones/acciones enemigas de espionaje y sabotaje, o de otras formas más sutiles con similares fines.

Cuando se mencionan operaciones/acciones del enemigo u oponente de actividades de espionaje y sabotaje o de otras formas más sutiles con similares fines, estos deben asociarse las mismas a la actividad permanente o esporádica de actores que representen amenazas o riesgos para la seguridad del instrumento militar, en particular, y del Estado Nacional en su conjunto, independientemente de la oportunidad en que estos sean declarados formalmente por parte de la autoridad política competente.

El escenario global, con sus mutaciones permanentes y constante evolución tecnológica, impone que el proceso de adecuación para la protección de la información y los medios clasificados sostenga por lo menos igual ritmo que las principales tendencias, a fin de no constituir o mantener modelos perimidos o ineficientes de seguridad frente a la necesidad de proteger.

El desarrollo tecnológico, con sus desafíos múltiples, no debe hacer olvidar que la conducta humana, por acción u omisión, es un elemento central para el sostenimiento de la protección pretendida, razón por la cual resulta esencial la adhesión consciente de todos los medios humanos del Instrumento Militar, sin distinción de rol, función o responsabilidad jerárquica, a fin de lograr respuestas eficientes ante las acciones del adversario, tanto en la paz como en la crisis o guerra.

3.017. Seguridad de la información. Condición que se alcanza cuando se aplica un conjunto de medidas y procedimientos establecidos para el correcto manejo y control de la información clasificada, en todas las instancias de su gestión, a fin de garantizar su confidencialidad, integridad y disponibilidad en todo su ciclo de vida, así como para prevenir y detectar los posibles compromisos de aquella, que puedan afectar al instrumento militar en el cumplimiento de su misión.

En el ámbito militar, dicha condición está asociada a la finalidad de la aplicación de las medidas de seguridad de contrainteligencia: Proteger los propios medios de las actividades de inteligencia del enemigo u oponente, donde la información clasificada es el eje central, dado que el adversario utilizará cualquier forma para acceder a ella o inhabilitar su uso propio. Especialmente, se identificará con la seguridad de documentos y material clasificado, y la seguridad del personal (en términos de acceso a información clasificada).

3.018. Gestión de la información. Conjunto de acciones que abarcan la elaboración, almacenamiento, custodia, proceso, utilización, presentación, reproducción, acceso, transporte, transmisión y/o destrucción de la información clasificada, sea cual fuere el método empleado.

En el ámbito militar, dicho conjunto de acciones se encuentra regulado por varias publicaciones que definen procedimientos, conforme a que la información se encuentra materializada bajo diferentes formas e integrada en múltiples subsistemas, pero todos ellos son alcanzados por las bases orientadoras de las MSCI.

3.019. Secreto militar. La legislación vigente define al secreto militar como “toda noticia, informe, material, proyecto, obra, hecho, asunto que deba, en interés de la Seguridad Nacional y de sus medios de defensa, ser conocido solamente por personas autorizadas y mantenido fuera del conocimiento de cualquier otra”.

La divulgación del secreto militar es una conducta punible conforme a la legislación nacional (ver Anexo 1).

3.020. Documento. El término “documento” comprende toda representación de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento, archivo o transmisión. (Incorporado por el Art 1° de la Ley N° 26.388, B.O. 25/6/2008, al Art. 77 de la Ley 11.179-Código Penal de la Nación Argentina).

3.021. Las MSCI y la guerra de la información. La guerra de la información (GI), tal como lo establece la PC-00-02, se orienta a “conseguir una ventaja competitiva sobre un oponente”, mediante el “uso y manejo de la información”, pudiendo para ello “adquirir diversas formas”.

Esta situación propone un escenario multidimensional de abordaje de la disputa por el control de la información, lo que desde el punto de vista de las medidas de seguridad de contrainteligencia advierte sobre la necesidad de fortalecer su aplicación, sobre la base de mayores y mejores diagnósticos de la situación de la información sensible (clasificada) para el instrumento militar, y la aplicación de tecnología actualizada para lograr el efecto de protección, dado lo central que ella es para esta modalidad bélica (guerra de la información), que se evidencia como preponderante en el conflicto moderno.

Si bien los objetivos de la guerra de la información pueden verificarse a lo largo de toda la historia militar, es la evolución de la tecnología sostenida en las últimas décadas la que amplió el horizonte de los servicios informáticos y las comunicaciones, otorgándoles a estas características de multimedia (imagen, sonido, texto, animación, etc.), instantánea (tiempo real), global (alcance prácticamente ilimitado), recíprocas (verificable en cualquier sentido del vínculo emisor receptor), interactivas, múltiples y/o masivas.

3.022. Las MSCI y las agresiones en el ciberespacio. Desde hace por lo menos dos décadas, el ciberespacio, entendido como ámbito virtual en el que se desarrollan actividades de procesamiento, almacenamiento y explotación relacionada con los datos e información digital, a través de redes interdependientes e interconectadas, software y firmware de dispositivos, ha ido alcanzando mayor presencia en los sistemas militares y de la sociedad en general.

El reconocimiento de la existencia de este nuevo ámbito otorga relevancia a la necesidad de dotarse de una adecuada capacidad de gestionar información en el ciberespacio, con aceptables niveles de protección frente a posibles agresiones y a la vez cerrar las posibilidades de acceso para quienes intenten ingresar en sistemas propios sin estar autorizados para hacerlo.

Lo “ciber” es transversal a prácticamente todas las actividades humanas, en forma directa o asociada en forma concurrente.

Gran parte de la información del instrumento militar circula por redes informáticas, algunas del tipo exclusiva y propietaria, y otras con vinculación a las que son de acceso por parte de terceros no integrantes. En este último concepto deben incluirse a los prestadores particulares / estatales fuera de la responsabilidad directa del Instrumento Militar.

Frente a este avance tecnológico, tal como ha sucedido con otros, las medidas de seguridad de contrainteligencia también requieren incorporar conocimiento y tecnología para continuar cumpliendo su función, habilitando nuevas especialidades concurrentes, siendo la disponibilidad de medios humanos altamente calificados factor de éxito determinante, pero siempre sobre la premisa que quien procura utilizar las ventajas de este nuevo ámbito para acceder a información protegida del propio instrumento militar o generar daño a sus sistemas será, potencialmente, parte de algún sistema de Inteligencia extranjero, aun cuando su identificación sea difusa, incierta o directamente imposible.

En el sentido de lo expresado en el párrafo anterior, no deberán subvalorarse indicios del accionar de cualquiera de las fuentes de amenaza cibernética que primariamente pueden distinguirse, tales como:

- Hacker, cracker.
- Delincuente informático.
- Terrorista.
- Insiders.
- Espionaje industrial.
- Espionaje militar.
- Sabotaje militar.

Todas estas fuentes de amenaza cibernética parten de un acceso no deseado a los sistemas del Instrumento Militar, que facilita la producción de diferentes efectos sobre la propia información clasificada o sistemas críticos.

3.023. Los elementos de inteligencia militar y las MSCI

El carácter de especialistas en la protección de información que poseen las organizaciones de inteligencia del sistema de inteligencia militar conjunto (SIMC) las constituyen en los asesores más calificados de los que dispondrá todo comandante o jefe para cumplir su responsabilidad de implementación de las medidas de seguridad de contrainteligencia. En tal sentido, su participación distinguirá tres situaciones diferenciadas:

a. Diagnóstico.

Oportunidad caracterizada por la ejecución de estudios de seguridad y/o apreciaciones de inteligencia, a partir de los cuales se establecen las necesidades de implementar, mejorar, sustituir o desactivar medidas de seguridad de contrainteligencia.

b. Implementación.

Oportunidad en que se concreta la adopción de las medidas de seguridad de contrainteligencia y que requiere asesoramiento de detalle para la formulación de las directivas que permitan su incorporación sistémica a las organizaciones de la jurisdicción militar y la supervisión técnica de su adecuado funcionamiento. La implementación de estas medidas materializa el inicio del efecto de protección procurado.

c. Supervisión.

Oportunidad de aplicación de procesos de auditoría sistemática o asistemática, conforme a lo determinado por el comandante, director o jefe de la organización militar que se trate, y/o el escalón de comando superior, con el fin de evaluar la eficacia y el grado de cumplimiento de las medidas de seguridad de contrainteligencia vigentes.

3.024. Criterios de eficacia/medidas de seguridad de contrainteligencia. La eficacia de las MSCI depende de los siguientes criterios:

a. Objetividad.

Deben estar referidas a aspectos concretos y de fácil comprensión aplicativa.

b. Esfuerzo integral.

Exigen instrucción, permanente adiestramiento e incorporación cultural, para lograr la sinergia necesaria en toda la jurisdicción militar.

c. Continuidad en el tiempo.

Son de aplicación permanente.

d. Aplicación estricta.

Deben ser ejecutadas sin omisiones en todos los niveles y circunstancias.

SECCIÓN III

TERMINOLOGÍA DE USO FRECUENTE ASOCIADA A LAS MSCI

3.025. Acción. Es el conjunto de medidas, previsiones y actividades destinadas al logro de un objetivo (PC-00-02).

3.026. Actor. Sujeto que, según sus capacidades o recursos, procede activa o reactivamente en función de su propia racionalidad (intereses) y su motivación (actitudes) (PC-00-02).

3.027. Administración de riesgo. Se entiende por administración de riesgos al proceso de identificación, control y minimización o eliminación, a un costo aceptable, de los riesgos de seguridad que podrían afectar a la información. Dicho proceso es cíclico y debe llevarse a cabo en forma periódica.

3.028. Ámbito militar. Concepto jurisdiccional ideal que compete a las Fuerzas Armadas, que incluye un conjunto de actividades tendientes a la protección de sus instalaciones y recursos humanos y materiales.

3.029. Amenazas. Acción consciente y deliberada de un actor que, teniendo capacidad, muestra la intención o da indicio de probable concreción de un perjuicio en contra de propios intereses.

3.030. Área. Superficie terrestre y/o marítima, con sus correspondientes espacios aéreos dentro de la cual se realizan operaciones bajo un determinado comando. Puede comprender dos o más zonas (según RFP-99-01).

3.031. Área de seguridad

Se considera a toda área o superficie donde esté ubicada una instalación considerada de interés operativo, sea permanente o transitoria. La permanencia y circulación de personas en ella, está sujeta a controles y especiales restricciones de seguridad. Según su naturaleza y grado de importancia, en cuanto al material y/o documentación que contiene, puede ser: controlada, restringida y excluida (RFP-99-01).

3.032. Área restringida. Área de seguridad en la cual el acceso se encuentra debidamente normado y limitado a individuos ajenos a la organización y a cierto personal perteneciente a ella y que comprende el espacio geográfico donde se encuentran instalaciones, personal de importancia, documentación y/o materiales de alta clasificación de seguridad (RFP-99-01).

3.033. Área excluida. Es el área donde exista o se trate, en forma permanente, información de alta clasificación de seguridad. A esta solo tendrá acceso el personal que pertenezca a ella y bajo estrictos controles de seguridad, ejecutados al ingreso, en el interior y al egreso de la misma.

3.034. Área controlada. Es aquella área de seguridad que circunda áreas restringidas o áreas excluidas. También recibe esta denominación aquella área que, sin contener a las anteriores, se establece a manera de cerco con la finalidad de controlar el acceso y la limitación de la circulación. Se establece para evitar el contacto de personas ajenas a la organización con elementos que existan en ella y merezcan resguardo sin estar comprendidos en las categorías anteriores (RFP-99-01).

3.035. Conocimiento. Todo hecho, dato o información que es adquirido por una persona a través de diferentes cualidades, como la experiencia, la comprensión y el estudio de factores incidentes de la realidad. Es una apreciación de la posesión de múltiples datos interrelacionados que, en forma individual, poseen menor nivel cualitativo.

3.036. Contrainteligencia. Actividad propia del campo de inteligencia que se realiza con el propósito de evitar actividades de inteligencia de aquellos actores que representen riesgos o amenazas para la seguridad del Estado Nacional (Ley Nro 25.520 - Art 2º y PC-00-02).

3.037. Contraespionaje. Actividad propia del campo de inteligencia que se realiza con el propósito de evitar actividades de inteligencia de aquellos actores que representen riesgos o amenazas para la seguridad del Estado Nacional (PC-00-02).

3.038. Contrasabotaje. Operación de inteligencia militar defensiva que comprende el empleo de medios y procedimientos destinados a contrarrestar la ejecución de operaciones de inteligencia militar de sabotaje de aquellos actores que representen riesgos o amenazas para la seguridad del Estado Nacional (PC-00-02).

3.039. Evaluación del riesgo. Se entiende a la evaluación de las amenazas y vulnerabilidades relativas a la información, y a las instalaciones de procesamiento de estas, la probabilidad de que ocurran y su potencial impacto en la operatoria de la Fuerza.

3.040. Incidente de seguridad. Un incidente de seguridad es un evento adverso en un sistema de seguridad que compromete la confidencialidad, integridad o disponibilidad, la legalidad y confidencialidad de la información. Puede ser causado mediante la explotación de alguna vulnerabilidad o un intento o amenaza de romper los mecanismos de seguridad existentes.

3.041. Información. Conocimiento parcial y localizado sobre personas, hechos, circunstancias o cosas que no han sido sometidas a un proceso de integración e interpretación (ver ROD-11-01 Art 1001). La información constituye, en esencia, un mensaje (bajo cualquiera de sus formas: gestual, oral o escrita) que modifica el conocimiento de una persona o sistema que la recibe.

3.042. Instalación militar. Es el conjunto físico integrado por bienes inmuebles asignados en uso, y administración a las Fuerzas Armadas, que se encuentran bajo la órbita de la jurisdicción militar incluye tierras, sistemas y complejos edificios, equipos, instalaciones subsidiarias y demás dependencias, como cuarteles, puestos, puntos de control e instalaciones necesarias para su funcionamiento, utiliza en acantonamiento o campaña, de forma permanente o transitoria, que permite el normal desarrollo de operaciones y actividades militares, tales como educación, instrucción, entrenamiento, apoyo, logística o de preparación para la Defensa Nacional (Resolución 1233/2009, Ministerio de Defensa).

3.043. Inteligencia. Conocimiento resultante del proceso al que se somete la información durante la ejecución del ciclo de producción de inteligencia, indispensable para una adecuada conducción cualquiera fuere el nivel que correspondiere. Se materializa en la actividad de obtención, reunión, sistematización y análisis de la información (PC-00-02).

3.044. Jurisdicción. Constituye un espacio o territorio correctamente determinado, en donde la autoridad posee competencia para administrar válidamente justicia en función de la debida distribución de atribuciones (PC-00-02).

3.045. Jurisdicción militar. Debe entenderse como “el ámbito territorial donde la autoridad militar ejerce competencias propias derivadas de las Leyes 23.554 y 24.948” (Resolución 1020/2009. Ministerio de Defensa).

Constituye el ámbito territorial militar, de acuerdo con las disposiciones legales vigentes en la materia, en donde la obligación primaria de la autoridad militar es la preservación de la Fuerza y el restablecimiento del orden dentro de dicho ámbito o jurisdicción.

3.046. Medidas. Conjunto de tareas, actividades, procedimientos y manejo de medios aplicados al logro de un objetivo (PC-00-02).

3.047. Medios. Elementos con la aptitud adecuada para el logro de un determinado fin. Pueden ser clasificados en medios humanos (personal), físicos (material) y orgánicos (servicios) (PC-00-02).

3.048. Operaciones de inteligencia militar. Operaciones desarrolladas, generalmente, por personal de inteligencia mediante el empleo específico de medios y procedimientos propios, a efectos de obtener información de importancia y/o afectar recursos vitales del oponente, para apoyar el planeamiento y ejecución de operaciones de la Fuerza, así como contrarrestar o neutralizar las actividades de Inteligencia del oponente sobre objetivos propios. Se clasifican en tres tipos (PC-00-02):

- a. Ofensivas: destinada a obtener información del oponente u enemigo real/potencial a efectos de afectar sus recursos vitales.
- b. Defensivas: destinadas a proteger información y material clasificado, recursos vitales propios y objetivos materiales críticos para el instrumento militar de las actividades de espionaje, sabotaje y/o accionar psicológico del oponente o enemigo real/potencial.
- c. Pasivas: se materializan en la adopción de las medidas de seguridad y protección de los recursos humanos y materiales, de carácter permanente y orientadas a la prevención de cualquier acción sobre la base de su finalidad específica.

3.049. Riesgo. Constituye la contingencia de vulnerabilidad o peligro en situaciones de incertidumbre, no implicando necesariamente un daño, ni otorgando certezas sobre el mismo, ni relaciones directas y determinantes, sino la sola probabilidad de ocurrencia del mismo (PC-00-02).

3.050. Zona de responsabilidad. Es el área en el cual un comandante / jefe tiene la responsabilidad en la conducción de las operaciones militares. Un acabado conocimiento de sus características contribuirá a efectuar un uso apropiado de la misma.

SECCIÓN IV

CLASIFICACIÓN DE LA INFORMACIÓN

3.051. Información clasificada. Cualquier información, con independencia de donde estuviere contenida y el formato que la caracterice, que requiere protección contra la divulgación no autorizada y a la que se ha asignado, con las formalidades y requisitos previstos en la legislación, una clasificación de seguridad.

3.052. Clasificación de seguridad (Decreto 950/02). Categoría o grado de reserva que se asigna a la información contenida en un documento, equipo o material. La clasificación de seguridad define el grado de peligro para la Seguridad Nacional que ocasionaría su incorrecta divulgación o conocimiento por parte de personas no autorizadas.

Esta clasificación distingue los siguientes grados: "ESTRICTAMENTE SECRETO Y CONFIDENCIAL", "SECRETO", "CONFIDENCIAL", "RESERVADO", y "PÚBLICO".

- a. ESTRICTAMENTE SECRETO Y CONFIDENCIAL: aplicable a toda información, documento o material que esté exclusivamente relacionado con la organización y actividades específicas de los organismos del Sistema de Inteligencia Nacional.
- b. SECRETO: aplicable a toda información, documento o material cuyo conocimiento por personal no autorizado pueda afectar los intereses fundamentales u objetivos vitales de la Nación.
- c. CONFIDENCIAL: aplicable a toda información, documento o material cuyo conocimiento por personas no autorizadas pueda afectar parcialmente los intereses fundamentales de la Nación o vulnerar principios, planes y métodos funcionales de los poderes del Estado.
- d. RESERVADO: aplicable a toda información, documento o material que no estando comprendidos en las categorías anteriores, no convenga a los intereses del Estado que su conocimiento trascienda fuera de determinados ámbitos institucionales y sea accesible a personas no autorizadas.
- e. PÚBLICO: aplicable a toda documentación cuya divulgación no sea perjudicial para los organismos del sistema de inteligencia nacional y que por su índole permita prescindir de restricciones relativas a la limitación de su conocimiento, **sin que ello implique que pueda trascender del ámbito oficial**, a menos que la autoridad responsable así lo disponga.

Cuando se considere innecesario establecer condiciones limitantes para la difusión de la información contenida en documentos, equipos o material, no se asignará clasificación de seguridad.

3.053. "Público – Militar"

- a. La clasificación de seguridad "PÚBLICO" debe ser entendida como una clasificación de seguridad y que como tal impone restricciones a la difusión abierta e indiscriminada de la información; en tal sentido deberá comprenderse que lo que fuere así clasificado solo podrá difundirse en el ámbito de la jurisdicción militar.
- b. Para reforzar el concepto precedente podrá adosarse al término "PÚBLICO" la expresión "MILITAR" separada por un guión, a fin de evitar que una mala interpretación del alcance de esta clasificación de seguridad exponga, ante terceros, el contenido solo previsto para la difusión dentro del ámbito militar (PÚBLICO – MILITAR).

SECCIÓN V

BARRERAS

3.054. Barrera. Definición del concepto desde el punto de vista de las MSCI. Serie coordinada de obstáculos físicos y/o lógicos (software) destinados a detectar, brindar alarma, retardar, canalizar, detener y/o negar las actividades del enemigo u oponente real o potencial, a fin de proteger la información, los medios humanos y materiales, y los sistemas de comunicaciones de interés.

El concepto de barrera alude a la aplicación de diversos obstáculos, destinados a interponerse entre lo protegido y el potencial elemento/sujeto de acceso no autorizado, que, en el marco de las MSCI, recibirán, cada uno de ellos, el nombre de componente de barrera.

SECCIÓN VI

APLICACIÓN DE LAS MEDIDAS DE SEGURIDAD DE CONTRAINTELIGENCIA

3.055. Aplicación de las MSCI durante períodos de paz y durante las operaciones

a. Aplicación de las MSCI durante períodos de paz

- 1) Durante períodos de paz. Conforme al grado de amenaza que el nivel superior proporcione al instrumento militar, se aplicarán las MSCI expresadas precedentemente y las que particularmente se requieran, sin que ello implique condición determinante para su implementación, ya que siempre se adoptarán MSCI básicas sobre la premisa del constante accionar de sistemas de Inteligencia extranjeros contra el IM.

Estas medidas se complementarán con la “Disciplina del Secreto” (discreción) y la “Necesidad de Saber” (delimitación del acceso a la información según las funciones asignadas).

- a) “Disciplina del secreto”: hábito basado en la instrucción y el adiestramiento para dar cumplimiento a las normas de contrainteligencia, a los efectos de salvaguardar la información clasificada.
- b) “Necesidad de saber”: deberá proporcionarse información exclusivamente a la persona u organización que tiene la obligación de conocerla. A tal efecto, deberá considerarse que el acceso a una información clasificada no constituye un derecho; el grado o jerarquía, por sí mismo, no autorizará a tener acceso indiscriminado a la información clasificada. La necesidad del conocimiento de una información estará en relación directa con el uso que se hará de la misma, el cargo o la función que desempeñe.

b. Aplicación de las medidas de seguridad durante las operaciones

- 1) Durante el desarrollo de operaciones tácticas

Las Medidas de seguridad de contrainteligencia de aplicación durante los períodos de paz podrán ser afectadas por:

- Las reglas de empeñamiento (RE), las cuales serán determinadas por el Poder Ejecutivo Nacional;
- Las disposiciones específicas que disponga el PEN dentro y fuera del TO;
- Las disposiciones judiciales que establezca el órgano jurídico competente; y
- Las limitaciones que impongan los tratados y compromisos internacionales firmados por el país que comprendan o no a los actores involucrados en el conflicto.

- 2) Medidas de seguridad complementarias

Entre las medidas o acciones que se pueden desarrollar para complementar las medidas de seguridad durante las operaciones tácticas, sin ser específicamente de Contrainteligencia, se mencionan:

- a) Protección de la población. Consistirá en llevar a cabo medidas de seguridad que permitan proteger a la población civil de las operaciones militares propias o del oponente. Para lograr este cometido se deberán instrumentar acciones que posibiliten identificar a la población civil, diferenciándola del instrumento militar propio o enemigo, y restringir sus desplazamientos, evitando que se vean en riesgo o bajo amenaza en aquellas zonas donde se desarrollan o se prevé el desarrollo de operaciones militares. La implementación de esta medida recaerá en los organismos estatales competentes, pudiendo quedar bajo responsabilidad del Comandante del TO en caso de que la situación así lo imponga. Dentro del TO se deberá emplear, en la medida de lo posible, las fuerzas de seguridad o policiales agregadas, asignadas o puestas en apoyo del instrumento militar.
- b) Tratamiento de los prisioneros de guerra. Esta actividad se deberá llevar a cabo conforme al Derecho Internacional para los Conflictos Armados (DICA) y siguiendo todo otro protocolo y convenio internacional firmado por la Nación.

- c) Restricción y/o control de la información. Durante el desarrollo de operaciones militares habrá información acerca de las operaciones y recursos militares, de infraestructura de interés nacional y la propia población que deberá ser protegida de las acciones del oponente real. En este sentido, será necesario instrumentar una serie de acciones y protocolos que permita restringir el conocimiento de determinados temas que, diseminados en forma indebida y/o inoportuna, pongan en riesgo a la población y al instrumento militar designado para responder a aquellos actores que amenazan a los intereses nacionales establecidos en la Constitución Nacional. Esta actividad deberá responder a normativas debidamente aprobadas por los poderes estatales competentes en la materia y considerando cuidadosamente el período por el cual se extenderá. Asimismo, quienes deban instrumentar estos protocolos y procedimientos deberán contar con los recursos materiales necesarios y los medios humanos debidamente adiestrados.
- d) Control de zonas militares. Será una parte del territorio nacional, enclavada en la zona del interior que, en razón de su carácter e importancia desde el punto de vista de la Defensa Nacional, deberá estar sometida a la jurisdicción de la autoridad militar (ROB-00-01 – “Conducción para el Instrumento Militar Terrestre”). Son aquellos espacios que serán protegidos de manera particular por el interés que representan para la Defensa y para la Nación, fuera de los TTOO. Será común asignar esta categoría a determinadas áreas, a los efectos de proporcionar la necesaria seguridad a la información o material clasificado, y al personal muy importante o con funciones críticas, que en ellas se hallen. La constitución de toda zona militar deberá ser declarada por el Poder Ejecutivo Nacional y se deberá consignar taxativamente las atribuciones conferidas a la autoridad militar que allí se desenvuelva.
- e) Evacuación de zonas. Será aquel procedimiento que buscará proteger a la población de los efectos de las operaciones militares que se desarrollen. Esta medida será una responsabilidad de las autoridades estatales o podrá ser delegada al comandante del TO. Esta medida podrá adoptarse con el objeto de posibilitar las acciones militares necesarias, en el marco de los objetivos de nivel estratégicos que se hallan establecidos.
- f) Cooperación cívico-militar. Son aquellos recursos y acuerdos en que se apoya la mutua cooperación entre el comandante de un TO, las autoridades estatales, organizaciones no gubernamentales (nacionales e internacionales) y la población, con el objeto de contribuir a proteger, preservar y sostener la vida de la población, el esfuerzo bélico y los otros recursos de la Nación que pudieran resultar vitales. Esta cooperación deberá establecerse a partir de normativas jurídicas y la responsabilidad recaerá en las más altas autoridades del Estado y, por delegación, en los organismos e instituciones involucrados.

CAPÍTULO IV

MEDIDAS DE SEGURIDAD DE CONTRAINTELIGENCIA REFERIDAS A LA SEGURIDAD FÍSICA DE LAS INSTALACIONES

SECCIÓN I

CONCEPTOS GENERALES

4.001. Definición. Conjunto de disposiciones que se adoptan para disuadir, detectar, identificar, neutralizar, negar y prever posibles respuestas a los efectos del acceso no deseado a la información clasificada y a los medios propios que se encuentren en instalaciones o áreas bajo control, protegiéndolos de todo daño que pudieren causar las actividades de Inteligencia de aquellos actores que representen amenazas o riesgos para la seguridad del instrumento militar y, eventualmente, otros factores del ambiente operacional, que en forma natural o por acción deliberada del factor humano produzcan similares efectos.

4.002. Conceptos generales. El acceso a la información conforma un vínculo entre el sujeto que accede y dicha información, que se expresa en términos de conocimiento o disponibilidad de ella.

Cuando se trata de información clasificada, el acceso se restringe solo a quienes estén autorizados, bajo la premisa de "Necesidad de Saber".

Los sistemas de Inteligencia del enemigo u oponente real o potencial procurarán establecer un vínculo como el señalado por fuera de la premisa establecida por el IM cuando se interese por determinada información bajo responsabilidad militar (Secreto Militar) o cuando procure dañar medios del propio instrumento militar. Las formas para el establecimiento de ese vínculo no deseado variarán desde intrusiones subrepticias de procesos prolongados en el tiempo hasta acciones instantáneas, evidentes, de gran impacto.

Para impedir la concreción del vínculo no deseado entre la información protegida y alguien sin "Necesidad de Saber", se recurrirá a interponer obstáculos entre la información u objeto sensible y el posible sujeto que procura el acceso (local o remoto) no autorizado.

La actual proliferación de medios técnicos e informatizados con aplicación directa en el campo de la protección de instalaciones constituye un conjunto de elementos a disposición que, aplicados convenientemente, inciden en gran medida a mejorar de la eficacia de un sistema de seguridad, pero ello no debe llevar a subestimar la importancia del factor humano, el más complejo de los intervinientes.

Un caso particular de la seguridad física lo constituyen los desplazamientos, ya sean estos ejecutados con medios orgánicos o no, por cuanto su naturaleza combina situaciones de movimiento y estáticas, caracterizadas por su rápida mutación. Ante estas circunstancias se emplearán criterios similares a los aplicados con la seguridad física de las instalaciones (barreras), para la protección de la información y materiales clasificados en tránsito.

4.003. Instalaciones militares. Es el conjunto físico integrado por bienes inmuebles asignados en uso, y administración a las Fuerzas Armadas, que se encuentran bajo la órbita de la jurisdicción militar y que incluyen tierras, sistemas y complejos edilicios, equipos, instalaciones subsidiarias y demás dependencias, como cuarteles, puestos, puntos de control e instalaciones necesarias para su funcionamiento, utilizadas en acantonamiento o campaña, de forma permanente o transitoria, que permiten el normal desarrollo de operaciones y actividades militares, tales como educación, instrucción, entrenamiento, apoyo, logística o de preparación para la Defensa Nacional (Resolución 1233 / 2009, Ministerio de Defensa).

4.004. Personal. A los fines de la aplicación de la seguridad física contemplada por las medidas de seguridad de contrainteligencia, el término aludirá a los integrantes del instrumento militar y a quienes que, no formando parte de él, circunstancialmente se encuentran bajo su responsabilidad y como tales puedan ser objeto de daño físico por parte de las acciones del enemigo u oponente, real o potencial.

Existe un conjunto de personas que por el conocimiento que poseen, de interés para la Defensa y/o por la función que realizan, debe ser especialmente protegido de la acción de la Inteligencia extranjera. A los efectos de la aplicación de procedimientos particulares para su seguridad, se las denominará "Persona Muy Importante" (PMI).

4.005. Particularidades de la seguridad física de las instalaciones. La seguridad física de las instalaciones de la Fuerza posee singulares características que deben considerarse al efectuarse el planeamiento e implementación de medidas.

La correcta aplicación concluirá en el desarrollo de un proceso lógico en el fin buscado. Se deben considerar las siguientes características:

a. Control de acceso.

El control de acceso es un conjunto de previsiones por adoptar, con la finalidad de impedir el acceso de personal no autorizado al interior de la instalación militar, y, dentro de estas, en restringir el ingreso espacios donde exista la posibilidad de tomar contacto con información o material clasificado.

Todo el personal dentro de estos espacios debe ser identificado inequívocamente para dejar en evidencia la presencia de cualquier persona extraña. Por extensión, se identificarán vehículos u otros objetos que revisten interés desde el punto de vista de la seguridad.

En muchos casos, no es necesario el acceso físico de personal externo para la obtención de información en instalaciones propias, ya que pueden operarse mecanismos desde posiciones remotas. Dispositivos para este cometido pueden ser ingresados voluntaria o involuntariamente por personal de la organización o frecuentadores habituales.

Asimismo, debe preverse que un eventual acto de sabotaje dentro de las propias instalaciones puede realizarse sin necesidad de que persona alguna ingrese en la instalación, enviando por mensajeros comerciales el artificio que lo materializa por, proyectándolo desde el área perimetral externa o introduciéndolo en algún medio que acceda a la instalación o permanezca próximo a ella.

El control de accesos se orienta, además, a la posibilidad de penetración de redes informáticas, concentrando la máxima atención de los responsables de implementar las medidas de seguridad de contrainteligencia, por la permeabilidad de estas y la constante evolución de las formas que la facilitan. Se deben considerar con atención especial los sistemas informáticos (redes) que controlen infraestructuras críticas de la instalación (edificios inteligentes).

El registro de acceso en sus diversas modalidades, como el video digital registrable, puede auxiliar a la acción preventiva de las MSCI, al establecer patrones de comportamiento sobre los cuales se pueden apreciar necesidades de perfeccionar el sistema, o permitir detectar conductas diferenciadas que deban ser advertidas como alarmas del dispositivo de seguridad.

La complementación del control de acceso con revisiones asistemáticas de ingresos y egresos facilitará la detección preventiva de posibles fallas y contribuirá a determinar la confiabilidad del control de acceso.

b. Control de áreas interiores

Las áreas interiores son los sectores en que puede dividirse el espacio de jurisdicción militar para su control, conforme a la naturaleza de la información por proteger, las características de las instalaciones existentes, los flujos de personal y las condiciones de seguridad imperantes en términos de amenazas.

El control de estas áreas también deberá operar como un criterio restrictivo para el propio personal, conforme a la premisa de "Necesidad de Saber". Para ello se establecerán niveles de accesibilidad claramente identificados, bajo la denominación de "Áreas de Seguridad".

Estas áreas interiores, identificadas de acuerdo con la seguridad que se brindará, respetarán el nivel de accesibilidad identificada como: "Controlada", "Restringida" y "Excluida". Generalmente, las medidas que permiten materializar un efectivo control de áreas serán:

- 1) Verificación de tiempo de permanencia. Permite constatar el tiempo real que emplea un visitante comparándolo con el tiempo previamente medido para efectuar un determinado recorrido.
- 2) Implementación de sistemas de guardias internas, con auxilios de medios electrónicos.

- 3) Patrullaje interno periódico en el área. Especialmente en instalaciones complejas o de alta compartimentación (oficinas, depósitos, áreas de producción, etc.).

Cada instalación es un caso particular, por lo tanto, el sistema que se empleará en el control de áreas interiores responderá a los parámetros de seguridad necesarios, conforme a lo que se busca preservar y las características de la instalación, incluyendo la interacción con flujos externos de personas y efectos.

La implementación de un sistema de control debe considerar que las pautas rutinarias ayudan a generar ventanas de oportunidad para quienes quieran violarlo, en consecuencia, deben adoptarse medidas que neutralicen esquemas previsibles.

4.006. Identificación de las áreas de seguridad. Toda área, sin excepción, deberá ser individualizada claramente en forma visual, sin dejar dudas respecto de dónde se encuentra el individuo y las medidas de seguridad que por tal corresponden a su especial carácter (Anexo 2).

La colocación de esta señalización debe tener en cuenta el tipo de personal que circulará por cada área, especialmente en un Área Controlada, dado que es posible que por ella transite personal que no integre la organización militar, lo que implica su desconocimiento de la normativa castrense. Es por ello que deben instalarse carteles adicionales explicativos acerca de lo que está autorizado o no a hacer una persona en dicho espacio.

En las áreas excluidas y restringidas circulará solo personal de la organización con un mayor conocimiento y formación, lo que hace innecesario carteles de prevención adicional; sin embargo, esta podrá existir cuando sea necesario establecer medidas adicionales de seguridad como la imposibilidad de acceder con determinados elementos técnicos, como ordenadores portátiles, teléfonos celulares, dispositivos de almacenamiento de información en formato digital, cámaras fotográficas o de video (tener en cuentas las capacidades tecnológicas incluidas en los actuales dispositivos tecnológicos).

4.007. Área de seguridad. Es aquella área o superficie donde esté ubicada una instalación considerada de interés operativo, sea permanente o transitoria. La permanencia y circulación de personas en ella, está sujeta a controles y especiales restricciones de seguridad. Según su naturaleza y grado de importancia, en cuanto al material y/o documentación que contienen, pueden ser: controladas, restringidas y excluidas.

4.008. Área controlada. Es aquella área de seguridad que circunda áreas restringidas o áreas excluidas. También recibe esta denominación aquella área que, sin contener a las anteriores, se establece a manera de cerco con la finalidad de controlar el acceso y la limitación de la circulación. Se establece para evitar el contacto de personas ajenas a la organización con elementos que existan en ella y merezcan resguardo sin estar comprendidos en las otras categorías.

4.009. Área restringida. Área de seguridad en la cual el acceso se encuentra debidamente normado y limitado a individuos ajenos a la organización y a cierto personal perteneciente a la misma y que comprende el espacio geográfico donde se encuentran instalaciones, personal de importancia, documentación y/o materiales de alta clasificación de seguridad.

Se deberá considerar como área Restringida a:

- a. Oficina del Cte, Dir o jefe del elemento u organismo.
- b. Oficina del 2do Cte, Subdir o 2do jefe.
- c. Salas de armas.
- d. Instalaciones destinadas al almacenamiento de agua potable.
- e. Instalaciones o locales destinadas a la administración de servicios (tableros de luz, cabinas de gas, grupos electrógenos, etc.).
- f. Oficina de control y cargo.
- g. Oficinas del SAF.

4.010. Área excluida. Es el área donde existe o se trate, en forma permanente, información de alta clasificación de seguridad. Solo tendrá acceso el personal que pertenezca a ella y bajo estrictos controles de seguridad, ejecutados al ingresar, en el interior y al egresar de la misma. Serán aquellos lugares donde, por el solo hecho de permanecer en ella, se tenga acceso a información clasificada.

Se deberá considerar como área excluida a:

a. Oficinas del área de personal.

Aquellos lugares donde se traten legajos de personal, cuadros de efectivos, sumarios y actuaciones de justicia, solicitudes de incorporación con información clasificada, etc.

b. Oficinas del área inteligencia.

Aquellos lugares donde exista información relacionada con el orden de batalla enemigo, carta de incidentes de inteligencia y contrainteligencia, mapas temáticos especiales con clasificación de seguridad, planes de obtención, planes de contrainteligencia, etc.

c. Oficinas del área de material.

Aquellos lugares donde se guarde o registre efectivos de material de valor (Grupo comodidad armamento, electrónica, comunicaciones, munición y explosivos, material con clasificación de seguridad, etc.).

d. Oficinas del área de informática / centros de cómputos.

Aquellos lugares desde donde se administre programas sensibles al elemento, guarde archivos de back up, se encuentren los sistemas de administración de redes, claves, sistemas de acceso, sistemas de alimentación de resguardo para los sistemas informáticos, etc.

e. Oficina del oficial de finanzas.

Siempre que en estos lugares se trate información clasificada de compras de material sensible o crítico.

f. Oficinas del área operaciones.

Aquellos lugares donde se maneje información relacionada con los planes de operaciones, organización, doctrina con media o alta clasificación de seguridad, etc.

g. Cifrario.

h. Oficinas de investigación y desarrollo.

Aquellos lugares donde se trate información o material de sistemas en desarrollo (material, sistemas operativos, criptología, etc.).

i. Local de instalación de la plataforma de integración (o centro de monitoreo).

Aquellos lugares donde se efectúe la integración, administración y control de los sistemas de vigilancia de las instalaciones.

j. Centro de comunicaciones fijo.

k. Centros de mensajes.

l. Centro de operaciones tácticas (COT).

m. Sala de situación (cuando visiblemente se exponga o trate información clasificada).

Solo cuando en estas instalaciones se encuentre desplegada o se trate información clasificada de las operaciones en desarrollo

- n. Depósitos, oficinas o talleres donde se encuentren desarrollando actividades con material clasificado.
- o. Farmacias y droguerías.
- p. Oficina del área de sanidad

Solo en aquellos lugares donde se guarde información relacionada con los legajos médicos, legajos psiquiátricos, imágenes de diagnósticos médicos, copias de resguardo en los centros de diagnóstico, información en las PC y terminales de los facultativos, etc.

- q. Polvorines.
- r. Área jurídica.

Aquellos lugares donde se guarde o actúe con temas relacionados con cuestiones jurídicas de la Fuerza.

4.011. El entorno y las áreas de seguridad. Una particularidad de la seguridad será la consideración del entorno ambiental inmediato. Orientado a minimizar los riesgos de daños y/o amenazas a la información u objetos protegidos, como consecuencia de efectos no deseados provenientes de las características del entorno de los espacios de jurisdicción militar originados en sus características particulares, fenómenos naturales asociados (incendios naturales, inundaciones, meteoros, deslaves, etc.) o de origen humano (derrames tóxicos, derrumbes, colapso o accidentes en infraestructuras críticas, etc.).

Esta consideración deviene en la necesidad de adoptar medidas de protección o reducción de los efectos negativos antes mencionados para evitar que estos sean utilizados por la Inteligencia del oponente para alcanzar su cometido. Asimismo, debe tenerse en cuenta la posibilidad de que ellos sean potenciados por actores/agentes, en caso de ocurrir fortuitamente, o directamente provocados.

SECCIÓN I

BARRERAS

4.012. Barrera. La Real Academia de la Lengua Española define el concepto de barrera con las siguientes acepciones:

- a. Obstáculo, embarazo entre una cosa y la otra.
- b. Valla, compuerta, madero, cadena u otro obstáculo semejante con que se cierra un paso o se cerca un lugar.

4.013. Barreras-MSCI. Definición del concepto desde el punto de vista de las MSCI. Serie coordinada de obstáculos físicos y/o lógicos (software) destinados a detectar, brindar alarma, identificar, retardar, canalizar, detener y/o negar las actividades del enemigo u oponente real o potencial, a fin de proteger la información, los medios humanos y materiales, y los sistemas de comunicaciones de interés.

El concepto de barrera alude a la aplicación de diversos obstáculos destinados a interponerse entre lo protegido y el potencial elemento/sujeto de acceso no autorizado, que, en el marco de las MSCI, recibirán, cada uno de ellos, el nombre de componente de barrera.

4.014. Finalidad. Las barreras, como parte de las medidas de seguridad de contrainteligencia, tienen por finalidad:

- a. Permitir el acceso solo a quienes estén autorizados.
- b. Establecer una mecánica definida para su normal transposición, lo que origina un procedimiento controlable y registrable.
- c. Imponer una conducta definida ante la barrera, que contribuya a identificar prematuramente la pretensión de traspasarla por quien no está habilitado para ello.

- d. Imponer acciones disuasivas y dificultades (acciones preventivas y correctivas) que desalienten el contacto no autorizado con la información u objeto protegido.
- e. Proporcionar advertencia (la alerta) y tiempo para facilitar la detección del curso de una penetración no autorizada.
- f. Permitir su integración para potenciar sus efectos.
- g. Disuadir al personal no autorizado de llevar cabo cualquier acción, ya sea por el esfuerzo adicional que implica su transposición o por el mayor tiempo necesario para realizar ello, lo que puede generar oportunidad de ser detectado y/o capturado.

4.015. Clasificación de las barreras

a. Barreras naturales.

Son obstáculos topográficos naturales funcionales a la finalidad de negar o entorpecer el acceso a una instalación (ríos, precipicios, montañas, desiertos, edificaciones u otros objetos, etc.).

b. Barreras artificiales.

- 1) Son dispositivos e ingenios de distinta naturaleza constructiva y/o técnica utilizados, en forma permanente o transitoria, con la finalidad de disuadir, detectar, neutralizar, negar y eventualmente, de ser posible, identificar cualquier tipo de intento de agresión, directa o indirecta, que se realice contra información y medios del propio Instrumento Militar.
- 2) Son construidas por el hombre para servir a las necesidades de seguridad de la información y constituidas por dispositivos o artefactos de distinta naturaleza, utilizados con el propósito de disuadir, impedir, retardar, detectar o neutralizar una penetración contra la información, los materiales o las actividades por proteger.
- 3) A pesar del perfeccionamiento de las tecnologías utilizadas en la conformación de las barreras y su integración, debe tenerse presente que no existe sistema alguno que finalmente, por sí, impida el acceso a la información u objeto preservado; solo reducirán las posibilidades de aproximarse a ellos, impondrán mayores costos, requerirán mayores tiempos y/o capacitación de los ejecutores y eventualmente exigirán el desarrollo de tecnologías especiales para tal fin.
- 4) De acuerdo a la función y las características, las barreras artificiales se clasificarán en:
 - a) Cercas.
 - b) Edificios.
 - c) Barricadas.
 - d) Sistemas de control de acceso.
 - e) Sistemas electrónicos.

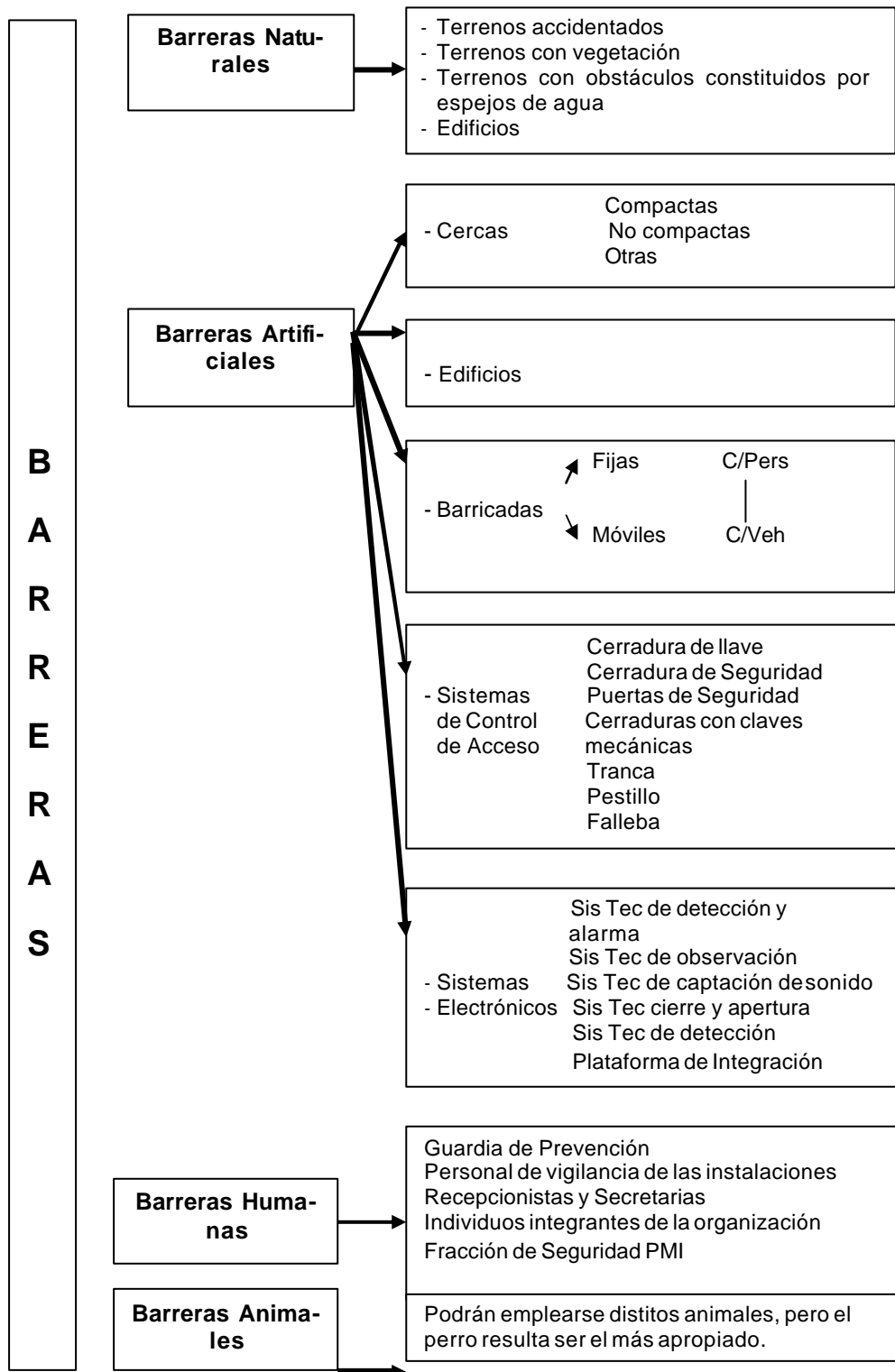
c. Barreras humanas.

Son medios humanos convenientemente organizados, equipados y adiestrados cuya misión será la de disuadir, detectar, identificar, neutralizar y/o impedir, a través de técnicas y procedimientos de contrainteligencia, la ejecución de actividades de inteligencia del enemigo u oponente real o potencial que puedan representar una real o potencial agresión sobre la información o medios por proteger.

d. Barreras animales.

Se entenderá como tales al empleo de animales con la finalidad de disuadir, detectar, alertar o neutralizar cualquier tipo de agresión directa o indirecta que se intente o ejecute contra un elemento de la Fuerza que constituya un objetivo por proteger.

Cuadro resumen de la clasificación de las barreras.



SECCIÓN III

BARRERAS NATURALES

4.016. Definición. Las barreras naturales son el conjunto de obstáculos naturales constituidos por los accidentes o características del terreno que rodean o se encuentran próximos al perímetro exterior de la instalación y contribuyen a proteger el objetivo.

4.017. Conceptos básicos. Estas características topográficas podrán ser positivas o negativas, puesto que, si en algunos casos representan obstáculos difíciles de franquear y sirven de barreras de seguridad, en otros dificultarán la observación y no permitirán alertar a tiempo la presencia de intrusos. Su análisis se adaptará para el caso particular de las medidas de contrainteligencia.

Los obstáculos naturales no representan por si solos barreras de seguridad ideales, sin que se les agreguen otras características. Si bien retardan al intruso o tienden a proteger la instalación o medios impidiendo su observación, también protegerán y ocultarán a/los intruso/s. Por lo tanto, las barreras naturales deberán evaluarse, en primera instancia, según la solidaridad hacia el individuo u organización con fines de daño, robo y/o agresión.

Posteriormente, se debe considerar la misma en función del retardo que ocasione.

4.018. Terrenos accidentados. Los terrenos accidentados, especialmente los acantilados, desfiladeros, barrancos, etc., serán difíciles de franquear y tenderán a retardar a aquellos que pretendieran penetrar o acceder por lugares no autorizados.

No obstante, se deberá considerar que los terrenos accidentados ofrecerán mayores posibilidades al agresor para ocultarse y desplazarse, y dificultará las posibilidades de vigilancia y detección. Por el contrario, los terrenos llanos y libres de vegetación u otros obstáculos facilitarán las acciones de vigilancia y control.

4.019. Terrenos con vegetación. La vegetación, considerada desde el punto de vista de la seguridad, ofrecerá las siguientes características, que deben ser consideradas en el planeamiento de un sistema de seguridad:

- a. Proporcionará cubiertas y encubrimiento.
- b. Dificultará los movimientos e impondrá limitaciones en el empleo de determinado material (determinado tipo de vehículos, sensores o armamento).
- c. Las características de la vegetación y las condiciones climáticas podrán constituir una amenaza o riesgo ante determinada situación (sequías que puedan provocar incendios que pongan en riesgo las instalaciones).

4.020. Terrenos con obstáculos constituidos por espejos de agua. Las barreras naturales constituidas por espejos de agua (ríos, lagos, mar, pantanos, otros), sin considerar su tamaño o forma, presentan ciertas características que es necesario contemplar al momento de llevar a cabo el planeamiento de un sistema de seguridad.

Al considerarse estas características naturales del terreno como barreras, deberán ser analizadas individual y colectivamente para determinar las posibilidades de seguridad que proporcionan, así como las facilidades que ofrece al oponente para su acceso.

Estas características propias por considerar serán:

- a. La observación será amplia y a grandes distancias, permitiendo la vigilancia y control sobre la superficie. Este control se ejercerá sobre embarcaciones o personas, que se desplacen en la superficie. La capacidad subacuática deberá apreciarse como una potencial amenaza y preverse obstáculos y sensores, si la situación lo justificar, desde el interior del espejo de agua hacia la costa.
- b. Una limitación importante la constituye la necesidad de contar con medios apropiados para responder a una agresión desde un espejo de agua y su efectivo control.
- c. Dificultad para el adecuado mantenimiento de los obstáculos y sensores subacuáticos y personal especializado para llevar a cabo esta actividad.

SECCIÓN IV

BARRERAS HUMANAS

4.021. Definición. Son medios humanos convenientemente organizados, entrenados y equipados para detectar y/o neutralizar a personas o actividades que puedan representar una real o potencial agresión sobre la información u objetos protegidos.

4.022. Características de las barreras humanas. Normalmente, actuarán en conjunto con otras, integrando un sistema de barreras, aunque en algunos casos lo harán aisladamente. Resulta ser uno de los sistemas más seguros en lo que respecta a la detección y neutralización de accesos no autorizados, ya que sólo mediante la neutralización física del personal que integra la barrera puede accederse a la instalación o afectar a la persona que se protege.

Toda barrera humana que se instale, deberá ser concebida sobre la base de un estudio que contemple las necesidades reales, en relación con la situación existente. El mismo criterio regirá el dimensionamiento de la custodia de una personalidad (seguridad PMI).

Al establecer o evaluar una barrera humana, deberán considerarse las características de las personas que la integren. Entre ellas podrán mencionarse: la situación personal, el estado físico, su predisposición espiritual y el medio en que actuará.

Dentro de las barreras humanas, podrán mencionarse a las guardias de prevención, personal de vigilancia de instalaciones, personal de vigilancia en funciones de escolta PMI, imaginarias, cuarteles, recepcionistas, entre otras.

4.023. Guardia de prevención. Los conceptos relacionados con su misión, organización y dispositivo respetarán las normas y parámetros particulares que cada elemento incluye en sus directivas u órdenes propias.

Desde el punto de vista de las medidas de seguridad de contrainteligencia, interesa especialmente:

- a. Cumplir estrictamente con su misión, como premisa fundamental de la seguridad.
- b. Hacer cumplir y observar el sistema de identificación y control establecido para el personal perteneciente a la instalación y/o ajeno a ella.
- c. Resguardar y vigilar áreas críticas y sensibles a los actos de espionaje, sabotaje u otro tipo de actividades de inteligencia de un oponente real/potencial y/o delictivas.
- d. Asegurar el cumplimiento de las Órdenes, Directivas y Procedimientos Operativos Normales referidos a seguridad del elemento.
- e. Escoltar/acompañar, dentro de lo posible, a las personas ajenas a la instalación, con la finalidad de evitar que se desvíen de los itinerarios autorizados.
- f. Controlar durante el acceso, estacionamiento y circulación de los vehículos (fundamentado en un plano de circulación y aéreas habilitadas), ajenos o pertenecientes a la instalación, una eventual introducción de personas, equipos, explosivos u otros elementos destinados a la ejecución de actividades de inteligencia del enemigo.
- g. En casos de incendio, accidentes, desórdenes, actos de agresión y/o inteligencia extranjera, además de lo inherente a las actividades normales de una guardia, desde el punto de vista de contrainteligencia se deberá:
 - 1) Aislar/limitar las áreas afectadas.
 - 2) Evitar alteraciones en el lugar de los hechos.
 - 3) Preservar las pruebas.
 - 4) Confeccionar listados de informantes, sospechosos o testigos de los hechos producidos, y proceder a ponerlos a disposición de la autoridad competente.

- 5) Procurar obtener todo tipo de información relacionada con los hechos acaecidos, a fin de proporcionar elementos de juicio a quienes deban efectuar dichos procedimientos.

4.024. Personal de vigilancia en las instalaciones. Será todo aquel personal que, sin pertenecer a una guardia de prevención, cumple funciones que incluyen directa o indirectamente la observancia de medidas de seguridad de contrainteligencia. Dentro de este núcleo se incluyen guardias civiles, serenos, encargados de control y vigilancia, y otros.

En general, este tipo de vigilancia complementa en forma sincrónica las tareas desarrolladas por el personal asignado a una guardia de prevención sin embargo, conviene destacar:

- a. Normalmente, el personal integrante no tendrá estado militar y podrá o no disponer de armamento.
- b. El armamento que podrá utilizar estará constituido por armas cortas.
- c. Su instrucción diferirá de la de las guardias de prevención, en cuanto a su aptitud combativa y conciencia de contrainteligencia, lo cual implicará el desarrollo de un adecuado plan de educación específico y modular (adecuado al personal militar o civil).

4.025. Recepcionistas y secretarios. Tendrán por finalidad la verificación de los documentos de identidad de aquellas personas que procuraren acceder a una instalación o dependencia de esta y/o entrevistar a la persona o personas, a cuyo servicio se encuentre afectado.

Las funciones de la receptoría podrán abarcar el contralor total de acceso a una instalación, conformando así el elemento de control e información de esta. Esta mantendrá una estrecha relación con la guardia de prevención, con la finalidad de facilitar su intervención, en caso necesario.

La misión general del elemento de control e informe será la de canalizar, controlar, orientar y permitir el acceso y salida del personal, que específicamente se determine. Procederá de la misma manera con la información relacionada a la instalación o a su personal todo ello, de acuerdo con normas, que se impartan al efecto.

4.026. Individuos integrantes de la organización. Será todo aquel personal que, sin pertenecer a alguna de las organizaciones abocadas directamente a la seguridad cumple funciones que incluyen directa o indirectamente la observancia de Medidas de Seguridad de Contrainteligencia.

4.027. Fracción de seguridad de personal muy importante. Será aquel personal instruido, equipado y adiestrado para brindar seguridad física a aquellas personas que hayan sido catalogadas como personas muy importantes.

SECCIÓN V

BARRERAS ANIMALES

4.028. Definición. Es el empleo de distintos animales con la finalidad de detectar o neutralizar cualquier tipo de agresión directa o indirecta que se intente o ejecute contra un elemento de la jurisdicción militar.

En el uso de estos animales pueden distinguirse aquellos afectados a la protección de un área, que circulan libremente dentro de esta, y los que actúan conducidos por un guía.

4.029. Características. Si bien podrán emplearse distintos tipos de animales, el perro es el que resulta más apropiado para los fines buscados. Constituirá un elemento valioso para la detección y captura de quienes pretendan vulnerar el objetivo.

Además, podrán ser adiestrados para descubrir la eventual introducción clandestina de explosivos, drogas u otros efectos. A esto contribuirá su desarrollado sentido del olfato, del oído, su fidelidad y el hecho de que pueden actuar aún en condiciones climáticas desfavorables y de noche. No obstante lo expresado, deberá tenerse en cuenta que el enemigo podrá desarrollar ciertos arbitrios para disminuir las facultades antes mencionadas.

Dentro de las formas de empleo posible, cuando actúen libremente podrán posibilitar la detección y, eventualmente, la captura de quienes pretendan vulnerar el objetivo. La identificación podrá lograrse solamente cuando su empleo se haga por medio de un guía.

El entrenamiento de animales, con la finalidad de desempeñarse como una barrera de seguridad, deberá considerarse con espacios temporales amplios, que incluirán etapas de adaptación, adiestramiento y confianza, educación, prácticas y ejecución de tareas (bajo supervisión).

Estas barreras serán útiles en sectores y aéreas de gran amplitud, con vegetación variada, limitadas barreras estructurales perimétricas y con reducido personal asignado a tareas de seguridad y control.

SECCIÓN VI

BARRERAS ARTIFICIALES

4.030. Definición. Son dispositivos e ingenios de distinta naturaleza constructiva y/o técnica, utilizados en forma permanente o transitoria, con la finalidad de disuadir, detectar, neutralizar, negar y eventualmente, de ser posible, identificar cualquier tipo de intento de agresión, directa o indirecta, que se realice contra información y medios del propio Instrumento Militar.

4.031. Tipos de barreras artificiales

a. **Cercas.** Es una estructura construida para regular el acceso físico o visual. En general, pueden considerarse tres tipos: compactas de visión restringida, no compactas de visión completa y otras cercas.

1) Cercas compactas de visión restringida. Son aquellas construidas con materiales sólidos, tales como ladrillos, piedras, cemento, maderas, metales y otros. Presentan las siguientes características:

a) Se utilizarán para limitar la observación de las actividades que se realizan en el interior de la instalación.

b) Encauzarán el ingreso o egreso de efectos o personas por accesos predeterminados.

c) Demandarán la construcción adicional de observatorios elevados, para poder tener acceso por las vistas, hacia el exterior, y de otras obras específicas para el empleo de armas, con el fin de repeler distintos tipos de agresiones.

d) Demandarán un alto costo y prolongado tiempo de construcción.

e) Deberán reunir los siguientes requisitos:

(1) Ser continuas y ofrecer igual seguridad en todo su trayecto, incluyendo accesos.

(2) Condicionar su altura al fin perseguido, ya fuere demorar o dificultar.

(3) Contribuir a una mejor acción del personal de seguridad afectado a esta.

(4) Obstaculizar, por medio de su parte enterrada bajo el nivel del suelo, la construcción de túneles o pasajes subrepticios. Esto incluye la protección de desagües y otros servicios, que deberán atravesar la estructura.

(5) Estar despejada de malezas o de cualquier otro obstáculo en un área próxima.

(6) Ser completadas con la construcción de obstáculos adicionales, tales como líneas de alambres de púas en voladizo, vidrios molidos, púas, etc.

(7) Contar con una iluminación detalladamente realizada, a fin de evitar los conos de sombra.

2) Cercas no compactas de visión completa. Son aquellas construidas mediante estructuras, que posibiliten la visión a través de ellas, y diseñadas para demorar el acceso físico a la instalación. Tendrán las siguientes características principales:

a) Deberán poseer un trazado que servirá, básicamente, para delimitar el área de la instalación.

- b) Permitirán dominar por las vistas, desde el interior hacia el exterior.
- c) Harán factible un uso más eficaz de la iluminación perimétrica.
- d) Deberán satisfacer los siguientes requisitos:
 - (1) Condicionar su altura al fin perseguido, ya fuere demorar o dificultar. Se estima, en general, que la altura no debería ser inferior a los 2,50 metros. Si en proximidades de la cerca, existieren estructuras materiales o vegetación que facilitaren salvarla, la altura mencionada deberá aumentarse o, en su defecto, se eliminarán aquellas.
 - (2) Disponer, en su parte superior, de voladizos de alambre de púas, a 45 grados, hacia el exterior. Eventualmente, los voladizos podrán colocarse hacia ambos lados.
 - (3) Tener la menor cantidad posible de accesos y estos deberán poder cerrarse de forma tal que se garantizare la continuidad de la cerca.
 - (4) Obstaculizar el paso a través de ella.
 - (5) Cuando la cerca circundare una vasta extensión, será conveniente la construcción de caminos paralelos, para facilitar el desplazamiento de patrullas.
 - (6) La zona despejada deberá extenderse, en la medida de lo posible, a una distancia de 20 metros fuera de la cerca y de 30 metros, hacia el interior de la instalación.
 - (7) Las cercas deberán emplazarse en concordancia entre sí, con el terreno natural y cualquier obstrucción creada por el hombre.
 - (8) Dichas cercas deberían brindar un grado equivalente de protección continua a lo largo de todo el perímetro.
- 3) Otros tipos de cercas. Son aquellas que podrán construirse con materiales distintos a los señalados en los apartados anteriores. Las que resultan de uso más común de las construidas con vidrios y plásticos de distinto espesor, transparentes o no. Se destacarán las siguientes características:
 - a) Posibilitarán o no una visión completa.
 - b) Constituirán un obstáculo rígido, de mayor o menor consistencia.
 - c) Su trazado, en general, no será de gran extensión.
 - d) En la estructura de su construcción intervendrán materiales sólidos de uso para construir las cercas compactas de visión restringida.
 - e) Formarán parte de las cercas señaladas anteriormente, ya fuere para proteger sistemas de alarma, proteger personal, etc.
- b. **Edificios.** Los elementos constituyentes de un edificio, aunque no hubieren sido construidos para servir de barreras, retardarán el acceso a una instalación; por ello se los considerará como barrera estructural.

Determinados edificios se construirán especialmente para proteger información, medios y/o materiales específicos, por lo que deben ser considerados con medidas particulares al respecto.

El retardo diseñado se verá disminuido por la existencia de puertas, ventanas u otras estructuras (conductos de ventilación, servicios e instalaciones especiales), siendo objeto de aplicación en el planeamiento inicial.

Las superficies interiores de un edificio podrán presentar muchas particularidades. La existencia de espacios libres (sótanos, túneles, etc.), serán evaluados como lugares de ocultamiento de personas, equipos, sistemas electrónicos, etc., puesto que no solamente se protegerá contra la entrada de personas, sino también contra la colocación de elementos técnicos destinados a la obtención de información y/o a eventuales sabotajes.

Para calcular el valor de un edificio como barrera estructural será necesario conocer los detalles de construcción. Esto podrá efectuarse inspeccionando el edificio y estudiando los planos. La verificación de los planos podrá revelar un lugar de acceso, disimulado por una construcción posterior.

Los edificios se construyen con un número determinado de aberturas, con la finalidad de posibilitar el ingreso y egreso, ventilación, iluminación, control de temperatura, etc. Estas aberturas serán cavidades practicadas en las barreras que representan las superficies de los edificios o estructuras y, por lo tanto, constituirán un riesgo latente para la seguridad de la información u objeto clasificado que se pretende proteger.

Es importante considerar que no siempre será indispensable que el intruso se encuentre en persona en el recinto, sino también que podrá lograr su propósito teniendo acceso visual auditivo al interior del edificio o estructura que le interese. Esto motivará que las aberturas sean motivo de particular atención en la planificación y adopción de las medidas de seguridad de contrainteligencia.

- c. **Barricadas.** Constituye un obstáculo o parapeto con la finalidad interrumpir, desviar o dificultar el avance. Podrán ser fijas o móviles, contra personal o vehículos.

Clasificación de los distintos tipos de barricadas:

1) Barricadas móviles contra personal.

Serán aquellos dispositivos físicos **móviles** contruidos con la finalidad de detener, desviar o dificultar el avance de personal a pie.

Se podrán construir de distintos materiales y su principal característica es que resultan relativamente fáciles de desplazar o reubicar.

Serán utilizados tanto en instalaciones permanentes (puestos de control, asientos de paz, etc.) como en instalaciones móviles (puestos de control, instalaciones de campaña, vivac, etc.).

2) Barricadas fijas contra personal.

Serán aquellos dispositivos físicos **permanentes o semipermanentes** contruidos con la finalidad de detener, desviar o dificultar el avance de personal a pie.

Serán utilizados en instalaciones permanentes (puestos de control, asientos de paz, instalaciones fuera de las Unidades militares señaladas como objetivos por proteger, etc.).

3) Barricadas móviles contra vehículos.

Serán aquellos dispositivos físicos **móviles** contruidos con la finalidad de detener, desviar o dificultar el avance de vehículos que intenten atravesar un perímetro.

Se podrán construir de distintos materiales y serán utilizados tanto en instalaciones permanentes (puestos de control, asientos de paz, etc.) como en instalaciones móviles (puestos de control, instalaciones de campaña, vivac, etc.).

4) Barricadas fijas contra vehículos.

Serán aquellos dispositivos físicos **permanentes o semipermanentes** contruidos con la finalidad de detener, desviar o dificultar el avance de vehículos que intenten atravesar un perímetro.

Se podrán construir de distintos materiales y su carácter permanente o semipermanente dificultará o impedirá su desplazamiento o reubicación.

Serán normalmente utilizados en instalaciones permanentes (puestos de control, asientos de paz, instalaciones de campaña, instalaciones fuera de las unidades militares señaladas como objetivos por proteger, etc.).

Las barricadas contra vehículos tendrán un diseño que deberá incluir aspectos relacionados con:

- (a) Distancia de seguridad suficiente entre la barricada planificada y las estructuras por proteger.
- (b) Amenaza explosiva.
- (c) Peso de los vehículos determinados como amenaza.
- (d) Velocidad esperada del vehículo de la amenaza.
- (e) Cantidad de puntos de acceso que requieren barricadas para vehículos.
- (f) Disponibilidad de recursos humanos y materiales para complementar la barricada.

- d. **Sistema de control de accesos.** Los sistemas de control de acceso son dispositivos físicos mecánicos y/o electrónicos, componentes de una abertura, ideados para asegurar dos o más objetos en una misma posición de modo que solo puedan ser operados directa o indirectamente por las personas idóneas y autorizadas para hacerlo.

Son dispositivos para asegurar aberturas de todo tipo, fijar un objeto móvil a otro fijo o inmovilizar la parte móvil o libre de un mecanismo. El término abarcará todos los dispositivos que permitirán satisfacer esos requisitos, ya fueren simples o complejos.

Entre los sistemas de acceso con dispositivos físicos mecánicos para asegurar aberturas, podrán mencionarse los siguientes:

- 1) Cerradura de llave. Es un mecanismo metálico que se acciona mediante una llave particular y única. Podrán distinguirse, entre otras:
 - a) Cerradura de combinación: Es aquella cuya apertura viene determinada por la combinación de una serie de tumbadores alfanuméricos. Ejemplo: cerradura de caja fuerte, valija, portafolios, candados especiales.
 - b) Cerraduras de rodete, de disco, de espiga y de palanca. Es aquella que posee un rodete o plancha posicionadora que impide pasar la llave para girar el pestillo.
- 2) Puertas de seguridad. Se construyen específicamente y, en general, brindan protección contra el fuego de armas portátiles y contra la irrupción por palanca y otras formas convencionales, a partir de un sistema de seguridad, con cerrojo deslizante en dos o más direcciones opuestas.
- 3) Tranca es un dispositivo que se fija en forma transversal a la superficie móvil que desea mantenerse cerrada. Se construye con distintos materiales, tales como madera, hierro, aluminio; son de diversas medidas y formatos, y se utilizan tanto en portones como en puertas, ventanas, muebles de madera o de hierro u otros materiales; se aseguran mediante grampas convenientemente dispuestas y fijadas en paredes o marcos.
- 4) Pestillo. Consiste en un pasador deslizante, de distinta forma y tamaño, que se fija a una puerta o ventana y que proporciona el cierre necesario, cuando se introduce uno o ambos de sus extremos en grampas u orificios practicados en el marco/pared de una abertura.
- 5) Falleba. Es un dispositivo que funciona como cerradura interna para asegurar puertas y ventanas, conformada por una varilla de hierro acodada en sus extremos, que gira mediante una acción de leva en direcciones contrapuestas que proporciona una traba adecuada a los fines de cierre.

e. **Sistemas electrónicos.**

1) **Sistemas técnicos de detección y alarma.**

Son dispositivos electrónicos, electroópticos, eléctricos, mecánicos o una combinación de ellos, que se instalarán para proporcionar vigilancia y proveer alarma y seguridad en áreas o en determinadas instalaciones. Dentro de los sistemas mencionados, se destacan los siguientes:

- a) Sistemas electrónicos de alarmas, constituidos en términos generales por:

- (1) Fuente de alimentación (principal).

- (2) Fuente de alimentación autónoma.
- (3) Central de alarma con temporizadores y sectorización de áreas de protección, unidades de activado/desactivado por claves, disparo de alarma acústica, lumínica, silenciosa, llamado telefónico a lugares predeterminados, disparo de elementos pirotécnicos y/o activación de agresivos químicos, etc.
- (4) Sensores de distinto tipo, para detectar la aproximación de personas o intento de penetración.
- (5) Líneas físicas de alimentación a la central y/o red de sensores, con sistemas de alternativas.
- (6) Sensores. Son aquellos dispositivos activos o pasivos que se activan ante las modificaciones de una situación, previamente reconocida por el sistema, como normal. La modificación de dicha situación se manifestará a través de una señal, que se traduce en una o varias acciones concurrentes. Dentro de los distintos tipos de sensores, pueden señalarse los siguientes:
 - (a) De contacto, por apertura de circuito. Consiste en un dispositivo que se acciona por separación de dos contactos. En general, se aplican sobre aberturas.
 - (b) Por vibración. Consiste en un interruptor móvil o pendular que, por efecto de un impulso, cambia de posición y, al chocar con otro contacto, cierra un circuito, que pone en funcionamiento el sistema. En otros, el movimiento produce la apertura del circuito se logra el mismo resultado anterior; en general, se complementa con los sensores de contacto.
 - (c) Por cédula fotoeléctrica. La alarma, en este caso, se activa por el corte del haz luminoso que proyecta la célula sobre un receptor sensible, activando un circuito que la pone en funcionamiento.
 - (d) Por detección acústica. Son aquellos dispositivos de captación microfónica que se activan en presencia del sonido que produce una persona, al aproximarse o penetrar a un lugar determinado, y que activa el circuito de alarma.
 - (e) Sísmicos. Son aquellos sensores que actúan por variaciones programables de vibraciones sostenidas, que pueden indicar la ejecución de determinadas actividades.
 - (f) Sensores infrarrojos. El sensor se activa por diferencia de temperatura, a la que está regulado. Estos sensores pueden activarse, por el corte del haz infrarrojo que proyecta lineal o reticularmente, y que activa la alarma correspondiente.
 - (g) Por variación de los campos electromagnéticos o de aire. Estos sistemas actúan por variación del campo magnético y/o desplazamiento de la masa de aire que se produce al ubicarse una persona, entre las terminales de un sistema regulado para actuar sin tales variantes.
 - (h) Detectores de movimientos por emisión de ondas. Son aquellos dispositivos que emiten ondas sonoras o eléctricas que, al chocar contra un objetivo, se reflejan sobre un dispositivo receptor, acusando la presencia de una persona en forma visual o por intermedio de la activación de una alarma.
 - (i) Sensores de interrupción de circuitos. Se aplican sobre las redes físicas de alimentación de sensores, circuitos cerrados de televisión y cualquier otro subsistema para proporcionar alarma, ante la interrupción física, en cualquier sector de la red.
 - (j) Alarmas portátiles contra agresiones personales. Son dispositivos de alarma de tamaño reducido, capaces de ser transportados en forma disimulada, alimentados por fuentes de energía de volumen reducido y accionables por distintos arbitrios, al alcance de quien los utilizare.

- 2) **Sistemas técnicos de observación.** Son aquellos que posibilitan el control visual de áreas en forma directa, mediante el empleo de elementos de teleobservación, tales como cámaras fijas visibles y/o encubiertas, cámaras móviles de cambio vertical, horizontal y rotativo, cámaras con gran angular y/o lente infrarrojo para observaciones en la oscuridad o con poca luz, cámaras giratorias accionadas por líneas telefónicas, cámaras flotantes.
- 3) **Sistemas técnicos de captación de sonidos.** Son aquellos que, mediante la captación electrónica de sonidos, posibilitan su ubicación, sea mediante el control humano o por activación de una alarma. Pueden mencionarse los siguientes: micrófonos ultrasónicos, micrófonos direccionales, alambre microfónico con alarma programada, micrófonos flotantes, receptores de micrófonos.
- 4) **Sistemas técnicos de cierre y apertura.** Son aquellos dispositivos que actúan mediante la aplicación de facilidades informáticas y electrónicas para permitir o negar la apertura de una abertura o asegurar esta.

Generalmente, se combinarán con componentes estructurales.

- a) Dispositivos electromagnéticos. Combinan facilidades informáticas y electrónicas, a los sistemas de cierre, con eventual capacidad para producir alarma y/o registrar intentos de vulneración.
- b) Cerradura con claves. Son aquellas cuyo cierre se basa en claves algorítmicas o numéricas. Pueden estar o no combinadas con otros sistemas de cierre. Su utilización es múltiple, desde un simple candado hasta cajas de seguridad, puertas o cofres de amurar.
- 5) **Sistemas de detección.** Son aquellos dispositivos que actúan mediante la aplicación de rayos X, captación de los gases de los materiales explosivos y/o por la captación de un campo electrónico, con la finalidad de localizar la existencia de objetos materiales, en poder de personas no autorizadas para su portación o de agresores potenciales, o en áreas a las cuales se hubiere prohibido el ingreso de armas o explosivos, o que configuren un peligro para la integridad física de personas o instalaciones.
- 6) **Plataforma de integración (centro de monitoreo).** Cuando las características particulares lo requieran, los sistemas de seguridad instalados reportarán a una plataforma de integración (centro de monitoreo) donde, con economía de personal, podrán mantenerse las áreas críticas, medios o instalaciones bajo control, combinando la observación por medios técnicos con el control de acceso informatizado, alarmas, altavoces de información, medios de comunicación, protección y detección contra incendios.

Dicho centro coordinará las actividades de seguridad externa e interna del elemento, y se reservare, la decisión de requerir apoyo o afectar propios medios para intervenir.

SECCIÓN VII

RECURSOS ACCESORIOS COMPLEMENTARIOS

4.032. Definición. Son aquellos sistemas organizacionales y recursos humanos y/o materiales que contribuyen a complementar las medidas de seguridad de contrainteligencia.

4.033. Consideraciones básicas. Las medidas de seguridad de contrainteligencia son un conjunto complejo de recursos que no dependen exclusivamente, para su ejecución, del instrumento militar. En ese complejo conjunto existen organizaciones y recursos que, sin ser integrantes y dependientes del instrumento militar, complementan a este en su objetivo. Las fuerzas de seguridad y fuerzas policiales cooperarán en funciones y actividades de identificación, vigilancia, respuesta y mitigación. El sistema judicial participará, mediante la aplicación de las leyes, en la mitigación del hecho, etc.

En otro orden de cosas, también complementan las medidas de seguridad de contrainteligencia aquellos sistemas que, sin ser considerados en las clasificaciones anteriores, son complementarios a las medidas de seguridad de contrainteligencia descriptos. Se deberá considerar entre estos a los sistemas de iluminación.

4.034. Sistema de iluminación. Es el conjunto de arbitrios técnicos que, por medio del aprovechamiento de energía eléctrica, mecánica o electrónica, permitirá aumentar la visibilidad en aquellos sectores oscuros, que no poseen luz natural, o en aquellos donde no resultare suficiente la claridad.

Las fuentes de iluminación pueden ser de variados tipos; para su distribución se requiere una red física y artefactos que potencien la capacidad de la fuente (lámpara) o de características especiales. Para la instalación deberá tenerse en cuenta la cantidad de luz que se requiere para cada circunstancia. Esto se establecerá calculando la iluminancia necesaria en un área determinada. Se calcula considerando la cantidad de luz (equivalente a LUMEN) y la distancia, mediante el método de “Fuente Puntual”.

Dichos requerimientos conforman los datos técnicos de rendimiento de los equipos por instalar. Los estudios de seguridad deberán determinar cuánta luz será necesaria para cada caso.

4.035. Método de cálculo de “fuente puntual”. Se determina el área de una esfera con un radio igual a la distancia especificada desde la fuente lumínica. se utiliza la distancia en metros y se multiplica al cuadrado la distancia. Posteriormente, se multiplica por “PI” y después por cuatro. Esta es el área de una esfera a la distancia especificada.

Se divide la intensidad de luz (que posee la fuente) entre el área esférica. El resultado es la iluminancia en LUX. Si la luz llega a la superficie en un ángulo menor de 90°, aplica un factor de corrección, multiplicando el valor calculado de la iluminancia por el coseno del ángulo fuera del eje.

4.036. Conceptos influyentes en la iluminación. La cantidad de luz necesaria de un área o lugar determinado se adecuará teniendo en cuenta algunas pautas o normas de carácter general:

- a. Área de penumbra. Se define a partir de una cantidad superior a CINCO (5) Lux y, permitirá la detección de movimientos individuales y desplazamientos de grupos. La posición del observador deberá ser adecuada, respecto del área de penumbra, por cuanto se dificultará la apreciación de los contrastes.
- b. Área perimétrica. Se determina a una cantidad superior a 15/20 Lux; brindará una adecuada iluminación que permitirá, incluso, la identificación. Si los artefactos de iluminación estuvieren correctamente instalados, por su ubicación, altura y direccionamiento, podrán producir el deslumbramiento necesario, para negar la observación, hacia el interior del objetivo.
- c. Iluminación de calzadas. Se establece un rango lumínico no inferior a CUARENTA (40) lux, por utilizarse en calles internas que requieran un tránsito seguro, con o sin auxilio de la luz vehicular.
- d. Iluminación de playones, áreas de seguridad o lugares de trabajo. Requieren CIEN (100) o más Lux, dependiendo de las tareas y nivel de detalle que demande.

4.037. Características de la iluminación. Sobre las características de la iluminación será necesario tener en cuenta algunos factores propios que en definitiva, brindará un aporte directo al planeamiento de referencia.

- a. Potencia nominal. Condiciona la magnitud del flujo emitido por la lámpara y las proporciones de la instalación, desde el punto de vista eléctrico.
- b. Rendimiento cromático. Determina la mayor o menor capacidad para la apreciación de colores.
- c. Temperatura de color. Condiciona la tonalidad de la luz, proporcionan tonos cálidos o fríos, según predominen las radiaciones, en el campo del rojo o del azul.
- d. Tamaño, fijación, accesorios, instalaciones auxiliares, consumos de energía, facilidades o dificultades para el mantenimiento.
- e. Direccionamiento, dispersión del haz de luz, distribución de esta, prestaciones de las unidades ópticas, reflexión de los espejos, altura de montaje.
- f. Capacidad y estado de la red de alimentación, conmutación a sistemas auxiliares, sectorización de la instalación, tipo de encendido.
- g. Condiciones climáticas predominantes, tonalidades y características del terreno, actividades del elemento por proteger.

4.038. Clasificación general de los equipos de iluminación por considerar. Los equipos de iluminación poseen una amplia clasificación que varía en función de sus características, uso particular y finalidad.

De acuerdo con nuestro planeamiento, los clasificaremos en:

- a. Reflectores. Son aquellos que, por medio de superficies especulares, distribuyen la luz emitida por la fuente luminosa. En relación con el grado de deslumbramiento que se pretendiere potenciar o disminuir, serán apantallados (cutt-off), semiapantallados (semicutt-off) y no apantallados (non cutt-off). En esta categoría entran los denominados proyectores, aparatos con los que es posible concentrar la luz, en direcciones bien definidas.
- b. Refractores. Constituidos por cubetas, globos o pantallas de vidrio u otros materiales transparentes y estriados, que dirigen los rayos de luz en direcciones predeterminadas.
- c. Difusores. Constituidos por materiales que disminuyen la luminancia de lámpara, para atenuar el deslumbramiento o bien, por razones estéticas específicas.

4.039. Instalación de los sistemas de iluminación. La instalación de los sistemas de iluminación, abarca principios referidos a la función específica de seguridad que deben cumplir y al grado de protección a otorgar. Siempre que fuere posible, la red de iluminación de seguridad será independiente de la red general y permitirá la conmutación automática a otra fuente de producción de energía, en caso de interrupción de esta.

Todo conductor eléctrico deberá embutirse o estar fabricado con una cubierta especial, conforme a normas IRAM. El tendido de los conductores, en lo posible, será subterráneo. En caso de ser aéreo, se lo instalará lo más alto posible y se evitará hacerlo sobre cercas, vulnerables desde el exterior.

La sectorización de la instalación será esencial, así como colocar las cajas conmutadoras y de distribución en áreas controladas. Los transformadores deberán encontrarse protegidos de agresiones internas o externas mediante cubiertas, cercas aislantes e iluminación apropiada.

Si bien las cuestiones relacionadas con los aspectos técnicos de los sistemas de iluminación no son responsabilidad directa del campo de Inteligencia, es de su competencia asesorar en las acciones de prevención sobre cualquier tipo de deficiencia estructural o funcional que permitiera o facilitara la ejecución de acciones indebidas por parte de actores (enemigo u oponente) que puedan afectar la seguridad de la Fuerza.

4.040. Empleo de los sistemas de iluminación. Según su empleo, los sistemas de iluminación requieren considerar aspectos particulares en el planeamiento de seguridad. Es recomendable tender a la implementación de medios lumínicos con movimientos mecánicos, incrementan el nivel de seguridad y considerar siempre la utilización de dos circuitos eléctricos independientes.

En el diseño de su empleo se tendrá especialmente en cuenta:

- a. Iluminación perimétrica: En aquellas circunstancias en que el trazado de la cerca perimétrica coincida con arterias o calles de circulación urbana, se tendrá especialmente en cuenta no afectar la seguridad de los vehículos que por ellas se desplacen. Deberán diseñarse sistemas de iluminación específicos, en los que el direccionamiento del haz de luz o la colocación de arbitrios antideslumbramiento no afecten la seguridad de los conductores.
- b. Iluminación de accesos a la instalación: Las puertas y/o ventanas tendrán prioridad en el planeamiento de la iluminación. Su ubicación, cantidad y uso se coordinará con los controles e inspecciones de personal/vehículos de ese Elemento, siendo condición excluyente facilitar aspectos básicos de seguridad en esos lugares.
- c. Iluminación de áreas de seguridad. El lugar asignado para inspeccionar vehículos y/o identificar personas deberá contar con una intensidad lumínica que permita la revisión integral del vehículo, equipos u objetos, complementando dicha capacidad con extensiones móviles. La iluminación de las áreas de revisión se activará para ese fin específico y el lugar elegido deberá facilitar la tarea y obtener ventajas, desde el punto de vista de seguridad.

- d. Iluminación de áreas críticas. Los lugares que contengan medios o recursos de energía eléctrica, calefacción, agua potable, sistemas de comunicaciones, materiales explosivos e incendiarios, maquinarias delicadas, áreas de almacenamiento o de producción de material de alta clasificación de seguridad u otros de importancia similar, serán considerados áreas críticas y, en consecuencia, la implementación del sistema de iluminación deberá contener multiplicidad y coordinación de medios lumínicos de manera de minimizar riesgos de vulneración y facilitar alertas tempranas.
- e. Iluminación de puertos, muelles o dársenas y grandes áreas o playas. Las grandes áreas, en general, se iluminan desde torres que soportan múltiples artefactos de iluminación y permiten el control de un área para maniobra, carga y descarga. Estas torres podrán ser fijas o con equipos móviles autoportantes, con torre columna desplegable y alimentación por generador.
- f. Playas de estacionamiento. Las playas de estacionamiento, además de proporcionar lugares de ocultamiento que ponen en peligro la seguridad, son ideales para que el enemigo ejecute atentados contra el personal propio. Una buena iluminación ayudará a reducir estas posibilidades.

Las playas de estacionamiento podrán iluminarse de un lado, instalando luces en los edificios cuando fuere posible. Las playas de estacionamiento grandes, que se iluminaren desde postes colocados en su perímetro, presentarán la ventaja de brindar iluminación a los sectores adyacentes a su límite.

- g. Iluminación interna de las instalaciones. El interior de una instalación deberá estar en condiciones de ser convenientemente iluminado, teniendo en cuenta que el grado de protección deberá ser compatible con las necesidades de observación del personal de la instalación y con los medios de vigilancia instalados.

CAPÍTULO V

MEDIDAS DE SEGURIDAD DE CONTRAINTELIGENCIA REFERIDAS A LA SEGURIDAD DEL PERSONAL

SECCIÓN I

CONCEPTOS GENERALES

5.001. Definición. Son el conjunto de disposiciones y acciones destinadas a proteger a las personas integrantes del instrumento militar (IM) o aquellas que se encuentren vinculadas al interés de la Defensa, para impedir o neutralizar las actividades de aquellos actores que representen amenazas o riesgos a la seguridad nacional, y eventualmente otros factores del ambiente geográfico, con la finalidad de resguardar la integridad física de ellas y/o la información sobre la que poseen conocimiento.

5.002. Conceptos generales. El personal que integra el instrumento militar o aquel que resulte de interés para la Defensa y que se encuentre bajo la responsabilidad de este tendrá un valor a partir de:

- la información sobre la que posee conocimiento;
- determinado personal, material o información a la que tiene acceso;
- sus capacidades, destrezas o habilidades físicas o intelectuales;
- la función crítica que desarrolla.

La actual proliferación de medios y procedimientos con aplicación directa en el campo de la protección de personal constituye un conjunto de elementos a disposición que, aplicados convenientemente, inciden en gran medida en la mejora de la eficacia de un sistema de seguridad, cuyo fin es la protección del personal bajo responsabilidad.

Con el objeto de clasificar al personal a partir de la importancia o valor que reviste para el instrumento militar, se establecen las siguientes posibilidades:

- a. Personal Muy Importante;
- b. Personal del Instrumento Militar con funciones críticas.
- c. Personal del Instrumento Militar.

A partir de considerar a las personas como integrantes o no del instrumento militar, se pueden hacer las siguientes distinciones:

- a. Personal militar integrante del Instrumento Militar propio;
- b. Personal civil integrante del Instrumento Militar propio;
- c. Personal civil ajeno al IM (proveedores, prestadores de servicio y contratistas);
- d. Personal militar o civil extranjero;
- e. Funcionarios públicos;

Cuando se considere la seguridad del personal muy importante (PMI) o personal con funciones críticas, se presentan situaciones complejas relacionadas con los desplazamientos y con los lugares de alojamiento o viviendas, o con lugares que frecuenta fuera de las instalaciones militares.

En el caso de los desplazamientos fuera de las instalaciones militares, existen limitaciones jurídicas – legales y de competencia que afectarán el accionar y los procedimientos, y que, como consecuencia, dificulta la seguridad por brindar exponiendo al personal que brinda la seguridad y al objetivo.

En el caso de aquellas PMI y personal con funciones críticas que residan temporaria o permanentemente en locaciones (hoteles, hospedajes, hospitales o centros de atención fuera de la jurisdicción militar, etc.), presentarán también una importante dificultad para lograr una adecuada seguridad y, al igual que durante los desplazamiento impondrá limitaciones jurídico-legales y de competencia que afectarán el accionar y los procedimientos, y que, como consecuencia, dificulta la seguridad a brindar exponiendo al personal que brinda la seguridad y al objetivo.

Ambas situaciones impondrán una mayor exigencia de medios humanos, materiales y financieros.

5.003. Personal muy importante (PMI). A los fines de la aplicación de las medidas de seguridad referidas a la seguridad del personal, el término aludirá a los integrantes del instrumento militar y a aquellos que, no formando parte de él, constituyen objetos de seguridad en relación con el conocimiento que poseen o el valor circunstancial, de acuerdo con la función que desempeñan mientras se encuentran en la jurisdicción militar o bajo su responsabilidad, y como tal puedan ser objeto de afectación.

5.004. Personal del instrumento militar con funciones críticas (PFC). A los fines de la aplicación de las MSCl referidas a la seguridad del personal, el término aludirá a los integrantes del instrumento militar que constituyen objetos de seguridad en relación con el conocimiento que poseen y con la información o material a la que tienen acceso, de acuerdo con la función que desempeñan dentro de un organismo, y como tal, puedan ser objeto de afectación.

5.005. Personal del instrumento militar. Todo individuo integrante del instrumento militar, ya sea militar, civil o contratista, que posee determinado conocimiento o acceso a material que es de interés proteger. Por esta razón, este personal constituirá un objeto por proteger en el ámbito de las medidas de seguridad de contrainteligencia.

5.006. Aspectos generales que abarcan las medidas de seguridad de contrainteligencia referidas al personal. El principal riesgo para la seguridad de las personas está constituido por la acción que desarrolla el enemigo u oponente, real o potencial, sobre el propio personal o sus entornos, a través de sus sistemas de Inteligencia.

Las medidas de seguridad de contrainteligencia referidas al personal tienen como objetivo la protección física del individuo y de aquella información de la cual posee conocimiento y que resulta de interés para el instrumento militar.

Las medidas que se adoptarán para asegurar la protección física de una persona son un conjunto de acciones que persiguen preservar la integridad física del individuo o allegados sin considerar otros aspectos mientras que aquellas medidas que apuntan a la protección de la información son el conjunto de acciones que, actuando sobre el intelecto del objetivo, conllevan una modificación de la conducta tendiente a generar “conciencia de contrainteligencia”.

En este sentido, cabe otorgar máxima atención al personal que cumple funciones críticas, sin que por ello se descuide al resto de los integrantes de las organizaciones militares, por cuanto cualquier miembro puede ser objeto o eventualmente sujeto de la acción adversaria de los sistemas de inteligencia, en procura de los fines que mueven su accionar, tales como obtener información protegida o cometer acciones que persigan un daño sobre el instrumento militar.

Debe tenerse en cuenta que los sistemas de Inteligencia adversarios obrarán en muchos casos sobre la premisa de obtener acceso constante a la información protegida, manteniendo a su sistema de obtención a resguardo de la acción propia mediante una combinación de tecnología y medios humanos.

SECCIÓN II

SEGURIDAD EN RELACIÓN CON EL CONOCIMIENTO QUE POSEE

5.007. Seguridad de las personas relacionada con el conocimiento que posee. Partiendo de la base que para proteger la información de interés de la que posee conocimiento un individuo es necesario adoptar acciones que actúen directamente sobre el intelecto estos con el objeto de concientizar acerca de la importancia de aplicar el concepto de “conciencia de contrainteligencia” y produzcan un cambio en la conducta en relación con la información por proteger.

Los aspectos considerados anteriormente refuerzan la necesidad de contemplar la debilidad que el ser humano representa en todo sistema de protección de la información, por la multiplicidad de abordajes que permite (directos o a través de su entorno) y la posibilidad de mutación de su actitud frente a la responsabilidad de protección de la información, es necesario actuar mediante el voluntario convencimiento de los individuos, principalmente a través de la educación.

5.008. Características propias de los individuos. De acuerdo con las características propias de la personalidad humana, es necesario considerar los siguientes aspectos como base para estructurar las Medidas de Seguridad de Contrainteligencia aplicables a la seguridad del personal en general y en particular a los que cumplen alguna función crítica:

a. Confiabilidad del personal.

La confiabilidad presupone la cualidad de confiable del personal y ello sugiere una referencia individual acerca de que es posible confiar en una persona determinada. Nuestra lengua asigna al término confiar, por lo menos, tres acepciones que son aplicables a la conceptualización que se procura como parte de la estructuración de las medidas de seguridad de contrainteligencia:

- Encargar o poner al cuidado de alguien algún negocio u otra cosa.
- Depositar en alguien, sin más seguridad que la buena fe y la opinión que de él se tiene, la hacienda, el secreto o cualquier otra cosa.
- Esperar con firmeza y seguridad.

Las tres definiciones ayudan a entender que la confiabilidad del personal está aludiendo a las condiciones propias de cada persona, que lo sindicamos como el posible depositario de aquello que se procura proteger, en la convicción de que su conducta, respecto de tal cometido, se ordenará a las formas y fines previstos.

Desde la individualidad se está en presencia de una cualidad, por lo tanto, es algo que es posible advertir, apreciar y evaluar conforme a patrones definidos, mientras que desde la organización que la requiere se procura el efecto de la cualidad, produciendo una conducta previsible del individuo, previsible conforme a las necesidades de dicha organización.

Es indudable que se trata de la integración más compleja en el sistema de protección de la información, por la naturaleza propia de toda persona que, como única e irrepetible, encierra una ilimitada cantidad de opciones frente al problema de la protección de la información a lo largo del tiempo que mantenga contacto con ella, incluyendo dentro de tal, al que involucra el conocimiento adquirido que permanecerá con el sujeto más allá de su función en el marco del instrumento militar. En este sentido, es indudable que el ser humano representa el eslabón más débil de la cadena de protección de la información y, en consecuencia, requiere la mayor y más permanente atención.

La conducta del personal, como expresión individual de las cualidades aplicadas a la vida cotidiana, será objeto de constante observación para detectar oportunamente la conveniencia de integrar o mantener a una determinada persona vinculada con información o material por proteger.

Existen características y situaciones del personal que integra el instrumento militar que deberán ser identificadas y evaluadas para determinar si pueden representar debilidades del sistema propio de protección de la información que otorguen posibilidades de explotación a los sistemas de inteligencia del enemigo u oponente. Entre ellas pueden distinguirse primariamente:

- 1) Exceso de confianza en la discreción ajena, que se pone de manifiesto cuando se confía información clasificada a personas no autorizadas a conocerla, basada en la creencia que no la divulgará o utilizará en forma conveniente.
- 2) Vanidad o el deseo de parecer informado, más allá de las reales responsabilidades, es causa de frecuentes indiscreciones.
- 3) Desconocimiento del valor de la información, que puede derivar en suministrarla a personal no autorizado, en conversaciones aparentemente intrascendentes (incluidas redes sociales y otras formas tradicionales o modernas de comunicación).
- 4) Negligencia, descuido o falta de interés en el correcto cumplimiento de las normas de seguridad ordenadas.

- 5) Existencia de debilidades, vicios o flaquezas de carácter personal, que pueden ser aprovechados por parte de la Inteligencia enemiga para obtener información, en forma directa o a través de terceros.

La posible existencia de las situaciones mencionadas implica que todas las instancias jerárquicas deben mantener una preocupación constante para advertir indicios de aquellas en el personal, y en especial el que posee funciones críticas, para evaluar adecuadamente el riesgo que ello significa y las acciones necesarias para evitar efectos no deseados respecto de la información protegida.

b. Educación.

Desde el instrumento militar se pretende que quienes lo integran o se vinculan a él y desempeñan funciones adopten conductas que, en consonancia con la necesidad de preservar determinada información, se integren en los esquemas de protección de la información, generando previsibilidad en dicho esfuerzo, no sólo frente a los procesos o situaciones normales, sino ante eventos que pongan en riesgo la información que se pretende proteger, por lo que se hace necesario desarrollar un proceso educativo en cada organización del instrumento militar que refuerce el valor de la confianza, como vínculo esencial del personal con la responsabilidad encomendada mediante una función.

c. Instrucción.

La capacitación en técnicas y procedimientos que acoten y regulen la relación entre el individuo y la información sensible bajo su responsabilidad posibilita:

- 1) Reducir las situaciones en que la persona deba resolver con "criterio propio" sobre algún aspecto de la gestión de la información sensible, que resultan en situaciones que puedan ser aprovechadas por la inteligencia enemiga.
- 2) Facilitar la normalización de tareas para reducir el riesgo de error humano, contribuyendo a ayudar a detectar la existencia de indicios de no confiabilidad.
- 3) Materializar entornos de contención frente a situaciones de error, negligencia o acciones deliberadas que puedan exponer indebidamente la información protegida, reduciendo el nivel de riesgo.
- 4) Facilitar la supervisión y el control.
- 5) Las medidas de seguridad de contrainteligencia son eminentemente preventivas y la capacitación para su aplicación deberá materializarse a través de un programa adecuado a las condiciones y características de cada organización, orientado a informar de sus deberes y obligaciones en relación con la seguridad, así como a interiorizarlo acerca de la forma de actuar del enemigo u oponente.

d. Supervisión y control.

- 1) La naturaleza de la actividad de preservación de la seguridad del personal con funciones críticas por involucrar la observación sistemática de la conducta de esta, requiere del mayor esfuerzo de prudencia para evitar invadir la privacidad de quienes forman parte del IM y que por sus condiciones personales y profesionales han sido destacados para desarrollar funciones críticas.
- 2) El contacto permanente y directo, junto al consecuente conocimiento de la persona, por parte de las instancias de la cuales dependa, dentro de la organización militar en que preste funciones, será el primer receptor de los reflejos de posibles situaciones que puedan advertirse como de interés desde el punto de vista de la seguridad sobre funciones críticas.
- 3) La confianza que presupone la asignación de una función crítica no debe implicar en modo alguno que las acciones de supervisión y control son innecesarias, y mucho menos que su ejecución obedece a que dicha confianza inicial ha sido defraudada.
- 4) La redundancia de la supervisión y la reiterada intervención de las instancias de control serán norma para asegurar la normalidad en el desarrollo de funciones críticas.

- 5) Las medidas de seguridad de contrainteligencia son una responsabilidad de comando por ello constituye uno de los pilares de la acción de conducción de una organización militar el asegurar las condiciones para el correcto desarrollo de funciones críticas en forma permanente, y particularmente de aquellas que pueden influir en el personal encargado de cumplirlas, como potenciales objetos de la acción de la Inteligencia del enemigo u oponente.

e. Prevención.

La prevención respecto de la seguridad del personal con funciones críticas resultará del efecto sinérgico de los siguientes aspectos:

- 1) Selección del Personal.

Consiste en el análisis de las cualidades del candidato a desempeñar un rol crítico y la propuesta a la instancia correspondiente para su designación.

- 2) Educación.

Mantenimiento de valores soportes para evitar desvíos en la conducta del personal que signifiquen riesgo para la seguridad de la información protegida.

- 3) Instrucción.

Internalización de procedimientos con énfasis en el conocimiento de los deberes y responsabilidades de acuerdo con el cargo y la posición en la organización.

- 4) Disciplina.

Acatamiento estricto de todas las disposiciones de seguridad vigentes.

- 5) Vigilancia continua.

Observación sistemática y asistemática sobre los procedimientos aplicados por el personal con funciones críticas en relación con la información protegida.

5.009. Proceder con el personal que se separa o se retira del servicio. Todo el personal será instruido sobre las penas que pesan sobre aquellos que difunden información clasificada y que se encuentran contenidas en el Código de Disciplina, se deberá labrar un acta para constancia, que quedará archivada en el elemento.

SECCIÓN III

SEGURIDAD FÍSICA DE LAS PERSONAS

5.010. Seguridad física de las personas. Es el conjunto de medios y procedimientos que se adoptará para asegurar la protección de una persona bajo responsabilidad del instrumento militar, a fin de resguardar la integridad física del individuo considerado de interés.

La integridad física de una persona considerada de interés para el instrumento militar conlleva una serie importante de exigencias en cuanto a los recursos por afectar (humanos, materiales y financieros), así como las consideraciones jurídicas que enmarcan una situación de estas características.

Los aspectos que serán gravitantes al momento de planificar y ejecutar este tipo de actividades lo constituirán la oportunidad y el espacio físico donde se desarrolle.

a. Espacio físico:

- 1) Dentro de la jurisdicción militar, la actividad se verá favorecida por la posibilidad de emplear todos los recursos necesarios.
- 2) Fuera de la jurisdicción militar, la actividad se verá dificultada producto del entorno civil, el mayor número de variables fuera de nuestro control, las limitaciones legales para el empleo de armas, el respeto por las normas de tránsito, la ubicación de las locaciones donde el objetivo permanezca, la competencia de cada actor que participe en la seguridad (FFSS, FFPP, etc.), y las coordinaciones que se deban establecer con distintas agencias.

- b. Oportunidad: este aspecto esta relacionado con la situación que se vive, el estado moral, la situación social, etc.

Ambos aspectos se potencian cuando esta actividad deba desarrollarse en un marco de operaciones de paz o de protección civil.

Las consideraciones particulares para llevar a cabo esta actividad se encuentran detalladas en el MOP-11-01 – “Seguridad a personas muy importantes”, edición 2007.

CAPÍTULO VI

PROCEDIMIENTOS DE SEGURIDAD REFERIDOS A LA IDENTIFICACIÓN Y CONTROL DE PERSONAL Y MATERIALES

SECCIÓN I

IDENTIFICACIÓN Y CONTROL DE PERSONAS Y VEHÍCULOS

6.001. Conceptos generales. Los medios humanos y materiales constituyen los recursos existentes en un comando, organismo o instalación encargados de materializar el control.

Los procedimientos de identificación y control son los diferentes cursos de acción que se adoptan en el elemento de la Fuerza o en aquel que se encuentra bajo su responsabilidad, con la finalidad de efectivizar las medidas de seguridad de contrainteligencia vigentes.

Dichos procedimientos de identificación y control deberán estar estrechamente coordinados entre sí para lograr una mayor eficacia.

Los medios encargados de la identificación y control serán la guardia de prevención, personal de vigilancia, escoltas o custodios, recepcionistas y secretarios.

6.002. Identificación de personal militar y civil del elemento. Se exigirá la presentación de la "Credencial del elemento" (Anexo 3), se verificará su identidad mediante el control de sus documentos personales (DNI o DNI tarjeta argentina) y el cotejo con las listas existentes en la guardia.

El personal militar deberá identificarse con la cédula de identificación del Ejército.

Se cuidará que toda persona que lo acompañare fuere identificada y, en caso de no pertenecer al elemento, cumpliera con los requisitos establecidos.

Se vigilará que quienes entraren acompañados no lo hicieren bajo amenaza de un arma oculta por parte del acompañante, aun cuando mostraren una credencial del elemento.

Otro aspecto importante será la identificación del personal de soldados, a fin de evitar infiltraciones.

6.003. Identificación de personal ajeno al elemento. El ingreso de personal ajeno deberá restringirse, debiendo limitarse las visitas al personal destinado este. Se requerirá la rápida individualización del visitado, para evitar que personas extrañas, preguntando por personal inexistente, estudiaren el sistema de guardia del elemento, efectuaren reconocimientos, etc., o logren infiltrarse en el interior.

Se fiscalizará su acceso y circulación, se evacuará expeditivamente su consulta y se controlará su salida, indefectiblemente. Para concretar su identificación, podrán materializarse las siguientes acciones:

- a. A toda persona ajena al elemento se le confeccionará la "Ficha Control" (Anexo 4), previa entrega del documento de identidad.

Su duplicado quedará en la guardia de prevención o mesa de control. El original quedará con el visitante hasta que la persona visitada otorgue (mediante firma) su conformidad de entrada. Mientras tanto, el visitante permanecerá en el lugar de espera que se estableciere. No se aceptará otro documento de identidad que no fueren los mencionados anteriormente; en casos de extranjeros, se solicitará su pasaporte.

- b. Autorizada la entrada, el visitante llevará en un lugar visible la "Tarjeta de Circulación" (Anexo 5 y 6) y será acompañado por personal de guardia o, en su defecto, será controlado por algún otro sistema.
- c. Terminada la visita y con la firma del entrevistado, entregará en la guardia o receptoría la "Tarjeta de Circulación" y la "Ficha de Control"; ambos elementos serán controlados antes de ser devuelto el documento de identidad.

- d. Cuando se tratare de una delegación, sólo se hará "Ficha de Control" para el jefe de este y se asentará el resto de la delegación en forma numérica en el libro de novedades de la guardia o de la receptoría, previo control nominal por listas, en las que constará el nombre y número de DNI de cada integrante. Estas listas serán entregadas a la guardia con anterioridad a la visita.
- e. Diariamente, al relevo de cada servicio, las fichas originales serán entregadas al departamento, división o grupo de Inteligencia, el cual deberá llevar un registro detallado.
- f. Las fichas de control llevarán una numeración correlativa que se iniciará cada mes y estarán rubricadas por el oficial de inteligencia. Los duplicados serán incinerados; las fichas que se hubieren llenado erróneamente serán elevadas también, a fin de hacer el control correspondiente.
- g. Por similitud con los documentos de identidad y para facilitar una efectiva y rápida identificación, en la "Credencial del Organismo" deberán consignarse los detalles que figuran en el Anexo 4. Dentro de lo establecido en dicho anexo, el jefe del elemento podrá introducirle modificaciones para adaptarlo a este.
- h. Con respecto al pasaporte, donde figurarán los datos filiatorios, debe verificarse la correspondiente intervención de las autoridades migratorias argentinas y su fecha de vencimiento del mismo. En caso de anomalías, se dará intervención a las FFPP o FFSS que corresponda.
- i. En caso de deterioro del documento, solo tendrá valor la presentación de cualquiera de los otros documentos enunciados. Si fuere una cédula militar de identidad, podrá presentarse una libreta de enrolamiento o cédula de identidad donde conste la situación de militar.

6.004. Procedimientos de control. Son aquellas acciones que sirven para verificar el cumplimiento de las medidas de seguridad de contrainteligencia, establecidas por parte de los medios responsables.

A los fines del control integral de un elemento, se dispondrá, entre otras, de la documentación que se menciona a continuación y que deberá encontrarse en las guardias de prevención o receptorías:

- a. Gráfico actualizado con las relaciones de dependencia y su distribución en la instalación.
- b. Guía telefónica jurisdiccional.
- c. Guía de direcciones postales, telefónicas y telegráficas del Ejército y de la instalación.
- d. Fichero actualizado del personal militar y civil que preste servicio en el elemento, en el que constará jerarquía, apellido y nombre, destino interno (piso, número de local y teléfono), registro de rubricas y cifras de código de guarismos, que cada uno tuviere adjudicado. Considerar la confección de un software de base de datos.
- e. Nómina, por orden alfabético, de las credenciales vencidas, extraviadas olvidadas de la instalación y de otros organismos que interesaren.

6.005. Control de acceso y salida de personal militar y civil. Las guardias y/o receptorías serán los órganos responsables de atender todos los aspectos relacionados con el acceso y salida del personal de la instalación.

- a. Controlará, sin excepción y obligatoriamente, el contenido de todo elemento (portafolio, valija, paquete, etc.), que debiere entrar o salir por el acceso habilitado, salvo disposición contraria del jefe de elemento u organismo.
- b. Con respecto al personal militar ajeno a la instalación, se asentará el ingreso o depósito de los portafolios en la "Modelo de ficha de control de tránsito de personal en instalaciones militares" (Anexo 4). Esta ficha de control se confeccionará previa entrega del documento de identidad. A su vez, se le entregará una "Tarjeta de Circulación", que deberá portar sobre la prenda externa, en forma claramente visible, en el torso medio superior.

- c. En las circunstancias en que el jefe de elemento lo ordenase, se deberá palpar de armas al personal civil que entrare o saliere de la instalación. Se deberá considerar detalladamente esta circunstancia y se tendrá en cuenta que el personal que efectúe esta función deberá responder al mismo género de la persona por registrar. Se deberá llevar a cabo con detalle y guardando el mayor respeto y decoro que la situación requiera. El elemento u organismo deberá disponer de un lugar específico para llevar adelante este procedimiento.
- d. Cuando debieren recibirse custodias especiales o delegaciones, deberá ponerse en conocimiento a la guardia de prevención y receptoría, con suficiente antelación, de la hora de llegada y del objeto de la visita, a fin de evitar interferencias o problemas. Solamente se entregará a cada uno de los visitantes la "Tarjeta de Circulación", contraentrega del documento de identidad. No se permitirá, bajo ningún aspecto, el ingreso de personal civil ajeno al Elemento con armamento.
- e. El personal civil o militar que careciere de documentación de identidad no podrá ingresar en el organismo.

6.006. Control de acceso y salida de vehículos. Las personas que ingresen o egresen de una instalación podrán utilizar vehículos, los cuales, por sus características, exigirán la adopción de medidas particulares, tanto en lo que se refiere a dichas características como a aquellas relacionadas con el tipo de instalación militar de que se tratare.

Deberá evitarse que el vehículo sea un medio que pudiera servir para burlar las medidas de seguridad de contrainteligencia vigentes. El control del vehículo involucrará su registro y custodia.

a. Registro del vehículo.

El vehículo deberá ser revisado por completo, incluso los distintos compartimentos y componentes.

La forma de efectuarse el registro deberá estar determinada en el PON del elemento.

b. Custodia del vehículo.

La custodia del vehículo estará referida al control que se mantendrá sobre este, desde que se le efectúe el registro al entrar en la instalación hasta que se retire del organismo.

La tarea que deba realizar en el organismo la persona que viajare en el vehículo y el hecho de que este fuere o no vehículo militar, perteneciente o no al elemento, será determinante para disponer si se quedará en la playa de estacionamiento, si entrará en la instalación, etc.

El jefe del elemento deberá impartir claras directivas, teniendo en cuenta los siguientes aspectos:

- 1) Vehículos orgánicos del elemento: no requerirán custodia, salvo en determinados casos.
- 2) Vehículos oficiales ajenos al elemento: permanecerán en la playa de estacionamiento, pero, si por causas especiales, debieren circular por el interior de la instalación, se consultará al jefe del elemento u organismo el temperamento por seguir.
- 3) Vehículos particulares del personal militar o civil del elemento: normalmente, se les asignará un lugar determinado en la playa de estacionamiento y no circularán por el interior de la instalación.
- 4) Vehículos en general, ajenos al organismo: se evitará la circulación por el interior de la instalación, deberán permanecer en la playa de estacionamiento.
- 5) Vehículos de proveedores y cantineros: se les asignará custodia cuando circulen por el interior de la instalación, a fin de transportar mercaderías, deberán regresar de inmediato a la playa de estacionamiento.

6.007. Control de la circulación interna de personas. Tanto el personal militar como civil deberá ser consciente de que la presencia de personas extrañas en el elemento no solo será una debilidad, sino que perturbará el régimen de trabajo.

Cada uno deberá limitar las visitas que, por motivos intrascendentes o afectivos, frecuentaren las dependencias de la instalación. Los controles de seguridad, tales como identificación en los accesos, regulación de la circulación, áreas de seguridad y requisitos que cumplirán los integrantes del organismo y visitantes serán motivo de permanente preocupación de todo el personal.

Cada jefe de elemento u organismo, dentro de los procedimientos operativos normales de medidas de seguridad de contrainteligencia, pondrá particular atención en la regulación de esta actividad. A los fines del control de la circulación interna, podrán ser empleados:

a. Guardia de prevención.

Será el principal elemento de control y el responsable de la fiscalización de toda persona que circular por el elemento. En algunos organismos, se podrá disponer de policía militar para esta tarea.

b. Elementos de control de seguridad.

En los organismos que dispusieren de varias plantas o pabellones, deberá establecerse un control de seguridad que dependerá de la jefatura militar o de la guardia de prevención. Su composición será determinada por el jefe del elemento, quien, a su vez, fijará la misión concreta en los procedimientos operativos normales.

El jefe del elemento de control y seguridad tendrá como misión principal no permitir la circulación de persona alguna que no estuviere identificada por la "Tarjeta de Circulación" y la "Ficha Control". El control podrá materializarse en:

1) Piso o sector:

Cuando la magnitud o extensión del organismo lo exigiere, se designará un responsable de las medidas de seguridad de contrainteligencia por piso o sector al cual, por procedimientos operativos normales, se le asignarán misiones concretas.

2) En ascensores:

Los ascensoristas, si los hubiere, o los elementos de control de seguridad no permitirán el ascenso o descenso de visitantes sin la previa verificación ocular del color y/o número de piso correspondiente a la "Tarjeta de circulación", los cuales deberán ser coincidentes con los asignados a la planta respectiva.

3) En escaleras:

El uso de las escaleras deberá estar perfectamente delimitado para poder controlar, restringir o canalizar su uso por determinado personal.

4) Sectores o lugares para visitas:

En los procedimientos operativos normales deberán fijarse los sectores y lugares de acceso para visitas. Personal de guardia, servicio de vigilancia y policía militar o de seguridad deberán controlar los movimientos de los visitantes, para asegurarse de que no entren en las áreas para las cuales no tuvieron la autorización correspondiente. Deberán contemplarse, especialmente, las siguientes circunstancias:

a) Visitas al personal de soldados voluntarios. No tendrán acceso al interior del elemento, salvo los lugares especialmente autorizados.

b) Visitas al personal de los cuadros. Quedarán bajo la responsabilidad del visitado, quien las recibirá en los locales autorizados al efecto, y no se les permitirá el libre tránsito por la instalación.

6.008. Áreas de estacionamiento. Para los vehículos ajenos al elemento se determinará la playa de estacionamiento, que en principio, estará fuera del sector de edificios. Si fuere necesario, por las características del organismo, se la delimitará dentro de este. Para su establecimiento, se considerarán los siguientes aspectos:

a. Que estuvieren alejadas de los depósitos.

- b. Que sus límites estuvieren a no menos de 5 metros de cualquier edificio, dentro de las posibilidades del elemento.
- c. Que se delimitaren los lugares para los vehículos particulares del personal de la instalación.
- d. Que se previeren lugares permanentes para vehículos de las visitas.
- e. Que se mantuviere una permanente vigilancia sobre el área y sobre los caminos que condujeran a ella.

6.009. Control de proveedores, cantineros y contratistas

- a. Proveedores.

Los proveedores permanentes, normalmente, deberán entrar hasta determinadas dependencias del elemento, a fin de entregar su mercadería. Dicho personal podrá disponer de una autorización de acceso, de acuerdo con lo que determinare el jefe del elemento y con la única finalidad de agilizar las tareas.

Los proveedores no permanentes se ajustarán al régimen de control establecido para el personal ajeno a la instalación y llenarán las exigencias establecidas para la entrada del personal ajeno en el elemento.

En todos los casos, los proveedores serán acompañados por personal de control mientras dure su permanencia. El personal de control cuidará que los proveedores se dirijan exclusivamente al lugar de destino interno y no concurran a otro, y también que no descarguen o carguen efectos que no fueren los que, por su tarea, correspondiere tramitar.

- b. Cantineros.

El personal de cantineros, en general, será considerado como proveedor permanente. Sin embargo, el hecho de permanecer diariamente en la instalación, de entrar y salir con mercaderías y de tener contacto con la mayor parte del personal del elemento, exigirá un control particular.

El control deberá ser llevado a cabo por todo el personal militar de la instalación, sobre la base del conocimiento de las disposiciones vigentes.

- c. Vendedores de artículos varios.

Estará prohibido el acceso de vendedores o promotores a los elementos militares, para la venta o promoción de cualquier artículo. Podrá existir una autorización especial del EMGE, pero este deberá haber llegado a través de los canales de comando correspondientes.

- d. Contratistas, subcontratistas, licitantes.

Cuando se tratare con representantes de entes o firmas ajenas a la organización del Ejército que debieren efectuar trabajos en el elemento, deberán tenerse en cuenta los siguientes aspectos:

- 1) Antes de proporcionarles a su solicitud, planos, especificaciones u otra información relativa a proyectos o estudios clasificados, deberán leer y firmar un acta por la cual certificarán quedar enterados de la clasificación de seguridad de los que se les revelare, grado del secreto por mantener, precauciones para el manejo del material y seguridad del archivo y conservación.
- 2) Deberá hacerse constar que han tomado conocimiento de las penalidades que la ley establece para casos de violación del secreto militar.
- 3) La autoridad militar que adjudicare trabajos clasificados deberá establecer restricciones sobre los movimientos de personas empleadas que entren en sus plantas y oficinas, de acuerdo con las condiciones particulares y con la situación de cada establecimiento.

La autoridad militar que hubiere realizado los contactos mencionados tendrá la responsabilidad de impartir directivas precisas, sobre los procedimientos que se adoptarán en relación con las medidas de seguridad de contrainteligencia necesarias.

Asimismo, deberá efectuar periódicas inspecciones para constatar el permanente cumplimiento de dichas medidas.

6.010. Personas o entes civiles alojados en instalaciones militares. Como norma, no se proporcionará alojamiento en instalaciones militares a delegaciones de colegios, universidades, entidades deportivas, etc. Las excepciones a lo expresado serán motivo de una solicitud previa, al comando correspondiente. En caso de concurrencia, con autorización y por disposición de la superioridad, el personal concurrente deberá quedar en todo momento bajo su control. A tal efecto:

- a. Serán recibidos por una comisión previamente designada y acompañados hasta el lugar de alojamiento.
- b. Se les avisará sobre el sector o sectores por donde podrán transitar.
- c. Se les determinará el o los lugares de acceso que podrán utilizar.
- d. Se les hará conocer la prohibición de efectuar tomas fotográficas o de otro tipo en el interior del elemento.
- e. Se verificará el cumplimiento de las medidas de seguridad.

La autorización dada por la superioridad será remitida al elemento por el Comando correspondiente y no la presentará la delegación, para evitar falsificaciones o falsas autorizaciones.

6.011. Personal militar o autoridades extranjeras

- a. Toda vez que los agregados militares o personal civil de las misiones diplomáticas extranjeras, acreditadas ante el gobierno argentino y personal militar extranjero, ya fuere incorporado a nuestro Ejército o de tránsito en el país, concurrieren a elementos u organismos de la Fuerza, con el objeto de efectuar visitas o realizar gestiones oficiales o particulares de cualquier naturaleza, se les informará, sin excepción, que para ello deberán requerir la autorización previa en el Estado Mayor General del Ejército. Simultáneamente, darán cuenta del hecho al mencionado Comando Superior, siguiendo la vía jerárquica.
- b. Cuando los organismos del Ejército apreciaran indispensable invitar a los referidos militares y diplomáticos extranjeros a los actos o ceremonias de carácter oficial que realizaren en sus respectivas dependencias, deberán formular dichas invitaciones por intermedio del Estado Mayor General del Ejército, salvo que existiesen autorizaciones especiales.
- c. La autoridad del establecimiento visitado, y de acuerdo con las directivas que a tal efecto impartirá el Estado Mayor General del Ejército, elevará un informe toda vez que al elemento u organismo ingresare personal militar o autoridades extranjeras. Los informes por elevar deberán responder, como mínimo, a la siguiente información:
 - 1) Identificación de las visitas.
 - 2) Permiso otorgado.
 - 3) Asuntos que despertaron su mayor interés.
 - 4) Naturaleza de las preguntas efectuadas.
 - 5) Habilidad, inteligencia y conocimiento de los visitantes.
 - 6) Probable objetivo.
 - 7) Conocimiento del idioma.
 - 8) Conclusiones.
- d. Si el programa de visitas previere la concurrencia de personal extranjero a un instituto o escuela de arma, se tendrá en cuenta que las exposiciones o demostraciones estarán referidas solamente a aspectos generales de doctrina y que, cuando se refirieren a organización, se desarrollarán en forma eminentemente esquemática. En general, no deberá exponerse sobre eficiencia y planes de empleo.

6.012. Visita de funcionarios del propio país. Las actividades propias del elemento y las directivas particulares que existieren en cada una regirán las visitas de funcionarios del propio país,

fabricantes o sus representantes, ingenieros o inventores que cooperaren en trabajos a cargo del gobierno nacional.

En general, estas visitas serán autorizadas únicamente por el Estado Mayor General del Ejército u otra autoridad responsable.

En el caso de visita de legisladores, se tendrá en cuenta lo establecido en el reglamento "Servicio Interno y en Guarnición" y las órdenes impartidas al respecto por el Estado Mayor General del Ejército.

6.013. Personal designado ayudante de oficiales superiores extranjeros. La presencia en el país de personal militar extranjero de elevada jerarquía impondrá la designación de personal superior en carácter de ayudante de aquellos. Dicha función requerirá, en quien la desempeñare, discreción con respecto a asuntos del servicio que no estuviere autorizado a revelar; en particular, será necesario que tenga permanentemente presente lo referente a la "disciplina del secreto".

La función de ayudante presentará, en forma permanente, variadas situaciones, las cuales requerirán una sólida conciencia de medidas de seguridad contrainteligencia, a fin de posibilitar un desempeño natural y cortés sin transgredir las disposiciones existentes. En general, se tendrá en cuenta lo siguiente:

- a. No hará comentarios sobre la situación política, económica y social del país de origen del oficial visitante, se limitará solo a escuchar cortésmente lo que este manifestare en su conversación.
- b. Evitará incursionar sobre temas políticos, económicos o sociales de nuestro país y, si el curso de la conversación llevare a ello, manifestará generalidades.
- c. Rechazará con toda altura y corrección cualquier comentario que implicare una crítica a nuestras autoridades nacionales y/o militares.
- d. No portará consigo documentación clasificada; en caso de tenerla consigo, no la entregará como antecedente ni hará conocer su contenido, sin autorización del comando superior respectivo.
- e. No conducirá al visitante a instalaciones militares donde existiere restricción de acceso.
- f. Pondrá en conocimiento del oficial extranjero que no se autoriza la toma de fotografías u otras imágenes en el ámbito del elemento, salvo orden en contrario.
- g. En caso de comprobarse alguna actividad subrepticia, deberá darse cuenta al Oficial de Inteligencia para determinar la responsabilidad del causante y se informará al comando superior para la adopción de la medida a que diere lugar, teniendo en cuenta el marco legal vigente en sus artículos referidos a las actividades de espionaje (Código Penal de la Nación Argentina).

6.014. Estudiantes militares o civiles extranjeros que realizaren cursos en institutos militares argentinos. Las medidas de seguridad de contrainteligencia por adoptar tenderán a evitar que, en el lapso de su estadía, obtuvieren, como consecuencia de una vida en común con personal militar propio, información de interés nacional o institucional que debiere preservarse. A tal efecto:

- a. Los institutos en donde revistaren becarios extranjeros elevarán al EMGE (Dir Grl Icia), por canal de comando, los datos de identidad obtenidos de los documentos personales de los causantes.
- b. En la orientación inicial que se les efectuare deberá hacérseles conocer las zonas por donde podrán moverse con entera libertad y aquellas que les estuvieren vedadas o reservadas para el propio personal.
- c. Por ninguna causa tendrán acceso a información que no fuere pública e indispensable para sus estudios.
- d. El personal docente del instituto deberá estar alertado, con la finalidad de poder adoptar los recaudos necesarios para evitar proporcionar información clasificada como "RESERVADO", "CONFIDENCIAL", "ESTRICTAMENTE SECRETO Y CONFIDENCIAL" y "SECRETO".
- e. En caso de tener que exponer temas que encuadraren dentro de la clasificación de seguridad expresada en d., los becarios extranjeros no deberán concurrir o serán separados temporalmente de la actividad educativa.

- f. No se les entregará documentación que pudiese vulnerar el concepto de “necesidad de saber”.
- g. Se establecerá un sistema para guardar la información clasificada, para evitar que los alumnos pudiesen sacarla del instituto.

6.015. Visitantes a fábricas y establecimientos militares que trabajan con proyectos o producen material clasificado. Personal superior de los cuadros o autoridades de gobiernos extranjeros podrán ser admitidos en establecimientos fabriles militares o civiles, donde se trabajare en proyectos o se produjeran materiales clasificados, solamente con autorización del Estado Mayor General del Ejército.

- a. No deberá enseñárseles ni explicar aspecto alguno sobre asuntos clasificados, excepto lo que considerare conveniente y/o necesario la autoridad responsable del establecimiento visitado y acorde con las directivas que se impartieren al respecto.
- b. Serán acompañados y mantenidos bajo control en todo momento.
- c. Toda solicitud de visita por parte de personal extranjero deberá encaminarse a través del Estado Mayor General del Ejército e incluirá los siguientes datos:
 - 1) Nombre/s y apellido/s, completos.
 - 2) Documento de identidad o pasaporte.
 - 3) Grado, título oficial, cargo o función que desempeñare en el momento.
 - 4) Nombre del establecimiento, planta, puesto o lugar que desee visitar.
 - 5) Propósito de la visita.
 - 6) Fecha o fechas en las cuales desee hacer la visita.
- d. La autoridad responsable del establecimiento visitado, complementando las disposiciones vigentes, deberá elevar, una vez concluida la visita, un informe que podrá contener:
 - 1) Nombre y apellido de los visitantes.
 - 2) Nacionalidad.
 - 3) Grado, cargo, título o función de los visitantes.
 - 4) Permiso para la visita.
 - 5) Asuntos sobre los que los visitantes demostraron mayor interés.
 - 6) Naturaleza general de las preguntas formuladas.
 - 7) Objeto manifestado de la visita.
 - 8) Estimación sobre el objetivo real perseguido.
 - 9) Habilidad, inteligencia y conocimiento técnico de los visitantes.
 - 10) Conocimiento del idioma, si correspondiere.
 - 11) Lista de lo que se les hubiere enseñado o explicado.

6.016. Proceder con periodistas. El proceder con los periodistas estará determinado por las directivas impartidas por el Estado Mayor General del Ejército, a los comandantes, directores y jefes de elementos ajustarán su proceder.

Dentro de la información autorizada a difundir, deberá tenerse en cuenta que en ella no deberá deslizarse información clasificada y de difusión no autorizada.

Únicamente el Estado Mayor General del Ejército podrá nombrar corresponsales militares o periodistas acreditados. Su actividad estará regida por los reglamentos correspondientes y directivas que, a tal efecto, dictare el Estado Mayor General del Ejército.

Los comandantes, directores y jefes de elemento no harán declaraciones ni autorizarán la actividad de periodistas dentro de sus organismos sin la autorización expresa del Estado Mayor General del Ejército. Este deberá llegar por el trámite normal de la correspondencia militar, para evitar falsificaciones o falsas autorizaciones.

En el caso de que un periodista trajera consigo alguna autorización extendida por el Estado Mayor General del Ejército, se ratificará su contenido ante ese comando para verificar su autenticidad; mientras tanto, su portador no podrá hacer ninguna gestión dentro del organismo o relacionado con él, con personal perteneciente a éste, dentro o fuera de la instalación.

En todos los casos, se le hará presente al periodista, con la atención debida, la imposibilidad de brindar información no autorizada debido a las estrictas órdenes existentes al respecto.

SECCION II

CONTROL DE INSTALACIONES Y EFECTOS

6.017. Control en edificios, pisos y sectores. Durante las horas de trabajo, la seguridad estará dada, en primera instancia, por el personal de cada dependencia, mientras que la guardia de prevención o el elemento de control de seguridad fiscalizarán los lugares de acceso y circulación de acuerdo con las órdenes existentes.

- a. Fuera de las horas de trabajo, la seguridad en las partes constitutivas del edificio o instalación recaerá en la Gu Prev, la que deberá asentar cada control y novedad que detectare de acuerdo con las órdenes y directivas que se impartan en el elemento u organismo.

6.018. Control en locales y depósitos para la guarda de documentación, materiales y otros efectos. Se comprobará que la documentación clasificada fuere archivada en muebles adecuados desde el punto de vista de seguridad. No podrá guardarse documentación clasificada en armarios o locales que carecieren de instrumentos de cierre adecuados.

- a. La documentación de alta clasificación de seguridad estará guardada en cajas de seguridad o locales preparados con puertas provistas de cerraduras de seguridad, de claves numéricas o de otro sistema que brindare similar seguridad.
- b. La documentación reservada y pública podrá estar en armarios metálicos que tuvieren cerraduras de seguridad.
- c. Las cajas de seguridad que contuvieren documentación de alta clasificación tendrán en la cara interna de la puerta un inventario de esta con un "Ficha índice de documentos en custodia" (Anexo 7), lo cual permitirá ejercer el control sobre ella.
- d. La evacuación de informes sobre la actividad o trabajo de cada dependencia será hecha, exclusivamente, por el jefe de esta.
- e. Ningún documento podrá ser sacado del lugar de trabajo, salvo excepciones debidamente autorizadas.
- f. En ningún caso podrá permanecer en un local personal que no hubiere sido autorizado para operar en el nivel de clasificación de documentos que allí se trataran.
- g. Previa a la entrada del personal de limpieza, el responsable del lugar controlará que no hubiere documentación clasificada fuera de los lugares de guarda.
- h. Al término de la tarea diaria, el jefe o el encargado de cada local, oficina, depósito, etc., verificará que la documentación y el material que hayan sido manipuladas se encuentren en el lugar de guarda prevista.
- i. Cuando el o los titulares de los locales debieran retirarse circunstancialmente estos deberán ser cerrados con llave y guardar la documentación clasificada.

- j. Después de retirarse el personal que trabajare, cada dependencia, por medio de personal del elemento de control de seguridad, policía militar u otro designado al efecto, controlará que no queden elementos clasificados fuera de sus lugares.

En caso de encontrarse material fuera de su sitio, se guardará en lugares seguros y se entregará al día hábil siguiente al jefe responsable, y se informarán la novedad y circunstancias del hallazgo.

- l. Cada organismo dispondrá el sistema más conveniente para la guarda de llaves.
- n. Fuera del horario de actividades, cualquier persona que encontrare alguna anomalía (abandono, locales abiertos, documentación fuera de los lugares de guarda, etc.) dará la novedad al jefe del control de seguridad o guardia de prevención, quien efectuará el control correspondiente, y la asentará en los documentos que correspondan. Verificada alguna anomalía, colocará una faja de seguridad y llamará al jefe de la dependencia para que verifique las novedades existentes.
- o. Las áreas de seguridad deberán tener en lugar visible el cartel correspondiente, a fin de ser debidamente identificadas.

6.019. Control en muebles, armarios, cajas de seguridad y otros. Deberá establecerse en cada elemento el proceder con las llaves de estos elementos y lugares de guarda.

- a. En los relevos de jefaturas deberán cambiarse las combinaciones de las cajas de seguridad o lugares (si fuere posible) en los que se guardare información de alta clasificación de seguridad.
- b. Los responsables del manejo de documentación de alta clasificación de seguridad procederán a registrar y controlar las planillas "Registro de seguridad de manipulación de información documentada con clasificación XXXXX" (Anexo 8). Esta ficha será empleada cada vez que se depositare o extrajere documentación de esta clasificación. Mantener, siempre que no fuese utilizada la documentación diaria, cerrado el armario o mueble que la contiene.

6.020. Control en aulas, salas cinematográficas y otros. En estos lugares no deberán tratarse aspectos clasificados en presencia de camareros, mozos, etc.

- a. Se cuidará que las conversaciones que se mantuvieren dentro de ellas no pudieren ser oídas desde el exterior del recinto.
- b. En la preparación y exhibición del material ilustrativo deberán adoptarse medidas de precaución para no dejar expuestos datos de carácter clasificado.
- c. Se dispondrá de un lugar adecuado para la guarda de las ayudas de exposición cuando se tratare de asuntos clasificados.
- d. Se confeccionará el material de ayuda con personal autorizado y en lugares que tuvieren la seguridad suficiente para proteger todo tipo de información.
- e. Con anterioridad y posterioridad a una conferencia o clase de alta clasificación, se efectuará una inspección de seguridad.

6.021. Control de talleres, depósitos, laboratorios y surtidores. No deberán tenerse a la vista cuadros indicadores de efectivos, cantidades, planillas de movimientos de efectos, entregas o recepciones.

- a. Se instruirá al personal en la prohibición de hacer comentarios sobre las existencias que se guardaren, naturaleza de estas reparaciones, movimientos, etc.
- b. Al iniciar la tarea diaria, se comprobará:
 - 1) En talleres y laboratorios:
 - a) Cierre de las puertas de acceso.
 - b) Cierre de las fuentes de energía (llaves de luz, motores, gas, Etc).
 - 2) En los depósitos:

- a) Cierre de las puertas de acceso.
 - b) Corte del fluido eléctrico.
 - c) Estado de las existencias (visualmente).
- 3) En los surtidores:
- a) Cierre de las llaves de paso.
 - b) Combustible derramado.
 - c) Control de numeración.
- c. Al finalizar las tareas diarias se comprobará y se asentará en la planilla correspondiente:
- 1) En talleres, parques y laboratorios:
- a) Guarda y limpieza de materiales y herramientas.
 - b) Cierre de las fuentes de energía.
 - c) Estado del material contraincendio.
 - d) Cierre de armarios, cofres, cajas de seguridad, etc.
 - e) Limpieza y recolección de materias y combustibles de desecho.
 - f) Cierre de locales y puertas de acceso.
- 2) En los depósitos;
- a) Ordenamiento de las existencias.
 - b) Guarda del material.
 - c) Guarda de la documentación.
 - d) Limpieza de sectores y eliminación de residuos.
 - e) Apagado de luces.
 - f) Cierre de locales y puertas de acceso.
- 3) En los surtidores.
- a) Control de numeración.
 - b) Cierre de llaves de paso.
 - c) Limpieza de sectores (combustibles derramados).

6.022. Control sobre evacuación y destrucción de documentos y materiales. Cada elemento planeará un sistema de evacuación y destrucción de determinados materiales, documentación y/o instalaciones, de ser necesario, para casos de emergencia. Esto estará contenido dentro de los procedimientos operativos normales de esta.

El PON contendrá el detalle de la evacuación, por parte del personal, documentación y del material, y la destrucción de lo que no pudiese ser evacuado. Serán establecidas las prioridades por medio de siglas de encubrimiento bien visibles, que responderán a números que fijarán dicha prioridad.

La destrucción estará motivada por el peligro de que la instalación pudiera caer en poder del enemigo en caso de no poder ser evacuada.

Evacuación. En el PON se establecerá en qué circunstancia se evacuará la instalación y de qué forma. Se determinarán prioridades en todos los aspectos referidos a personal, documentación y material, así como, responsables de la tarea y constancias por asentar.

La destrucción se llevará a cabo de acuerdo con las prioridades fijadas y, en lo posible, de acuerdo con la siguiente forma: quemándolos, utilizando máquinas apropiadas, productos químicos, etc, cuando se tratare de documentos. Con el material se procederá con analogía y aun aplicando otros métodos de destrucción.

Cuando se tratare de material de gran volumen, que hiciere difícil la destrucción total, se lo hará por prioridades, destruyendo primero el material más importante.

CAPÍTULO VII

MEDIDAS DE SEGURIDAD REFERIDAS A LA DOCUMENTACIÓN Y MATERIAL CLASIFICADO

SECCION I

CONCEPTOS GENERALES

7.001. Definición. Conjunto de disposiciones destinadas a preservar que los materiales y documentos que contengan información clasificada se produzcan, tramiten, utilicen, custodien y/o guarden y destruyan, bajo la premisa de impedir su incorrecta difusión o toma de conocimiento por personas no autorizadas, a fin de evitar que sean objeto de una posible acción por parte de actores que representen amenazas o riesgos para la seguridad del instrumento militar y del Estado Nacional.

7.002. Consideraciones básicas. La información puede estar contenida en diversos soportes (papel, digitales y otros), bajo diferentes formatos (textos, imágenes, gráficos, entre otros) y también en objetos cuya cualidad permita incorporar información clasificada (equipo encriptador, un navegador con rutas cargadas, un sensor con registros acumulados, una línea de datos de sistemas de armas u otros), que por su naturaleza, en determinadas circunstancias, sean la información por proteger.

Esta variabilidad requiere que la protección de documentos y materiales clasificados sea extensiva a toda la secuencia de acciones que involucra la exposición de estos elementos, mediante la adopción de medidas y procedimientos que desalienten la configuración de situaciones propicias para que puedan ser abordados por la Inteligencia del enemigo u oponente real o potencial (PC-12-04).

Cada instancia interviniente en los diferentes procesos en que se involucre información clasificada deberá generar las medidas y procedimientos que particularicen la aplicación de las pautas establecidas en la presente publicación, teniendo especialmente en cuenta que, en principio, la exposición innecesaria de la información clasificada podrá estar dada por la negligencia, impericia, indiscreción, ignorancia o imprudencia del personal propio.

Estas medidas serán aplicadas en todo tiempo y lugar y bajo cualquier situación en que se desarrollen actividades de la Fuerza. Se aplicarán en todos los niveles, adecuándolas a las necesidades particulares de cada uno de ellos y en relación con la situación de ese momento.

7.003. Seguridad de la información documentada. La seguridad de la información documentada es la resultante de aplicar un conjunto de medidas para alcanzar un nivel adecuado de confidencialidad, integridad, disponibilidad, no repudio y autenticación de la información clasificada durante todo el proceso de su gestión.

7.004. Información documentada. Es toda aquella información que se encuentre contenida en un soporte permanente. Así podrá ser considerada la información registrada de alguna manera, en textos escritos con medios tecnológicos o a mano, cartografía, manuales, códigos, diarios, elementos de identificación de origen, grado o destino, archivos militares, oficiales o privados, cintas magnetofónicas, fotografías, bases de datos digitalizadas, video y todo otro dispositivo que por su característica se utilice para contener información.

7.005. Información oficial. Toda información que proceda de fuentes estatales, en cualquiera de sus niveles, incluyendo los propios gubernamentales o militares, debe ser considerada de carácter oficial y dada a conocer únicamente cuando se cuente con expresa autorización de la fuente. También incluye toda aquella información de origen estatal extranjero que haya sido confiada al personal nacional en virtud de su rango, cargo o función desempeñada.

SECCION II

NORMAS DE SEGURIDAD DE CONTRAINTELIGENCIA QUE RIGEN LA CONFECCIÓN Y EL TRATAMIENTO DE LA DOCUMENTACIÓN

7.006. Normas de seguridad a aplicar sobre la información documentada. Son el conjunto de pautas destinadas por materializar la participación en la protección de la información documentada por parte de las instancias que intervienen en su gestión. Ellas son:

- a. Clasificación.
- b. Reclasificación.

- c. Elaboración y tramitación.
- d. Determinación del distribuidor.
- e. Reproducción.
- f. Registro.
- g. Archivo, custodia y guarda.
- h. Transmisión.
- i. Entrega y recepción de la información documentada.
- j. Control de entrada y salida de documentación.
- k. Destrucción (normal y de emergencia).
- l. Evacuación.
- m. Control de la información documentada. Responsabilidades.

7.007. Clasificación. Determinación de la clasificación de seguridad de la información documentada. La clasificación de las informaciones, documentos o materiales consiste en la fijación de su carácter en relación con el grado de reserva que se le asigne y con las restricciones para su difusión. Ello surge de considerar el significado de los contenidos de la información y de la magnitud del riesgo que implica su conocimiento por parte de personal no autorizado.

La responsabilidad de la asignación del carácter de la información contenida en documentos y materiales será de las autoridades que se especifiquen para cada caso.

Para las informaciones, el responsable será aquella autoridad que tuviere a su cargo la fuente de donde esta emanare.

Para los documentos y materiales, será aquella autoridad que los origine.

Quien imponga la clasificación de los documentos debe considerar que constituye una falla de la seguridad tanto el asignar una categoría menor a la necesaria, por el riesgo que implica ampliar su difusión, como el asignar una clasificación de seguridad excesiva, lo cual provoca que se desaproveche la información se evite que llegue a quien tiene necesidad de saber.

Las autoridades pertinentes fijarán quién podrá tomar conocimiento de las informaciones precisadas para ello o determinará el grado de autorización a los fines de su difusión. Ninguna información oficial incluyendo aquella de naturaleza pública, podrá ser difundida ni ser conocida por personas ajenas al ámbito oficial, que no fueren responsables de su tratamiento. Cuando una información pudiere ser de conocimiento público, deberá determinárselo expresamente.

La violación de las normas de seguridad establecidas traerá como consecuencia la sustanciación de las actuaciones correspondientes y la aplicación de las penalidades contenidas en el "Código de Disciplina de las Fuerzas Armadas" y su reglamentación, y en las demás leyes o normas dictadas al efecto.

Genéricamente y a los efectos del establecimiento del vínculo legal de las personas con la información clasificada, se encuentra definido en la legislación vigente el "Secreto Militar", que alude no a la clasificación establecida por el Decreto 950/2002, sino al tipo de información que por su contenido resulta de interés preservar para la Defensa.

7.008. Escala de clasificación de la información. A la información oficial originada en el Ejército, así como a toda otra por tramitarse en esta, procedente de otros organismos oficiales o privados, se les asignará la clasificación de acuerdo con lo establecido en la Reglamentación de la Ley Nacional de Inteligencia - Título V - Artículo 10º y el Decreto 950/2002:

- Estrictamente Secreto y Confidencial.
- Secreto.

- CONFIDENCIAL
- RESERVADO.
- PÚBLICO.

Las tres primeras serán consideradas como de alta clasificación de seguridad.

Se asignará la clasificación de “ESTRICTAMENTE SECRETO Y CONFIDENCIAL” a toda aquella información que, por su naturaleza, contuviere datos relacionados con actividades de los órganos de Inteligencia.

Se asignará la clasificación de “SECRETO” a toda información que, por su carácter e importancia, requiere una máxima protección de seguridad, ya que su divulgación indebida causaría daño excepcional a la Fuerza y/o a la Nación, o perjudicaría la ejecución de sus respectivos planes.

Se asignará la clasificación de “CONFIDENCIAL” a la información cuya divulgación indebida afectare los intereses de la Fuerza y/o la Nación, o que se refiriere a conceptos que podrían afectar el prestigio y/o moral del personal, así como la disciplina.

Se asignará la clasificación de “RESERVADO” a toda aquella información que, no estando comprendida en las clasificaciones anteriores, pudiese ser conocida por el personal perteneciente la Fuerza.

Se asignará la clasificación de “PUBLICO” (PÚBLICO – MILITAR) a toda aquella información, cuyo conocimiento estará limitado al personal perteneciente al Instrumento Militar.

7.009. Imposición de la clasificación de seguridad

- a. Corresponderá la clasificación “ESTRICTAMENTE SECRETO Y CONFIDENCIAL” a lo siguiente:
 - 1) Antecedentes y documentación que se refiere a las actividades, fuentes, medios y/o procedimientos utilizados por las unidades y organismos de Inteligencia.
 - 2) Identidad, actividad, empleo, ubicación u otra información de cierto y determinado personal de Inteligencia.
 - 3) Antecedentes referidos a personal, cuando estuviere cumpliendo misiones especiales de servicio.
 - 4) Todo tipo de antecedentes relacionados con el enemigo, registrados en los archivos de Inteligencia.
- b. Corresponderá la clasificación de “SECRETO” a la información contenida en los siguientes asuntos originados o tramitados en el Ejército:
 - 1) Objetivos políticos y políticas nacionales, en todos sus contenidos que, por su trascendencia, obligaren a tal clasificación.
 - 2) Asesoramientos al Jefe del Estado Mayor General del Ejército sobre aspectos relacionados con sus funciones extra-Fuerza que determinare la legislación en vigencia y/o medidas subsidarias.
 - 3) Objetivos de guerra y militares.
 - 4) Política militar.
 - 5) Planes de desarrollo y funcionamiento del Ejército y de Campaña, operaciones y tácticos.
 - 6) Objetivo orgánico de guerra.
 - 7) Documentos derivados de los planes tácticos de la Fuerza.
 - 8) ordenes de batalla y determinados cuadros de organización.
 - 9) Información extranjera, cuyo origen o contenido no se debiere divulgar.

- 10) Estudios, investigaciones, experiencias o inventos de importancia vital para la seguridad nacional y/o militar.
- 11) Documentación y material criptográfico.
- 12) Estudios, investigaciones, experiencias o inventos de importancia vital para la seguridad nacional y/o militar.
- 13) Adquisiciones, fabricaciones y construcciones de materiales críticos para la defensa nacional, así como ciertas características fundamentales de abastecimiento y obras militares, buques, aeronaves y material de guerra en general.
- 14) Datos fundamentales relativos a materiales críticos de importancia.
- 15) Cartografía e imágenes que dieren ideas de una intención operativa, situación de tropas, datos estadísticos y otros que por su actualidad, en caso de divulgación, pusieren en peligro la seguridad de la Nación.
- 16) Documentación que, por su contenido, pudiese permitir la divulgación de asuntos, contenidos en reglamentos secretos o en otra documentación de ese carácter.
- 17) Informaciones sobre el empleo de técnicos y/o equipos que pudieren permitir la divulgación de sistemas particulares de comunicaciones establecidos o que se estableciere por la Fuerza.
- 18) Información sobre pago de efectos, cuya adquisición fuera clasificada como SECRETO.
- 19) Datos, antecedentes, informes, documentación, etc., procesados en sistemas de computación de datos, así como sus tarjetas y medios técnicos de confección referidos a documentación de carácter SECRETO.
- 20) Datos, base de datos de usuarios, videos, imágenes, base de datos de eventos de alarmas, base de datos de eventos de acceso, claves lógicas, procedimientos, procesos, datos técnicos de los equipos empleados y toda otra información relacionada con los sistemas de seguridad deberán ser considerados de carácter SECRETO.

c. Corresponderá la clasificación de "CONFIDENCIAL", entre otras, a la información contenida en los siguientes asuntos:

- 1) Política de la Fuerza en el marco nacional e institucional.
- 2) Objetivo orgánico de paz.
- 3) Objetivo orgánico del Ejército.
- 4) Política orgánica del Ejército.
- 5) Planes parciales, órdenes y directivas derivadas de planes secretos, cuya divulgación no causare daño excepcional a la Nación o no perjudicare a la ejecución de los planes de Estado.
- 6) Preceptos doctrinarios que se volcaren en los proyectos, instalaciones, directivas, informes, críticas de ejercitaciones, maniobras, etc.
- 7) Ejercitaciones y maniobras que no debieren divulgarse, así como todo aquello que permitiere conocer en forma amplia el estado de adiestramiento y/o moral de las FFAA.
- 8) Observaciones o conceptos que afectaren la moral o disciplina al referirse al desempeño de oficiales.
- 9) Informaciones contenidas en el orden de batalla, cuadros de organización y/o distribución de efectivos.
- 10) Información sobre eficiencia de servicios, instalaciones y elementos.
- 11) Inventarios de codificación, documentación y material criptográfico.

- 12) Actuaciones de los tribunales de calificación u otros en lo que respecta a oficiales superiores, jefes y oficiales subalternos.
 - 13) Aspecto de los legajos personales referidos al estado sanitario y datos que pudieren afectar la moral de las personas.
 - 14) Conceptos, calificaciones y sanciones disciplinarias del personal de oficiales.
 - 15) Todo lo que constituye SECRETO MÉDICO.
 - 16) Información de pagos de efectos y toda la documentación relacionada y concurrente, cuya adquisición fuere clasificada como CONFIDENCIAL.
 - 17) Estudios, adquisiciones y obras que conviniere mantener en este carácter, particularmente lo referido a materiales de guerra.
- d. Corresponderá la clasificación de “RESERVADO”, entre otras, a la información contenida en los siguientes asuntos:
- 1) Estado o condiciones de sanidad de determinadas zonas o efectivos.
 - 2) Ascensos, nombramientos, traslados, altas y bajas del personal militar, salvo aquellos que, a juicio del JEMGE, se considerare conveniente su publicidad.
 - 3) Actuaciones de las juntas de calificaciones, conceptos y sanciones disciplinarias del personal de suboficiales y de determinado personal civil.
 - 4) Los reglamentos que así se especifican en el Registro de Publicaciones Militares y determinadas publicaciones.
 - 5) Planes de conjunto y ubicación de organismos.
- e. Corresponderá la clasificación de “PÚBLICO” (PÚBLICO - MILITAR), entre otras, a la información contenida en los siguientes asuntos, de acuerdo con los temas que traten, dado que según el mismo, podrán tener una clasificación de seguridad superior:
- 1) Reglamentos vigentes en la Fuerza.
 - 2) Proyectos de reglamentos.
 - 3) Trabajos de gabinete.
 - 4) ordenes del día.
 - 5) Reglamentos y/o manuales que contengan leyes de carácter nacional (Código de Disciplina de las Fuerzas Armadas, Ley para el Personal Militar y otros).

7.010. Identificación de documentos. Con el objeto de identificar la clasificación de seguridad de la información documentada y contribuir a su control, se han fijado una serie de medidas formales que se concretarán a través de las siguientes tareas:

- a. Confección de la carátula.

Las carátulas, en los documentos que debieren llevarla serán del color que correspondieren según la clasificación de seguridad que a continuación se determina:

ROSA: documentos de carácter PÚBLICO.

AMARILLO: documentos de carácter RESERVADO.

AZUL CELESTE: documentos de carácter CONFIDENCIAL.

VERDE NILO: documentos de carácter SECRETO.

MARRÓN CLARO: documentos de carácter Estrictamente SECRETO Y CONFIDENCIAL.

b. Sellos.

Se deberá considerar también que en la parte superior e inferior el sello o la inscripción con la clasificación de seguridad, según correspondiere, se colocará de acuerdo con lo especificado en el RFP-70-05 - Documentación, Capítulo II, artículos 2.012 y 2.019.

7.011. Vicios de clasificación. Para evitar la clasificación excesiva, la autoridad responsable, antes de aprobarla, deberá examinar con detenimiento, si la clasificación asignada se ajusta a las normas fijadas.

La costumbre de clasificar excesivamente la información resta seriedad al sistema, disminuye la importancia del material clasificado, aumenta las medidas de guarda y control y limita la celeridad y el alcance de la difusión.

El aumento o disminución de la clasificación se llevará a cabo mediante una minuciosa apreciación. Todo cambio en la clasificación se ejecutará por una orden concreta del comandante o jefe, quien dejará constancia por escrito con intervención del oficial de inteligencia.

La información emanada de un comando superior no podrá ser reclasificada si no mediere una autorización expresa de dicho comando. Por razones de seguridad, a una información originada en un comando superior podrá aumentársele la clasificación, pero deberá informarse a dicho comando, a fin de ratificar o no el cambio.

7.012. Reclasificación. Consistirá en la modificación de la clasificación de seguridad originalmente asignada, en función de la disminución o acrecentamiento del valor de la información correspondiente.

La documentación recibida de una instancia superior solo podrá ser reclasificada a una categoría más restrictiva y nunca se le asignará una menor con la que fue recibida. La prerrogativa de asignarle menor categoría siempre será retenida por la instancia que generó dicho documento.

Toda la documentación deberá ser revisada en forma periódica a efectos de su reclasificación, con el objeto de evitar una sobrecarga del sistema de guarda y custodia de documentación.

En caso que durante la revisión de una documentación, se decidiera que su clasificación ya excede la necesaria, ya sea por el paso del tiempo u otra circunstancia y haya sido recepcionada de una instancia superior, se consultará por la necesidad de su reclasificación de la misma a una menor categoría. Sólo luego de haber recibido constancia escrita de la autorización para una reclasificación a menor categoría, se procederá a llevarla a cabo.

La reclasificación descendente (menor clasificación) es determinada por la autoridad de clasificación original.

La reclasificación ascendente (mayor clasificación) podrá ser ejecutada por cualquier autoridad respecto de sus elementos dependientes, mientras que para la proveniente de otras instancias deberá recurrir a la autoridad que impuso la clasificación original.

Para efectuar la reclasificación se procederá a cruzar, con tinta de color rojo, el sello modificado y a su derecha se colocará la nueva clasificación. Se dejará constancia al final del texto del documento se deberá colocar la siguiente leyenda:

MODIFICACIÓN DE LA CLASIFICACIÓN DE SEGURIDAD A: (colocar la nueva clasificación).

POR ORDEN DE: (autoridad que lo ordena)

GFH: (fecha)

EJECUTADO POR: (quien ha intervenido en la tarea) **HABIÉNDOSE ORDENADO LA MODIFICACIÓN EN TODOS LOS EJEMPLARES DEL PRESENTE DOCUMENTO DE ACUERDO CON EL DISTRIBUIDOR."**

En soportes del tipo digital, se anulará la clasificación anterior, se regrabará con la nueva clasificación y se dejará debida constancia.

Una vez concretadas las medidas indicadas para reclasificar el documento, se deberá dejar constancia del enterado de cada organismo o individuo que haya tenido conocimiento de la información en el documento aludido.

Los documentos obtenidos de otros ministerios, organismos o que procedieren de países extranjeros deberán clasificarse con un carácter, por lo menos, igual o equivalente al de su clasificación de origen.

7.013. Elaboración y tramitación. La elaboración de la documentación y su posterior tramitación deberán responder a una serie de formalidades que contribuirán a su interpretación y fijarán, también, aspectos acerca de Medidas de Seguridad de Contrainteligencia que posibilitarán su protección y, en alguna medida, auxiliarán en la determinación de su autenticidad.

Los aspectos formales para su elaboración deberán responder a las prescripciones doctrinarias establecidas en los reglamentos "Documentación" (RFP-70-05), "Escritura en Campaña" (RFD-99-02), "Inteligencia Táctica" (ROD-11-01), "Servicio Interno y en Guarnición" (RFP 70-01) y directivas particulares que pudieran surgir y que contribuyan a su interpretación y protección.

Entre las medidas de seguridad de contrainteligencia que se considerarán durante la elaboración de los documentos y su tramitación, es fundamental determinar taxativamente quiénes han participado en elaboración y quiénes han tomado conocimiento, así como otras inscripciones, marcas o rotulado de la información documentada (cualquiera sea su soporte), por saber:

a. Determinación del personal interviniente en su confección y tramitación.

De acuerdo con la naturaleza del contenido del documento, éste será tratado personalmente por la autoridad que le diere origen al mismo o el personal auxiliar especialmente autorizado; en todos los casos, se dejará constancia del personal que intervino en su tratamiento. Aspectos que deberá tenerse en cuenta:

- 1) A fin de identificar a todas aquellas personas que tramitaren documentación, será establecido en cada elemento de la Fuerza, mediante números arábigos, un código de guarismos. Su asignación y control serán registrados en forma correlativo en un libro que se denominará CÓDIGO DE GUARISMOS, que confeccionarán las divisiones centrales, centros de mensajes, etc., según el elemento de que se tratare o la situación, en que se encontrare.
- 2) El código se iniciará con el denominador que, a juicio del elemento, se creyere más conveniente de acuerdo con la cantidad de personal; este se consignará en el acta de apertura del libro.
- 3) La rúbrica y la cifra asignadas serán aplicadas en el sello "Interviene ". Toda rúbrica deberá ser acompañada por el número de codificación.
- 4) Cuando por razones de movimiento de personal un número quedare libre, este no podrá asignarse a un nuevo personal hasta que hubiere transcurrido un MÍNIMO DE UN AÑO.
- 5) En todas las hojas y carillas escritas de un documento se colocará, en el centro y en la parte superior e inferior, la leyenda con la clasificación de seguridad correspondiente.
- 6) Los documentos de alta clasificación (Confidencial, Secreto y Estrictamente Secreto y Confidencial) llevarán inscripta, a la derecha de la clasificación de seguridad, la identificación del documento en cada página subsiguiente a la primera. Esta se regirá de acuerdo con las normas en vigencia. Ejemplo de la segunda página de un documento: SECRETO (AEB 088).
- 7) También podrá utilizarse un sistema de números perforados en todas las páginas del documento impreso gráficamente, sello o inscripción.
- 8) Los diferentes dispositivos de almacenamiento, tanto analógico como digital, deberán llevar las inscripciones acerca de la clasificación de seguridad en el soporte físico y en los documentos que contienen.

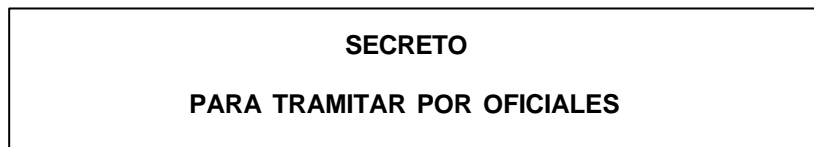
b. Dejar especificado cuando un documento deberá ser tramitado.

c. Determinar el tiempo de conservación de esa información.

d. Completar la clasificación existente con las siguientes indicaciones:

- 1) Para tramitar por el jefe del organismo.
- 2) Para tramitar por el Jefe de Inteligencia (G-2/S-2).
- 3) Difundir hasta jefes de subunidad, etc.
- 4) Para "Tramitar por Oficiales", etc.

La leyenda correspondiente se colocará debajo de la clasificación de seguridad, en la parte superior y con preeminencia a toda otra indicación.



- e. Foliación. Cada foja llevará en la parte inferior y sobre la clasificación de seguridad la leyenda Pág 1-5 o 3-6, según correspondiere, de acuerdo con la cantidad de fojas del documento.
- f. Rúbrica. Todos los documentos de alta clasificación de seguridad impresos serán rubricados, de puño y letra, por el emisor responsable o por la persona que hubiere intervenido y controlado su confección (G-2, G-3, etc). La rúbrica irá colocada a 2 cm a la derecha de la clasificación de seguridad, que se halla en la parte superior central de cada foja.
- g. Ensobrado e inscripciones particulares.

De acuerdo con lo establecido en la doctrina vigente respecto a las formalidades por tener en cuenta para ensobrar y rotular la información documentada, se deberá considerar que en aquellos documentos con alta clasificación de seguridad (Confidencial, Secreto y Estrictamente Secreto y Confidencial) deberán adicionarse otras medidas:

- 1) Se utilizará doble sobre. En el sobre interior en que se encontrare el documento, en su parte externa, figurará el código, número. Su cierre será cruzado con la firma del jefe remitente y los bordes de la tapa del sobre se asegurarán con cinta adhesiva transparente. En el sobre externo, se colocará: Código, número que corresponda, fojas y adjuntos, si los hubiere, y su correspondiente destinatario.

En caso de que la documentación a remitir fuere muy voluminosa, se acondicionará como encomienda que se deberán adoptar las mismas medidas señaladas precedentemente.

- 2) La documentación de carácter RESERVADO y PÚBLICO se utilizará con sobre único, no transparente, con las leyendas y sellos establecidos en el reglamento de Servicio Interno y en Guarnición (RFP 70-01).

7.014. Determinación del distribuidor. El distribuidor debe ser preparado teniendo en cuenta que solo aquellos organismos o personas con necesidad de tomar conocimiento deben ser incluidos en él. Un exceso de destinatarios/corresponsales sólo pondrá en riesgo su confidencialidad.

7.015. Reproducción. En relación con la documentación de carácter ~~ESTRICTAMENTE SECRETO~~ Y CONFIDENCIAL, SECRETO y CONFIDENCIAL, estará prohibida su reproducción, tanto por parte de las personas que tomaren conocimiento de esta, como por parte de los elementos destinatarios.

El extracto o síntesis de un documento que hubiere sido autorizado a confeccionarse, para ser guardado como antecedente a los fines de consulta, deberá ser redactado de manera tal que el texto no vulnere el grado de clasificación originario. Todo elemento que, por razones de trabajo, necesitare un extracto o síntesis de un documento secreto deberá solicitárselo a la autoridad que lo originó del mismo. Igual criterio se adoptará con respecto a copias parciales o totales de un documento.

Los órganos de dirección de Inteligencia y las unidades de Inteligencia, cuando mediare un cambio de clasificación de seguridad de SECRETO a Estrictamente Secreto Y CONFIDENCIAL y a los fines de su proceso y difusión, podrán reproducir el documento, en la medida que correspondiere, poniendo bajo estricto contralor las copias que se produjeren.

En cuanto a la documentación de carácter RESERVADO, el comandante, el jefe o el oficial designado por este serán las únicas autoridades que podrán autorizar la reproducción de documentos de ese carácter, se deberá controlar la cantidad de copias efectuadas.

7.016. Registro. La documentación clasificada se registrará en inventarios separados conforme a la clasificación de seguridad asignada al documento. Dichos inventarios se clasificarán "RESERVADO" salvo los de material criptográfico, que tendrán un tratamiento particular (ver Material Criptográfico).

Los inventarios y otros registros transitorios impondrán el asiento claro de la identificación del traslado de responsabilidad, con constancia de la fecha de entrega, procedencia, destino, trámites realizados y personas que tomaron conocimiento, tal como se establece en el reglamento "Servicio h-terno y en Guarnición" (RFP-70-01).

Los registros deberán mantenerse actualizados, a fin de contribuir, en cualquier oportunidad, a determinar el tránsito de determinado documento, con explícita identificación de intervinientes y oportunidades de disponibilidad de acceso de cada uno de ellos.

7.017. Usuario de documentación clasificada. El usuario es aquel personal que, en cumplimiento de una misión o función, accede a la información clasificada conforme a la "Necesidad de Saber", cumpliendo los requisitos establecidos para tal situación en lo referido a protección, normas de su proceso y reserva de su contenido.

7.018. Archivo, custodia y guarda. Se deben tener en cuenta las características de las instalaciones, locales, muebles y soportes destinados a tal efecto para poder definir las medidas de seguridad de Contrainteligencia que se aplicarán. Los locales deben garantizar la inviolabilidad a acciones simples de intrusión y el impedimento o demora controlada (tardanza y alerta) frente a la acción con intervención de ayuda tecnológica.

Conviene resaltar que debe incluirse en la idea de neutralización del acceso y eventual penetración evitar la posibilidad de escucha externa (aberturas de materiales sin capacidad de absorción de sonidos, tabiques delgados, techos sin aislamiento, ductos, etc.) que facilite tomar conocimiento de conversaciones (interpersonales y/o telefónicas) efectuadas en el interior de los locales, sin la necesidad de encontrarse dentro del mismo.

Todo comandante, director o jefe de una organización militar será responsable de mantener a resguardo toda aquella información que estime esencial para poder continuar con las misiones y funciones asignadas. Especialmente, contemplará aquellos casos en que la información principal pudiera ser destruida por acción de agentes externos, internos o por accidente.

a. Archivo de información clasificada documentada.

El archivo de la información documentada clasificada consiste en su almacenamiento en condiciones de preservación del acceso indebido y rápida recuperación para su uso.

Conlleva no sólo la consideración de locales y mobiliario de seguridad (cajas fuertes, armarios de seguridad, etc.) sino también de los soportes que la contienen (tipo de papel, informáticos, etc.) a fin de mantener su aptitud de uso.

Toda información clasificada documentada, independientemente del soporte, debe ser preservada en armarios de seguridad en locales seguros.

La información documentada con alta clasificación de seguridad se preservará en cajas de seguridad.

Las cajas y armarios de seguridad deberán poseer registro de llaves y combinaciones con indicación de quiénes son sus tenedores, con la aceptación explícita de dicha responsabilidad.

b. Custodia de información clasificada documentada.

La información clasificada, durante su vida útil (elaboración – destrucción), en todo momento se mantendrá bajo la tutela de un responsable, el que podrá variar pero no dejar de tener existencia concreta.

Esto deberá ser especialmente fluido durante el proceso de elaboración y difusión de la información clasificada. Cuando la tenencia de este tipo de información apunte a lapsos prolongados, el responsable de la custodia (documentación en tránsito) se transformará en depositario de la misma.

c. Guarda de la información documentada.

La guarda de la información documentada se podrá realizar sobre la base de cualquier soporte una vez que ésta ha dejado de tener valor actual, pero sea necesario su conservación.

La información documentada podrá mantener el grado de clasificación de seguridad que se le asignara, pero se deberá tener especialmente en cuenta que es importante que los lugares que se asignen para su guarda cumplan con los requisitos aprobados.

Los períodos podrán variar pudiendo algunos documentos deberse guardar a perpetuidad, u otros por cortos, medianos y largas plazos.

7.019. Entrega y recepción de la información documentada

a. Entrega y acuse recibo. Para toda aquella documentación que correspondiere, según normas vigentes, deberá acusarse recibo.

El acuse recibo será tramitado como documento público, para lo cual, en el mismo, no se hará mención del objeto del documento, sino únicamente de su clave de identificación Reglamento de Escritura en Campaña o de su codificación (identificación del expediente).

Su recepción, por parte de la Unidad remitente de un documento clasificado, constituirá una permanente tarea de fiscalización, a fin de comprobar que la misma, ha seguido el curso establecido.

La documentación de carácter RESERVADO y PÚBLICO será entregada a las autoridades indicadas en el inciso anterior.

b. Recepción.

Documentación de carácter Estrictamente Secreto y Confidencial, Secreto y Confidencial. Será recibida y abierta únicamente por el destinatario, quien lo registrará, controlará y tendrá bajo su custodia o por personal superior, designado a tal efecto.

Documentación de carácter Reservado y Público. Será abierta en la mesa de entrada, despacho y dependencias. Este cargo deberá ser desempeñado por personal militar, quien será responsable de su registro, contralor y custodia. En ningún caso, deberá ser tramitada por soldados.

La documentación recibida fuera del horario de actividades se mantendrá en custodia en el Servicio de Vigilancia del elemento, hasta tanto pudieren cumplimentarse las normas establecidas precedentemente.

7.020. Control de entrada y salida de documentación

a. Mesa de Entrada y Salida (MES).

Todos los organismos designarán en sus mesas de entrada y salida, centros de mensajes, etc., personal que desarrollará particularmente y en forma adecuada a las características del lugar y la información en trámite, las siguientes tareas:

- 1) Control de las modificaciones de clasificación.
- 2) Verificación de cargos.
- 3) Recepción de acuse recibo.
- 4) Destrucción de documentos y redacción de las actas respectivas.
- 5) Inventarios de documentación.

b. Salida de documentación.

Todo el personal del elemento o ajeno al mismo, civil o militar, que debiere salir de la instalación con documentación, transportada por distintos medios y formas (portafolios, paquetes, cajones, etc.), deberá contar con la autorización de salida de asuntos clasificados, por escrito, extendida por el oficial de inteligencia o jefe del elemento. Esta autorización deberá ser entregada en la

Guardia de Prevención, a fin de efectuar el contralor correspondiente, sin cuyo requisito no se permitirá la salida.

El detalle de aplicación de estas medidas estará contenido en los PON(s) del elemento u organismo.

c. Entrada de documentación.

Cuando ingresare documentación clasificada en las condiciones ya establecidas, la persona responsable que la condujere deberá, a su salida del elemento, entregar en la Guardia el Recibo de Entrega y Recepción de Información y Material Clasificado (Anexo 9).

Al término del turno de guardia, las tarjetas y certificados serán entregados al Oficial de Inteligencia o a la jefatura del elemento, si así correspondiere.

7.021. Transmisión de la información. La transmisión de la información podrá hacerse por medio de las distintas facilidades de comunicaciones y las medidas de seguridad que deben aplicarse se incluyen el capítulo “Medidas de Seguridad de Contrainteligencia referidas a las Comunicaciones”.

7.022. Destrucción de documentación clasificada. La destrucción de información documentada, independientemente del medio soporte responderá a determinadas situaciones y necesidades:

- a. La información que hubiere cumplido con su propósito y no fuere necesario mantenerla.
- b. La situación táctica imponga la destrucción de emergencia.
- c. La destrucción parcial involuntaria que inutilice el documento y deba completarse su destrucción.

Los documentos clasificados, sin distinción del tipo de soporte de registro, que deban ser destruidos, lo serán bajo el control del personal responsable o autoridad designada, en cumplimiento de una orden superior o por determinación de la autoridad de origen (Anexo 10). En cada caso se labrará el acta correspondiente (Anexo 10 – Agregado 01).

Los métodos adecuados para la destrucción serán:

- a. Destrucción mecánica mediante trozadores diseñados para ello, conforme a la naturaleza del soporte.
- b. Incineración controlada con pulverización de residuos.
- c. Destrucción de contenidos en soportes magnéticos, por campo eléctrico que afecte la orientación de partículas.
- d. Destrucción por medios químicos.
- e. Destrucción de contenidos en medios informáticos no descartables, a través de software de eliminación. Esta acción no debe considerarse eficiente en ninguna oportunidad, razón por la cual, los medios informáticos no descartables utilizados para la gestión de información clasificada, aún después de haberse eliminado su contenido deberá considerarse como material clasificado, y destruirse físicamente mas allá de su recuperación de considerarse obsoleto.

Ante la eventualidad de que una situación determinada obligue a destruir la información documentada para evitar que sea obtenida por el enemigo en caso de una acción bélica o sea dañada o extrañada en caso de catástrofes o acciones intencionadas, se deberá contar con planes y recursos materiales que posibiliten la eliminación de la misma.

En cualquiera de los casos debe constatarse que la destrucción de la documentación clasificada sea total y no se posibilite, bajo ningún medio, la reconstrucción total o parcial de la misma.

En ningún caso, la documentación a destruir, podrá estar bajo la custodia de soldados, si no se encontrare presente personal de los cuadros responsable de la misma. TODA TRANSGRESION A LA PRESENTE PRESCRIPCION SERA CONSIDERADA DELITO O FALTA GRAVE, según correspondiere al tipo de documentación.

Cuando se destruyere material de alta clasificación de seguridad o RESERVADO, se dejará constancia por medio de una planilla, que se archivará en la dependencia responsable del documento destruido (Anexo 10).

Estará TERMINANTEMENTE PROHIBIDA, la venta de papel utilizado en documentos, cualquiera fuera su carácter, estado o vigencia. Dicha venta **sólo será permitida, si previamente el papel fue-re sometido al proceso de trituración, u otros procesos destinados a tal efecto.** Se exceptuarán las revistas, folletos y otras publicaciones de carácter PÚBLICO, siempre que su contenido no afectare las normas de seguridad.

7.023. Evacuación de la información documentada. En algunos casos, será necesario llevar a cabo la evacuación de aquellos soportes con información documentada (papel, digital, Etc), en estos casos, es imprescindible contar con planes que aseguren la evacuación evitando su destrucción e impidiendo su diseminación indebida.

Es importante considerar que cualquier evacuación, por la misma situación, será una actividad donde la sucesión de acciones y el desorden pondrán en riesgo la información; en estos casos, se deberá considerar la posibilidad de la destrucción antes que la pérdida o el riesgo de que se conozca en forma indebida. Esto también posibilitará prestar mayor atención y cuidado a aquella información que resulte prioritaria.

7.024. Responsabilidades en el control de la información. La responsabilidad, para determinar el acceso a la información, corresponderá al comandante, director o jefe, con el asesoramiento del Oficial de Inteligencia y del responsable de la posesión de determinada información y no de quien hubiere de recibirla. Esta responsabilidad no eximirá a quien solicitare o recibiere el conocimiento correspondiente, de la obligación de hacer conocer su "NECESIDAD DE SABER", antes de recibir dicha información. El término "quien solicitare", podrá referirse a una persona, organismo, entidad, Fuerza, etc.

No se podrá difundir información clasificada sin la autorización expresa del comando o jefatura que la poseyere o la hubiere originado.

La difusión de información a la prensa estará taxativamente regulada por las órdenes que se impartan al respecto.

La información clasificada deberá ser tratada dentro del lugar destinado al trabajo y su uso estará restringido, sujeto a autorización de trato, por el superior responsable y EN NINGUN CASO PODRA SER SACADA DEL LUGAR DE UBICACION NORMAL, salvo que fuera pública y debidamente autorizada. Estará prohibido que personal que tuviere acceso a la información, guarde parte o la totalidad de la misma, en archivos particulares.

Responsabilidad del comandante, director o jefe:

- a. El comandante, director o jefe, será el responsable, dentro de su jurisdicción, de que se mantenga un constante control de la información contenida en los documentos, el material, las instalaciones, los sistemas de comunicaciones o las personas a sus órdenes o bajo su responsabilidad.
- b. El control incluirá la producción de la información clasificada, su divulgación, difusión y custodia.
- c. La responsabilidad primaria, que es del comandante o jefe, será compartida por la persona que estuviere en situación física de controlarla personalmente.
- d. No sólo será responsable quien la tuviere bajo su custodia directa, sino todo aquel que, sin tenerla, tomare conocimiento de la información, observare que se estuvieren violando normas de seguridad dictadas, etc., y no adoptare las medidas necesarias para evitar la difusión no conveniente de la misma.

Responsabilidad del jefe u oficial de inteligencia.

- a. Asesorará al comandante, director o jefe en todo lo atinente a la protección de la información.
- b. Propondrá quienes podrán tratar la información existente.
- c. Creará un sistema de control, para que todas las personas que tuvieran acceso a la información clasificada, estuvieren debidamente adiestradas y autorizadas para ello, de lo que se dejará constancia en un registro.
- d. Actualizará los estudios de seguridad y programas de inspecciones de seguridad, relacionados con el control de la información.

- e. Ejecutará toda otra tarea necesaria, que contribuyere a la protección de la información.
- f. Llevará una lista de la totalidad del personal con conocimientos de documentos con alta clasificación de seguridad.

7.025. Transgresiones a las normas de seguridad. Todo integrante de la Fuerza, que tuviere conocimiento de la difusión o posibilidad de difusión de información clasificada, a cualquier persona no autorizada o de uso inadecuado, informará de inmediato a su superior jerárquico, quien a su vez informará, en primer lugar, al responsable de su custodia y luego al comandante, director o jefe, con intervención del oficial de inteligencia del elemento.

Cuando la información comprometida, pudiere poner en peligro la seguridad de la Fuerza o de la Nación, será puesto de inmediato en conocimiento del comando, dirección o jefatura, de quien dependiere el elemento.

Deberá recalcarse que la violación de las normas de seguridad establecidas tiene como consecuencia la substanciación de las actuaciones correspondientes y la aplicación no sólo de las sanciones militares, sino también las penalidades contenidas en el Código Penal, en los artículos referentes a la materia.

Una vez sospechada o detectada la violación de las medidas de seguridad, se procederá, de inmediato, a efectuar la investigación correspondiente, a fin de deslindar responsabilidades, determinar cuales fueron las medidas vulneradas, extraer experiencias y rever los procedimientos con el objeto de aplicar medidas correctivas a las normas.

SECCIÓN III

MEDIDAS DE SEGURIDAD REFERIDAS AL MATERIAL

7.026. Consideraciones básicas. Las medidas de seguridad de contrainteligencia referidas al material, se regirán por conceptos similares a los expresados para la información documentada. El jefe del elemento será el responsable de la protección de la información contenida en el material, además de la custodia y cuidado del mismo.

7.027. Material clasificado. Es cualquier elemento, equipo, parte, conjunto, pieza, programa, desarrollo, sistema o similar, fabricado o en proceso de fabricación, por cuyas características técnicas, importancia o información contenida, requiera ser restringido a la difusión, independientemente si el mismo se encuentra o no en servicio.

7.028. Criterios de clasificación de material clasificado. Se basarán en los alcances del Secreto Militar y se empleará la clasificación utilizada para los documentos.

7.029. Criterio de responsabilidad del material clasificado. Con las adaptaciones surgidas de la naturaleza de los objetos que se trate, son aplicables las responsabilidades expresadas para los documentos.

7.030. Responsabilidades sobre material clasificado

- a. Todo el personal es responsable de la seguridad de la información contenida en materiales clasificados en cuya gestión intervenga.
- b. Los Comandantes/Jefes de elementos entenderán no sólo en la adopción de adecuadas medidas de seguridad de Contrainteligencia en relación con el material clasificado, sino también en la ejecución de una permanente fiscalización.

7.031. Seguridad del material criptográfico. Se desarrolla en el capítulo correspondiente a las Medidas de Seguridad de Contrainteligencia referidas a Criptografía del presente reglamento; a publicación "Normas y Procedimientos Criptográficos para la Acción Militar Conjunta" (PC 26-12) y las órdenes, directivas y PON(s) desarrollados a tal efecto.

7.032. Transporte y guarda del material. Todo material contiene información y, en tal sentido será de acuerdo con el grado de riesgo, que se derivare de una inadecuada difusión de los datos, que pudieren emanar del mismo.

Desde el punto de vista de la seguridad de contrainteligencia, la protección se concretará, mediante medidas de carácter específico y otras de carácter general, relacionadas con la educación del personal y con medidas de seguridad de tipo operacional.

Los aspectos operacionales estarán relacionados con la guarda, uso y transporte y con las medidas de seguridad de orden general, que deberá adoptarse y que se encuentran desarrollados en las distintas prescripciones reglamentarias del campo de la logística. La entrega de material clasificado deberá registrarse, mediante el recibo que se especifica en el Anexo 9.

En cuanto a medidas específicas de seguridad de Contrainteligencia, regirá todos aquellos aspectos pertinentes, contenidos en el presente capítulo, adaptados a la situación que se viviere y considerando que siempre debe preverse, la existencia de una amenaza del enemigo.

7.033. Transgresiones a las normas de seguridad. Todo integrante de la Fuerza, que tuviere conocimiento de la difusión o posibilidad de difusión de información clasificada, de parte de cualquier persona no autorizada o de uso inadecuado, informará de inmediato a su superior jerárquico, quien a su vez informará, en primer lugar, al responsable de su custodia y luego al comandante, director o jefe, con intervención del oficial de Inteligencia del elemento.

Cuando la información comprometida, pudiere poner en peligro la seguridad de la Fuerza o de la Nación, será puesto de inmediato en conocimiento del comando, dirección o jefatura, de quien dependiere el elemento.

Deberá recalcarse que la violación de las normas de seguridad establecidas tiene como consecuencia la substanciación de las actuaciones correspondientes y la aplicación de las medidas disciplinarias que contempla el Código de Disciplina de las Fuerzas Armadas, sino también las penalidades contenidas en el Código Penal, en los artículos referentes a la materia.

Una vez sospechada o detectada la violación de las medidas de seguridad, se procederá, de inmediato, a efectuar la investigación correspondiente, a fin de deslindar responsabilidades, determinar cuales fueron las medidas vulneradas, extraer experiencias y rever los procedimientos con el objeto de aplicar medidas correctivas a las normas.

CAPÍTULO VIII

MEDIDAS DE SEGURIDAD REFERIDAS A LAS COMUNICACIONES

SECCIÓN I

CONCEPTOS GENERALES

8.001. Definición. Las medidas de seguridad referidas a las comunicaciones son el conjunto de normas, procedimientos y características de diseño de los equipos destinados a neutralizar y/o reducir la efectividad de las actividades de los sistemas de Inteligencia del enemigo real o potencial sobre las transmisiones de interés para la fuerza, así como asegurar la operación efectiva y permanente de los sistemas propios.

8.002. Consideraciones básicas. Para alcanzar con éxito el logro de lo expresado anteriormente, se deberán tener en cuenta los siguientes aspectos:

- a. Protección de las transmisiones. Se tendrá en cuenta lo expresado en el reglamento "Conducción de Comunicaciones" (ROD-05-01), Capítulo XIV, Sección III, Artículo 14.011, a. b.
- b. Protección criptográfica de la información. Se tendrá en cuenta lo expresado en el reglamento "Conducción de Comunicaciones" (ROD-05-01), Capítulo XIV, Sección III, Artículo 14.011, c.
- c. Seguridad de la información transmitida o transportada por estafetas. Para los casos en que la transmisión de la información sea ejecutada a través de estafetas, se deberán arbitrar las medidas de seguridad correspondientes para negar o disminuir las posibilidades de su interceptación por parte del oponente real o potencial.

El estafeta podrá transportar la información documentada o material clasificado bajo un soporte cualquiera o él mismo será el portador de ese conocimiento. Dicha protección deberá ser continua desde el punto de partida del mensaje hasta su recepción por parte del o los interesado/s.

Durante la ejecución de esta actividad, el secreto acerca del recorrido, el personal, las medidas de seguridad física previstas, la adopción de medidas de engaño y todo otro dato que pudiere resultar de interés durante el planeamiento serán de suma importancia para limitar las posibilidades de interceptación por parte del enemigo.

Se deberán impartir órdenes claras y precisas respecto del proceder ante una eventual interceptación por parte del enemigo u oponente, a los fines de evitar su captura, así como planes de alternativa que flexibilicen el accionar del personal implicado, ante la presencia de algún inconveniente que afecte el cumplimiento de la misión.

- d. Seguridad de las instalaciones. Constituyen el conjunto de medidas, procedimientos y normas destinadas a la preservación de las instalaciones empleadas para el normal funcionamiento de los sistemas de comunicaciones en toda oportunidad, independientemente de las actividades del enemigo real o potencial, quien buscará limitar/neutralizar su eficiencia mediante la afectación de estas.

8.003. Factores que influyen en la seguridad de las comunicaciones. La transmisión de información clasificada constituye un momento crítico en la gestión de los documentos que la contienen, por cuanto en esa oportunidad se incrementan las posibilidades de su interceptación por parte de actores no deseados.

Todo el personal deberá tener presente, como premisa, que las comunicaciones podrán ser interceptables cualquiera fuere el enlace que se utilice. Tal situación impone para la transmisión de asuntos clasificados la necesidad del empleo de criptosistemas aptos, correctamente aplicados.

La participación tecnológica en las comunicaciones impone la conciencia de afrontar la responsabilidad de utilizar un sistema en el que concurren diversos elementos materiales y personal para alcanzar la finalidad de transmitir información. Por esta razón se desagregará el proceso de comunicación para determinar con mayor exactitud las responsabilidades de protección de la información de acuerdo con la naturaleza de la participación en el sistema.

La seguridad de las comunicaciones es una acción propia del campo de Inteligencia, por cuanto el elemento por proteger es información clasificada, donde convergen la responsabilidad técnica de los sistemas de comunicaciones, que proporcionan el medio adecuado para concretar la transmisión de la información, y la propia de los usuarios de este. Es por ello que no puede concebirse a las medidas de seguridad para alcanzar esta protección buscada sin la adecuada interacción de los factores participantes.

8.004. Conceptos asociados por tener en cuenta. La relación entre la seguridad y las comunicaciones, exige precisar conceptos rectores que determinen una integración armónica y coordinada entre ambas, a fin de alcanzar un óptimo grado de eficiencia en el conjunto.

a. Seguridad de las comunicaciones.

Protección resultante de todas las medidas destinadas a negar al oponente la información de valor que pueda ser extraída de la interceptación, escucha y análisis de las comunicaciones.

b. Seguridad en las comunicaciones.

Medidas y controles para denegar el acceso a través de las redes a entidades no autorizadas, así como para garantizar la autenticidad de las partes en comunicación.

c. Seguridad criptográfica.

Componente de la seguridad de las comunicaciones que, mediante la provisión de sistemas criptográficos eficientes y su adecuada utilización, confiere resistencia al descryptamiento a las comunicaciones cifradas propias.

d. Seguridad de transmisión.

Componente de la seguridad de las comunicaciones que deriva de la elección de los medios y métodos de comunicaciones que mejor respondan al propósito de impedir la interceptación del tráfico propio y su posterior análisis. Se materializa en la habilitación de las diferentes facilidades de comunicaciones para los niveles de clasificación de la información que ellas transmitirán.

La información clasificada solo podrá ser transmitida por los sistemas habilitados de acuerdo con la clasificación de seguridad para la que se encuentren habilitados. Dicha habilitación será determinada por el sistema de Inteligencia a la que pertenece la organización militar que se trate.

8.005. Responsabilidades y misiones. El comandante, director o jefe será el único responsable en lo que a la seguridad de las comunicaciones de los elementos bajo su mando se refiere; podrá delegar su autoridad en el grado que considere necesario y conveniente (ROD-00-01, Cap. I, Sec. I, Art. 1.002).

En función de lo expresado precedentemente, el comandante, director o jefe, basado en las ordenes vigentes del escalón superior, determinará los detalles que se tendrán en cuenta para ser observados con la finalidad de preservar y aumentar la seguridad del sistema de comunicaciones del elemento bajo su mando. Las previsiones que deberá observar para el cumplimiento de su misión serán:

- a. Confección del apartado correspondiente a las medidas de seguridad de las comunicaciones en las respectivas órdenes y procedimientos.
- b. Articulación de un sistema de control eficaz que permita el monitoreo constante de las comunicaciones de interés, así como del cumplimiento de las normas impuestas, incluyendo la ejecución de inspecciones sistemáticas y asistemáticas.
- c. Adopción de medidas correctivas que permitan, rápidamente, eliminar las violaciones a las normas impuestas así como las causas que las originasen.
- d. Establecimiento y comprobación de planes de emergencia que aseguren la destrucción efectiva de todos aquellos elementos que componen el sistema de comunicaciones (documentación, equipos, instalaciones), a los fines de evitar la obtención de información de interés por parte del enemigo.
- e. Considerar durante el planeamiento y ejecución de las operaciones (tanto en tiempo de paz o guerra) de todos aquellos aspectos de las medidas de seguridad de contrainteligencia necesarios, sobre los sistemas de comunicaciones, a fin de asegurar su adecuado y permanente funcionamiento.

- f. Formación, en todo el personal que le dependa, de una verdadera “conciencia de contrainteligencia”, mediante la educación continua, sistemática y asistemáticamente.

Asimismo, el comandante o jefe contará con el asesoramiento de los oficiales de inteligencia y de comunicaciones, los que a su vez, a través de la autoridad delegada, ejercerán la supervisión y control sobre el sistema de comunicaciones propio, a los fines de asegurar su operación en forma permanente y disminuir los efectos del accionar del enemigo real o potencial.

8.006. Responsabilidades del oficial de inteligencia. El oficial de inteligencia orientará sus acciones a la obtención de información relacionada con las capacidades de guerra electrónica enemiga.

En forma subsidiaria, producirá inteligencia de contrainteligencia desde el punto de vista de los sistemas de comunicaciones y confeccionará los documentos de contrainteligencia pertinentes a las comunicaciones con el necesario asesoramiento del oficial de comunicaciones.

8.007. Responsabilidades del oficial de comunicaciones. Asesorará al comandante, director o jefe sobre aquellos aspectos referidos a las capacidades de guerra electrónica del oponente o enemigo real o potencial de interés.

- a. Proporcionará asistencia técnica al oficial de inteligencia respecto de los aspectos táctico-técnicos para la confección del perfil electromagnético (PEEM) de la unidad u organismo al cual apoye y acerca de cuáles serán las medidas de seguridad de contrainteligencia desde el punto de vista de comunicaciones, adecuadas para cada situación.
- b. Asesorará al oficial de inteligencia sobre las vulnerabilidades que presenten, desde el punto de vista de las MSCI, las instalaciones físicas de los sistemas de comunicaciones deberá efectuar una apreciación acerca del grado de afectación que podría provocar el accionar enemigo sobre su normal funcionamiento.
- c. Supervisión de la correcta ejecución de los planes CONEM y EVEM y de la implementación de las medidas correctivas necesarias.
- d. Educación e instrucción sobre las Medidas de Seguridad de Contrainteligencia respecto de comunicaciones.

SECCIÓN II

ESTUDIO DE SEGURIDAD DE COMUNICACIONES

8.008. Evaluación de las vulnerabilidades de los sistemas de comunicaciones. Una vulnerabilidad, desde el punto de vista de los sistemas de comunicaciones, está representada por la debilidad que este presenta y que, al resultar expuesta a un determinado grado de daño, ante un modo de acción específico por parte de un enemigo u oponente real o potencial, impide y/o dificulta su normal desempeño.

Para la correcta detección de las vulnerabilidades presentes en los sistemas de comunicaciones, se deberá contar con información relacionada con las capacidades del enemigo u oponente real o potencial, y de las debilidades propias en cuanto a las características de diseño en el sistema por evaluar (redes y facilidades de comunicaciones disponibles, redundancia de medios, capacidad de sus sistemas criptográficos, instrucción del personal, actividad en que se lo emplea y reserva de material entre otros aspectos).

Para el estudio y posterior determinación de las vulnerabilidades se deberá encarar el estudio de las vulnerabilidades desde los siguientes puntos de vista:

- a. Desde el punto de vista de las emisiones.

- 1) Determinación del perfil electromagnético (PEEM).

Se define como perfil electromagnético al conjunto de emisiones de comunicaciones y de no comunicaciones, asociadas a una organización y/o sistema de armas y sensores en particular, que permiten determinar su presencia, identificación, composición, localización, actividades que realizan y material empleado, entre otros aspectos.

La definición de los perfiles electromagnéticos deberán realizarse desde los períodos de paz y será la resultante de la explotación de todas las fuentes disponibles, a través de los distintos procedimientos de obtención a disposición del elemento encargado de su confección.

La finalidad de la determinación del PEEM será proporcionar las bases de estudio que permitan identificar las vulnerabilidades, desde el punto de vista de las emisiones (se deben considerar no solo los emisores radioeléctricos, sino también los grupos electrógenos y todo aquello que emite algún tipo de señal), que presentan los sistemas de comunicaciones propios, de interés y/o bajo control de la Fuerza.

Durante la confección del PEEM propio, a cargo del oficial de inteligencia, con el asesoramiento y asistencia de los oficiales de comunicaciones y operaciones, se tendrán en cuenta los patrones de emisión (tanto de comunicaciones como de no comunicaciones) del elemento desplegado para cada tipo de actividad que se ejecute, teniendo en cuenta su disposición en el terreno y los medios electrónicos asociados disponibles.

Para el desarrollo de los mencionados perfiles deben aprovecharse todas las ejercitaciones que realice el elemento, buscando que al momento del despliegue de los medios, sean empleados todos los emisores que le correspondan.

Es conveniente, y a los fines de facilitar su diseño y posterior estudio, definir los PEEM de medios de comunicaciones separados de los de No Comunicaciones.

Una vez desplegados los elementos en el terreno, el oficial de inteligencia registrará en la carta la disposición de los elementos junto con el sistema electrónico asociado, del cual se detallará (Anexo 11):

- a) Equipo de comunicaciones y no comunicaciones.
 - b) Rango de frecuencia de operación.
 - c) Tipo y modo de operación.
 - d) Potencia y modos de emisión.
 - e) Facilidades de comunicaciones instaladas.
- 2) A continuación, con el asesoramiento del oficial de comunicaciones, trazará los lóbulos de irradiación de todos los sistemas (Comunicaciones y No Comunicaciones), teniendo en cuenta los siguientes aspectos (Anexo 12):
- a) Irradiante empleado.
 - b) Potencia de emisión.
 - c) Tipo y modo de operación.

Se deberá tener en cuenta que el trazado de los lóbulos deberá ser realizado para cada tipo de irradiante y potencia de emisión empleada.

A su vez, al margen de cada calco de PEEM, se deberán consignar cuáles son las características del equipo empleado para la interceptación, escucha y radiolocalización, para el trazado del mencionado perfil.

Esta información será de suma importancia al momento de comparar las capacidades de guerra electrónica del enemigo.

- 3) Los datos por detallar del o los equipos receptores son los siguientes:
- a) Irradiante empleado y altura.
 - b) Distancia de interceptación/escucha/localización (respecto de cada emisor).
 - c) Relación señal/ruido.

Finalmente, superponiendo los distintos lóbulos de irradiación obtenidos, se trazará un límite que una los extremos de los lóbulos más extensos y visualizar así cuál es el límite de irradiación de la fracción/elemento en estudio, proporcionando elementos de juicio que permitan evaluar las posibilidades de acción enemiga (Anexo 13).

Finalizado esto, se podrán distinguir cuáles son los patrones de actividad electrónica de la organización en estudio según las actividades que realiza, permitiendo, de esta manera, detectar cuáles son aquellas emisiones distintivas que la diferencian de las otras.

Ejemplos:

- a) Ocupación de una zona de reunión: las emisiones radioeléctricas serán mínimas, en favor de las comunicaciones alámbricas, pero existirán emisiones de radares de vigilancia terrestre, en funciones de seguridad, así como enlaces en muy alta frecuencia.
- b) En la ejecución de un ataque, las emisiones en alta frecuencia y muy alta frecuencia serán de un volumen mayor y de una mayor cantidad de correspondientes en actividad.

Una vez establecido el PEEM específico, de acuerdo con la misión/actividad que realizará el elemento u organización, se lo someterá a las capacidades de guerra electrónica asignada al enemigo u oponente, buscando detectar aquellas debilidades que, al ser detectadas y atacadas, afecten el cumplimiento de la misión y faciliten la obtención de información de interés por parte de este.

El oficial de inteligencia asesorará desde el punto de vista de contrainteligencia, apoyado y asesorado por el oficial de comunicaciones, acerca de cuáles deberán ser las medidas que el elemento adoptará para negar y/o dificultar el accionar del enemigo u oponente, real o potencial.

b. Desde el punto de vista de la infraestructura.

Como fue expresado anteriormente, la seguridad de las instalaciones constituyen el conjunto de medidas, procedimientos y normas destinados a la preservación de toda estructura y/o edificación empleadas para el funcionamiento de los sistemas de comunicaciones y No comunicaciones, en todo momento, independientemente de las actividades del enemigo real o potencial, quien buscará limitar/neutralizar su eficiencia mediante la afectación de estas.

Todo comandante o jefe deberá contar con el asesoramiento del oficial de inteligencia y de comunicaciones para:

- 1) Ordenar la confección y puesta en vigencia de los planes de emergencia para la destrucción del material y documentos.
- 2) Controlar la protección de las instalaciones ante cualquier situación.
- 3) Informar y adoptar las medidas correspondientes en caso de producirse cualquier violación a la seguridad de las instalaciones.

Las medidas de seguridad relacionadas con la infraestructura afectada a los sistemas de comunicaciones serán:

1) En el asentamiento de paz:

- a) El local destinado al centro de comunicaciones deberá estar localizado (dentro del cuartel) en un lugar que permita canalizar/limitar el acceso del personal y proporcionar el mayor grado de aislamiento para que, en caso de ataque, le permita continuar operando, en forma autónoma respecto del exterior.

Asimismo, deberán contar con solo una puerta de acceso y ventanas de reducidas dimensiones, debidamente aseguradas, para evitar todo tipo de ingreso y limitar al máximo la observación desde el exterior hacia el interior.

- b) Deberá contar con los elementos necesarios de lucha contra el fuego como así también de las alarmas que se crean convenientes para asegurar la integridad edilicia.

2) En campaña:

- a) El centro o puesto de comunicaciones, deberá estar instalado (con todos sus medios) fuera de los límites del puesto de comando al cual apoya.
- b) Los irradiantes deberán ser instalados alejados de los equipos, previendo enmascarar adecuadamente las líneas de transmisión. Asimismo, en la medida de lo posible, se hará uso intensivo de irradiantes direccionales, a los fines de dificultar el accionar de la guerra electrónica enemiga.
- c) Los grupos electrógenos u otros sistemas de alimentación de respaldo deberán ser protegidos y estar suficientemente alejados de las instalaciones a las cuales apoyan, debiéndose prever siempre, que permita operar el centro/puesto de comunicaciones.
- d) Deberá contar con un servicio de protección perimetral, a los fines de proporcionar seguridad inmediata.

En función de lo expresado en los puntos 1) y 2), el Oficial de Inteligencia, asesorado por los Oficiales de Comunicaciones y Operaciones, determinará cuales son las falencias existentes en la infraestructura a considerar, como así también procederá a establecer el grado de limitación por cada acción que pueda ejecutar el enemigo u oponente sobre la infraestructura.

Ejemplo:

Daño	Limitación que produce	¿Se dispone de sistema de reemplazo?		Solución de alternativa/previsiones	Vulnerabilidad	Capacidad remanente
		SI	NO			
Dstrucción del grupo eléctrico	Suministro de energía eléctrica	X	--	Banco de baterías	Interrupción de servicio de comunicaciones satelital	3 Hs de operación solo Red Cdo interna y externa
Dstrucción de irradiantes AF	Enlace Elon Sup	X	--	Empleo de irradiantes omnidireccionales	Facilita MAE del enemigo	---
Dstrucción del Puesto de Comunicaciones	Comando, control y comunicaciones	--	X	Coordinación con elementos vecinos. Pedido al Elon Sup de material para reserva	Limitación en el comando y control de los elementos propios	---

SECCIÓN III

PROTECCIÓN DE LAS TRANSMISIONES

8.009. Definición. La protección de las transmisiones consistirá en la instrumentación y adopción de medidas de seguridad de contrainteligencia, destinadas a anular, neutralizar o por lo menos restringir, las actividades de inteligencia del enemigo sobre las transmisiones propias, mediante el uso de arbitrios técnicos.

8.010. Procedimientos para la protección de las transmisiones. Los aspectos referidos a la protección de las transmisiones están contenidos en el Reglamento Conducción de Comunicaciones (ROD-05-01). El empleo de aparatos telefónicos, exige procedimientos específicos y el empleo de codificadores, pues serán vulnerables a la interceptación.

Asimismo, todo aparato de uso militar deberá tener agregado, en lugar visible, la indicación de su grado de vulnerabilidad y en una tarjeta, las contramedidas a adoptar, en ese caso (Anexo 14).

En general y a los fines de la seguridad en las transmisiones, se tendrán en cuenta, los siguientes lineamientos generales:

- a. Empleo correcto de los medios: ello demandará una adecuada educación de los corresponsales y el establecimiento de una estricta disciplina de tráfico.
- b. Protección contra la intromisión: se logrará mediante el empleo de arbitrios técnicos, tales como inversores de voz y, básicamente, mediante la autenticación del personal que se comunica.
- c. Protección contra la escucha: se logrará mediante el uso de aquellos medios, que detentaren el mayor grado de discreción, en relación con el tipo de información a transmitir y con el tiempo disponible para su difusión.
- d. Protección contra el análisis de tráfico: se logrará mediante las medidas de protección criptográfica de la información.
- e. Protección de los medios técnicos: la seguridad de las transmisiones también se logrará, protegiendo los medios técnicos a utilizar; ello estará relacionado con medidas de seguridad tácticas, tales como disciplina del tráfico y retaceo de indicios técnicos (potencias, frecuencias, Etc).
- f. Discreción en el uso de los medios alámbricos: el logro de esta previsión se obtendrá con el mínimo y más discreto intercambio informativo, a través del uso del teléfono.

Lo expresado precedentemente, se implementará mediante un estricto control, en el acceso a la información transmitida por parte del personal no corresponsal, sin "necesidad de saber".

CAPÍTULO IX

MEDIDAS DE SEGURIDAD REFERIDAS A LA CRIPTOLOGÍA

SECCIÓN I

CONCEPTOS GENERALES

9.001. Definición. Las medidas de seguridad referidas a la criptología son el conjunto de normas y procedimientos destinados a negar o neutralizar el accionar del enemigo u oponente sobre la información o el material relacionado con la criptología.

9.002. Glosario de términos

Criptología: ciencia que estudia y establece los métodos, para cifrar la información y los procedimientos para el descryptamiento, con la finalidad de proteger la propia información y facilitar la reunión de aquella, relativa a un oponente real o potencial.

Criptosistemas: conjunto de elementos, reglas y principios criptológicos relacionados entre sí, para posibilitar la seguridad de las comunicaciones.

Material criptográfico: claves, códigos, equipos criptográficos, directivas, inventarios y toda otra documentación, relacionada con la criptografía.

Clave: convención variable de carácter SECRETO, que hace posible la utilización de un método criptológico.

Cifrar: operación que consiste en procesar información en claro con un criptosistema, para obtener un cifrado (información ininteligible).

Descifrar: operación que consiste en procesar un cifrado, con un criptosistema, para obtener un texto en claro.

Descriptar: traducir al lenguaje claro, un texto cifrado, desconociendo total o parcialmente, la clave utilizada.

9.003. Consideraciones básicas. Las claves en vigencia no deben estar referenciadas en los planes u órdenes de operaciones. Cuando fuere menester aludirlas en relación con éstos documentos, se hará en sobre cerrado bajo estrictas medidas de seguridad.

El acceso, posesión o conocimiento del material y/o documentación criptográfica únicamente está permitida al personal cuyas funciones requieren tener a cargo dicho material y/u operarlo, los que deberán contar con la respectiva acreditación para la gestión de información clasificada.

Ningún integrante de la Fuerza podrá justificar exclusivamente sobre la jerarquía que ostenta, el tener acceso libre al material o a las actividades criptográficas. En caso de plantearse una situación de tal tipo el responsable de la tenencia o uso del material criptográfico dejará constancia en un acta sobre la oportunidad y el motivo que ha dado origen a la trasgresión, remitiendo el original al organismo superior de Inteligencia a sus efectos.

9.004. Capacidades atribuibles al enemigo u oponente. Cuando se manipula documentación y equipos criptográficos, debe considerarse la aptitud del enemigo u oponente para ejecutar las siguientes acciones:

- a. Acceder por interceptación a la totalidad del tráfico propio.
- b. Acceder mediante criptoanálisis a los contenidos transmitidos.
- c. Presentar un nivel de criptoanálisis superior al propio.
- d. Obrar como un corresponsal subrepticio del criptosistema a partir de obtener las claves en uso.
- e. Concretar la captura o el salvamento de material criptográfico.

Resulta determinante tener en cuenta que el enemigo u oponente ejerce estas aptitudes tanto en tiempo de paz como de crisis o guerra, en consecuencia, la seguridad criptográfica se mantendrá sin solución de continuidad entre dichas situaciones.

9.005. Debilidades del sistema. Se deben considerar:

- a. La posibilidad de interceptación del tráfico propio.
- b. La tecnología propia con la disponible para otros actores en función de acrecentar sus capacidades cuando tengan interés de vulnerar la seguridad criptográfica propia.
- c. La comisión de errores en el uso de los sistemas criptográficos que puedan ser aprovechados por terceros interesados en vulnerar la propia seguridad.
- d. La vigencia prolongada de claves o procedimientos en uso.
- e. Deficiencia en la gestión de claves.
- f. Minimizar los incidentes de violación de la normativa sobre claves.

9.006. El material criptográfico y su clasificación de seguridad. El material criptográfico esta constituido por:

- a. Los criptosistemas, su reglamentación, sus historiales y toda la documentación relativa a su uso, control, producción, almacenamiento, asignación, transporte, recepción y destrucción.
- b. La información en claro, procesada con criptosistemas, cuando permita establecer su relación con el correspondiente mensaje cifrado.

Todo el material criptográfico será clasificado "SECRETO" y se regirá su uso por normas particulares, de acuerdo al tipo de comunicación que con él se procure proteger. Entre los aspectos que deben considerarse con esta clasificación de seguridad son:

- a. Procedimientos y dispositivos criptográficos.
- b. Claves.
- c. Llaves y contraseñas de acceso a equipos.
- d. La información procesada por el dispositivo.
- e. Inventarios de material criptográfico.
- f. La documentación relativa a criptosistemas y a los planes criptográficos.
- g. Borradores utilizados en el proceso.

SECCIÓN II

RESPONSABILIDADES

9.007. Responsabilidades del jefe de elemento. Será el responsable del mantenimiento de la seguridad criptológica, por lo tanto, debe:

- a. Dar estricto cumplimiento a las directivas que, con respecto al empleo de los sistemas criptográficos, imparta la autoridad con competencia.
- b. Designar al oficial de claves, oficial de claves reemplazante y al suboficial auxiliar de claves, cuando corresponda.
- c. Realizar, personalmente, las tareas de recepción, control, uso y destrucción de las claves de conocimiento exclusivo del jefe, si existieren, así como también, el tratamiento que demandarán los mensajes en claro, que hubieren sido cifrados con dichas claves.

- d. Controlar que se disponga de las facilidades adecuadas, para garantizar la seguridad física y las condiciones de empleo del material criptográfico.
- e. Controlar sistemática y asistemáticamente todo el material provisto con cargo, como mínimo, en forma trimestral.
- f. Prever los procedimientos de destrucción de emergencia del material clasificado.
- g. En caso de pérdida o vulneración del material criptográfico, proceder a producir los informes y otras medidas determinadas en el PON JEMGE vigente, referido al empleo del material criptográfico del Ejército.

9.008. Responsabilidades del oficial de claves. Para el desempeño de sus funciones, además de lo determinado en la Directiva del JEMGE, tendrá en cuenta los siguientes aspectos:

- a. Será co-responsable, con el jefe del elemento, de la custodia de toda la documentación y material criptográfico.
- b. Podrá delegar en el suboficial auxiliar, el manejo de las claves o material integrante de los criptosistemas.
- c. En caso de ausencia, será reemplazado por el oficial (suboficial) de claves reemplazante.
- d. Deberá controlar que se cumplan los requisitos de seguridad en la operación y el mantenimiento del equipamiento asignado.
- e. Informará de inmediato al jefe de elemento, toda presunta violación de las instrucciones para el empleo de los criptosistemas que detectare. Esto se aplicará, tanto a las producidas dentro de su jurisdicción, como a aquellos hechos observados en el tráfico recibido, cualquiera fuere su origen.
- f. Elaborará un plan de destrucción de emergencia del material criptográfico.
- g. Mantendrá un registro de recepción y distribución de información clasificada.

9.009. Responsabilidades de los usuarios. Deberán mantener en secreto toda la información relativa al criptosistema de aplicación en su ámbito y a la información por él recibida o enviada, que hubiere sido procesada por este.

9.010. Vigencia de la responsabilidad en caso de relevos. El personal vinculado con el material criptográfico que, por cualquier causa fuere separado de éste, conservará la responsabilidad de resguardar la información a la que hubiere tenido acceso en razón de sus funciones. Estará sujeta a todas las normas de seguridad relativas a éstas y a las sanciones prescriptas, para los responsables de la divulgación voluntaria o involuntaria de información clasificada.

SECCION III

SEGURIDAD FÍSICA DEL MATERIAL CRIPTOGRÁFICO

9.011. Seguridad física. La seguridad física debe planificarse y ejecutarse con prioridad sobre cualquier otra instalación. A tal efecto, debe considerarse que:

- a. Deberán proporcionarse las medidas de seguridad más estrictas que fueren factibles, tanto para el almacenamiento del material criptográfico en uso o en reserva, como en su manejo, transporte, reparación o destrucción.
- b. Se negará el acceso de personas no autorizadas a los equipos, que forman parte de criptosistemas o a los equipos de comunicaciones, que incluyeren componentes criptográficos.
- c. Se efectuarán periódicamente, estudios de seguridad de los locales destinados a realizar actividades criptográficas, empleando, si se dispusiere, el equipamiento técnico necesario, para detectar la presencia de elementos de escucha subrepticia.

9.012. Cajas fuertes, cofres y armarios metálicos

a. Exigencias mínimas.

1) Cajas fuertes.

- a) Ser robustas y pesadas.
- b) Tener cierre a combinación de tres discos, si fuere posible.
- c) Brindar protección contra incendio.

2) Cofres metálicos.

- a) Ser de chapa, reforzados en el marco y en la puerta.
- b) Tener un cierre a llave de seguridad, de doble paleta.
- c) Ser estancos.

3) Armarios metálicos.

- a) Ser de chapa y estar reforzados en el marco y en la puerta.
- b) Tener un cierre a llave de seguridad, de doble paleta o a combinación de tres discos.
- c) Estar, en lo posible, sujeto al piso, mampara o paredes.

b. Normas con respecto a las combinaciones y llaves de cerraduras de seguridad:

1) Los números que forman la combinación, deberán ser seleccionados al azar.

2) La combinación de una caja fuerte deberá ser recordada de memoria, por el personal autorizado.

3) El registro de la combinación en vigencia, será guardado en un sobre cerrado, rotulado SECRETO, indicando su contenido y los nombres de las personas que conocen dicha combinación. Cada sobre no deberá tener más de una combinación y será entregado al Jefe del elemento, el que será responsable de su inviolabilidad.

4) Cada caja fuerte deberá tener una combinación distinta.

5) La combinación de una caja fuerte debe ser cambiada por personal responsable y, a su vez, debe confeccionarse el registro correspondiente de las personas que la conocen. Se deberá considerar siempre:

- a) Cuando se la recibiére por primera vez.
- b) Cuando cualquier persona que conociere la combinación, cambie de destino.
- c) Cuando se implementare un criptosistema, que modificare el vigente o se recibieren claves.
- d) Cuando se sospechare o se conociere que la combinación, pudiere estar en conocimiento de personas no autorizadas.
- e) Por lo menos, una vez por año.

6) Llaves de cerraduras de cajas fuertes, cofres, armarios metálicos y cifrarios:

- a) Se tendrá en servicio la mínima cantidad de llaves de una misma cerradura.
- b) Las llaves de los criptosistemas deberán ser mantenidas bajo la máxima condición de seguridad.

- c) Una copia de cada una de las llaves, será entregada, en un sobre cerrado, al jefe del elemento. Cada sobre no deberá tener más de una llave; en él se indicará, además, cuántas copias de la llave existen y en poder de quién se encuentran.
- d) Si se perdiera una llave, se procederá de inmediato al reemplazo de la cerradura.
- e) Las llaves de locales que contienen material criptográfico no deberán colocarse en llaveros generales.

9.013. Cifrarios

a. Cifrarios en instalaciones fijas.

- 1) Normalmente, los requerimientos de seguridad física correspondientes a un cifrario, hará necesario, que una sala fuere destinada exclusivamente, a las funciones criptológicas.

En caso de resultar imposible destinar una sala independiente, deberán adoptarse las siguientes medidas: emplear y almacenar el material criptográfico en un sector que se adecuará de tal forma, que quedare aislado física y visualmente de las personas no autorizadas, que pudieren encontrarse en el lugar, mientras se efectuaren trabajos, con el equipo cifrador o la documentación relacionada.

- 2) En todos los cifrarios, será necesario que las facilidades empleadas para la realización de los trabajos criptológicos y para el almacenamiento del material correspondiente, ofrecieren como mínimo, aún cuando no fuere posible utilizarlas exclusivamente para funciones criptográficas, los siguientes resguardos:
 - a) Las puertas deberán ser de construcción sólida y poseer cerraduras seguras; deberá emplearse una sola puerta de entrada, la que permanecerá con llave, cuando no estuviere ocupada o cuando se realizaren en el local, trabajos criptológicos.
 - b) El local se dispondrá de tal manera que, desde su entrada no podrán observarse las actividades criptológicas y que toda persona, antes de ingresar, pueda ser identificada.
 - c) Las ventanas deberán tener una protección, a fin de evitar la observación desde el exterior e impedir la entrada subrepticia.

b. Cifrarios en instalaciones móviles. Deberá cumplimentarse lo señalado en el apartado anterior, en la medida de lo posible. Además deberá tenerse en cuenta lo siguiente:

- 1) Nunca deberán permanecer sin seguridad.
- 2) En tránsito, deberán contar con una protección equivalente a la especificada para el elemento de más alta clasificación que contuvieren.

9.014. Almacenamiento, manipulación y custodia del material clasificado. El almacenamiento del material criptográfico implica una serie de acciones concretas con material (equipos y medios) y documentación que serán destinados a su guarda y custodia en cajas, cofres o armarios de seguridad y sólo podrá permanecer fuera de su lugar de almacenamiento el tiempo que demandare su utilización, preparación para envío o destrucción. Este material esta constituido por:

- a. Los procedimientos criptológicos.
- b. Los listados de claves secretas y de contraseñas.
- c. Las llaves de operación y las de acceso al interior de los equipos criptológicos.
- d. Los equipos inyectoros de claves.
- e. Los equipos criptológicos.
- f. Los módulos de claves de reserva.
- g. Las publicaciones componentes de los criptosistemas.

- h. Los módulos de claves en vigencia, cuando el usuario lo considerare necesario.

Si sólo se contare con una caja, cofre o armario de seguridad, tendrá prioridad el almacenamiento del material criptográfico, con respecto al de sus publicaciones componentes.

- a. Manipulación de la información clasificada.

La información cifrada y sus correspondientes copias, en lenguaje claro, serán archivados separadamente. Ambos serán guardados, con la misma clasificación de seguridad.

- b. Manipulación de los materiales de trabajo.

Las hojas de trabajo, las copias excedentes, las cintas y soportes magnéticos empleados en la preparación y procesamiento de la información clasificada, serán objeto de las mismas prevenciones que correspondiere a cualquier otro material clasificado. Cuando se hiciere un borrador, o se transcribiere información clasificada, se emplearán hojas sueltas de papel, colocadas sobre una superficie dura. En todos los casos, el material excedente resultante deberá ser destruido por trituración o cualquier otro método adecuado.

- c. Custodia.

Cuando no se dispusieren las facilidades establecidas anteriormente, el jefe de elemento establecerá los procedimientos que ofrecieren una seguridad adecuada, mediante la asignación de personal de custodia necesario.

9.015. Lugar de instalación de los equipos criptológicos

El funcionamiento del sistema de comunicaciones y el responsable del elemento u organismo, determinarán el lugar de instalación del equipamiento criptográfico. Todos los equipos criptográficos (no instalados en sistemas de comunicaciones) y los métodos manuales, serán utilizados en locales considerados como áreas excluidas.

Los equipos instalados en sistemas de comunicaciones, serán utilizados desde el lugar que correspondiere, al más eficaz uso del sistema. Las llaves de operación, los inyectores de claves o cualquier otro dispositivo que se utilizare para la introducción de claves, deberán estar bajo el control permanente del personal responsable y constatado su registro en la planilla correspondiente a tal efecto.

Para telegrafía, transmisión de datos y facsímil, los equipos se utilizarán en las centrales de comunicaciones o de computación, en las estaciones receptoras y en general, en el lugar donde se encontrare el equipo terminal de comunicaciones, con las limitaciones de permanecer siempre dentro de un área restringida. Los criptosistemas para voz serán empleados por personal convenientemente instruido y debidamente autorizado.

En las instalaciones fijas se utilizarán, preferentemente, desde cabinas acústicas, con total atenuación del sonido, desde adentro hacia afuera. En las unidades móviles, se utilizarán desde lugares, en los que la conversación en claro, no pudiere ser escuchada, grabada o retransmitida, por personas no autorizadas.

Los equipos instalados en unidades móviles y que pudieren quedar fuera del control del personal responsable de ellos, deberán tener, si fuere posible, un montaje de quita, a efectos de poder retirarlos de sus emplazamientos.

9.016. Transporte del material criptográfico

El transporte se efectuará siempre desprovisto de las claves y/o componentes secretos, factibles de ser removidos, que permitieren su uso. Cuando su peso y tamaño lo permita, deberán ser llevados en forma personal, por el correo responsable.

Cuando por su peso y tamaño debieran viajar en bodegas de carga, las llaves de operación deben ser enviadas, teniendo en cuenta lo determinado en las directivas que se establecen en particular por el organismo responsable de su control.

9.017. Remisión del material criptográfico

Según las características y facilidades con que contare el elemento, los medios de envío autorizados serán: personal autorizado del criptosistema, correo militar y correo diplomático (cuando fuere a la mano).

9.018. Mantenimiento de equipos criptológicos

a. Condiciones generales.

- 1) En lugares autorizados para la instalación de equipos del elemento.
 - a) Los equipos a reparar, no deberán tener instalada clave alguna.
 - b) Para la prueba de funcionamiento, se utilizará una clave ya provista para ese propósito.
 - c) Las claves serán retiradas u ocultadas de la vista de los técnicos que efectúen la reparación, excepto cuando el mantenimiento, lo realice personal designado por la Dir Grl Icia.
 - d) Siempre que los técnicos se encontraren trabajando, deberá hallarse presente personal responsable del criptosistema.
- 2) En talleres no pertenecientes al elemento.
 - a) Se verificará, que los equipos sean entregados sin clave y sin ningún aditamento, que pudiese revelar la modalidad de su uso.
 - b) Antes de ser puesto nuevamente en servicio, el equipo será sometido a una inspección, tendiente a determinar su confiabilidad, en cuanto a transmisión subrepticia de información, interferencia o sabotaje.
- 3) Queda prohibida la reparación de un equipo criptográfico por personas no autorizadas por el órgano Director de Inteligencia.

SECCION IV

DESTRUCCIÓN DEL MATERIAL CRIPTOGRÁFICO

9.019. Consideraciones básicas. El material criptográfico sólo será destruido, cuando así lo ordene el jefe del elemento y éste deberá considerar taxativamente las órdenes y disposiciones vigentes. Antes de proceder con esta tarea, se revisarán exhaustivamente todos los componentes, a fin de verificar que estuviere completo y que se destruya lo que corresponda o sea necesario.

El personal responsable de la elaboración del plan de destrucción será también, quien deberá ponerlo en ejecución. Cuando en la preparación de información clasificada, se emplearen hojas de trabajo, borradores, papel carbónico u otros elementos similares, se procederá a su destrucción inmediata, a medida que dejaren de ser necesarios.

9.020. Procedimiento para la destrucción de rutina. En el caso de que el material fuere provisto por otro organismo, sólo se procederá a destruirlo, por orden expresa del mismo. Cuando se proceda a la destrucción del material criptográfico, en cumplimiento de órdenes emanadas del organismo o elemento que hubiere provisto ese material, se procederá de acuerdo con lo establecido en el PON JEMGE 06/00.

9.021. Destrucción de emergencia. El personal designado para el transporte, custodia o supervisión del material criptográfico tendrá la responsabilidad de efectuar la destrucción de emergencia. Las medidas que deberán adoptarse, para asegurar la destrucción efectiva del material en caso de emergencia, dependerán de las condiciones existentes en la zona y de la posibilidad de pérdida o captura (de acuerdo con la situación).

En general, la destrucción de emergencia se efectuará de acuerdo con el siguiente detalle:

- a. El material reemplazado, apenas se presente alguna duda, sobre su seguridad física.
- b. El material de reserva, cuando hubiese amenaza de peligro, sin esperar hasta último momento.
- c. El que se encontrare en vigencia deberá ser retenido para su empleo, todo el tiempo posible, preservándose el sistema de más amplia difusión hasta el último momento y destruyéndose el resto.

Los equipos criptológicos electrónicos serán abiertos y destruidos sus circuitos componentes. Si el equipo tuviere módulo clave, será retirado y destruido su circuito electrónico. La exigencia mínima consistirá en el borrado de emergencia de las claves. La destrucción de emergencia será informada de inmediato a la autoridad superior y a la Dir Grl Icia.

CAPÍTULO X

MEDIDAS DE SEGURIDAD REFERIDAS A INFORMÁTICA

SECCIÓN I

CONCEPTOS GENERALES

10.001. Definición. Es un conjunto de procedimientos y técnicas que se relacionan con diferentes tipos de aplicaciones (software) y dispositivos (hardware) destinados a prevenir, proteger y garantizar la integridad, confiabilidad y disponibilidad de la información clasificada gestionada a través de sistemas de información y la tecnología para su procesamiento.

10.002. Glosario de términos informáticos

Sistemas informáticos: conjunto de partes interrelacionadas, hardware, software y de recursos humanos (humanware) que permite almacenar y procesar información.

Información: se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.

Sistema de información: se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales.

Tecnología de la información: se refiere al hardware y software operados por el elemento o por un tercero que procese información en su nombre, para llevar a cabo una función propia, sin tener en cuenta la tecnología utilizada, ya se trate de computación de datos, telecomunicaciones u otro tipo.

Datos sensibles: información inherente a inteligencia, cuya entidad posee características de seguridad superior a "Reservado".

Confidencialidad: se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.

Integridad: se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.

Disponibilidad: se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.

Autenticidad: busca asegurar la validez de la información en tiempo, forma y distribución. Asimismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.

Auditabilidad: define que todos los eventos de un sistema deben poder ser registrados para su control posterior.

Protección a la duplicación: consiste en asegurar que una transacción sólo se realiza una vez, a menos que se especifique lo contrario. Impedir que se grabe una transacción para luego reproducirla, con el objeto de simular múltiples peticiones del mismo remitente original.

No repudio: se refiere a evitar que una entidad que haya enviado o recibido información alegue ante terceros que no la envió o recibió.

Legalidad: referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeto el organismo.

Confiabilidad de la Información: es decir, que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.

Incidente de seguridad informático: Es un evento adverso en un sistema de computadoras, o red de computadoras, que compromete la confidencialidad, integridad o disponibilidad, la legalidad y confiabilidad de la información y los recursos tecnológicos. Puede ser causado mediante la explotación de alguna vulnerabilidad o un intento o amenaza de romper los mecanismos de seguridad existentes.

10.003. Consideraciones básicas. Las medidas de seguridad de contrainteligencia que se describen, persiguen como objetivo principal, preservar las particularidades de la información contenidas y/o procesadas por medios informáticos.

El incremento en el número de aplicaciones que se da a los sistemas informáticos, la concentración de información y el procesamiento de datos, así como la incorporación en la Fuerza, de sistemas cada vez más complejos, que incluyen procesamiento en línea y tiempo real, han aumentado los riesgos de seguridad.

El criterio que rige la seguridad de la información procesada en medios informáticos, debe ser el mismo que el de la información documentada en otros soportes, en todos los aspectos que conforman la gestión de dicha información, tales como producción, distribución, custodia, reproducción, destrucción, etc., con las particularidades que impone esta tecnología, especialmente en lo atinente a la implementación de nuevos y mayores resguardos derivados de las debilidades de estos sistemas.

La seguridad informática exige la aplicación constante y coordinada de medidas de seguridad relacionadas a instalaciones y equipos, personas y comunicaciones.

La posibilidad de acceso a la información que brinda la tecnología informática hace que no pueda considerarse que una situación de debilidad en la seguridad informática de un equipo aislado pueda no tener efectos sobre el conjunto de los sistemas informáticos de una organización militar.

En tal sentido, las medidas de seguridad referidas a Informática se adoptarán para ser efectivamente cumplidas por todos los sistemas informáticos que constituyan la apoyatura permanente o circunstancial de la organización militar, lo que incluye equipos aislados (fijos o portátiles), redes cerradas, redes abiertas y otros dispositivos compatibles con los sistemas informáticos, como teléfonos inteligentes u otras expresiones de computadores personales de tamaño reducido con capacidad de compartir protocolos informáticos.

Esta variedad de posibilidades y combinaciones informáticas también incluye a la infraestructura que soporta los elementos mencionados, tanto sea con vínculos estáticos (cable, fibra óptica) o por aire.

10.004. Criterios de uso. Todo sistema informático destinado a la gestión de información clasificada deberá contar con la habilitación del órgano de Inteligencia del nivel que se trate, a fin de la determinación del nivel de información clasificada que podrá tramitarse a través de él.

Las redes abiertas no deberán habilitarse para el uso de información clasificada salvo que se cuente con adecuados sistemas de encriptamiento y estos sean autorizados para la transmisión de información clasificada. Esta autorización emanará de las máximas autoridades responsables de Inteligencia e Informática.

Resulta determinante que toda aquella información que posea clasificación de seguridad, no sea trabajada o se encuentre almacenada en equipos con conexión directa a la red de Internet.

La habilitación será certificada periódicamente y se incluirá como parte de las infraestructuras analizadas para la confección de estudios e inspecciones de seguridad.

En el proceso previo a la habilitación del sistema, el organismo administrador deberá realizar un estudio de seguridad que incluya las normas de seguridad informática específicas, debiendo solicitar el asesoramiento de Inteligencia y dejar constancia del mismo en el estudio de seguridad.

10.005. Vulnerabilidad de los sistemas informáticos. Los sistemas informáticos (hardware / software) estarán sujetos, entre otros, a los siguientes riesgos:

- a. Destrucción intencional por inutilización permanente o transitoria de los equipos, de los dispositivos de almacenamiento, de sus contenidos, del software que en ellos se ejecute o almacene, o de los servicios que ellos presten.
- b. Violaciones por intromisión, tales como:
 - 1) Interceptación: toma de control por terceros, no perceptible por un operador.
 - 2) Artimañas: conexión por conocimiento no autorizado de la contraseña.
 - 3) Derivación: conexión irregular, ignorada.
 - 4) Engaño: conexión fingida, simulando otra conexión autorizada.
 - 5) Fisgoneo: observación en pantalla, de deshechos de listados de datos no autorizados, de información residual en dispositivos de almacenamiento o colas de impresión.
 - 6) Mediante programas tipo “Caballo de Troya”, virus o robots: software subrepticio no visible para el operador, que sustraen datos de un archivo o interfaz humana, para insertarlos en otro archivo local o enviarlos a través del sistema de red local o Internet, programas que ocasionen pérdida de datos o denegación de servicio.
- c. Accidentes en los locales, por acciones imprevistas o involuntarias.
- d. Inutilización permanente o transitoria por causas naturales, de los equipos.
- e. Errores por manipuleo inadecuado.
- f. Fallas de energía.

10.006. Dispositivos informáticos

- a. Máquinas y dispositivos de escritorio.

Las computadoras y dispositivos de escritorio (impresoras, faxes, pequeños concentradores, concentradores USB, etc.), son uno de los puntos más difíciles de controlar, pues dependen totalmente del uso o mal uso que el usuario final pueda realizar de ellos o sobre ellos. La única solución en este caso es la implantación de una política clara y comprensible para el usuario final de uso de los dispositivos que están a su cargo.

Es importante responsabilizar de alguna forma al usuario final del hardware que está a su cargo como parte de su trabajo normal. Se debe encontrar una adecuada relación entre la facilidad y flexibilidad en el uso de los dispositivos a cargo del usuario final y la seguridad física de estos dispositivos.

- b. Computación móvil.

Cuando se utilizan dispositivos informáticos móviles se debe tener especial cuidado en garantizar que no se comprometa la información de la Fuerza.

Cuando nos referimos a estos dispositivos denominados de computación móvil, debemos incluir notebooks, laptop o PDA (asistente personal digital), tablet, teléfonos celulares y sus tarjetas de memoria, dispositivos de almacenamiento removibles, tales como CD, DVD, dispositivos de almacenamiento de conexión USB, dispositivos criptográficos, cámaras digitales, etc. Esta lista no debe considerarse taxativamente, ya que existen otros dispositivos que pudieren contener información clasificada.

Se debe tener en cuenta que la portabilidad de estos dispositivos los hace susceptibles de ser robados o sustraídos temporalmente con facilidad.

Debe determinarse una indubitable política de uso y responsabilidad para las personas que utilizan ordenadores portátiles institucionales y sobre todo para quienes tienen que trasladarse con estos dispositivos fuera del organismo. La información disponible en este tipo de equipos será la mínima indispensable para el cumplimiento de una función determinada y con las mayores barreras lógicas, encriptamiento y fragmentación de los contenidos informativos posibles.

Debe responsabilizarse seriamente a los usuarios de los equipos portátiles a mantener un estricto control de entrada / salida de estos dispositivos y de la integridad física de los mismos. Al reingresar un equipo portátil al elemento se deberá verificar la inexistencia de virus, software no deseado, etc., para habilitar nuevamente su uso interno.

En la verificación de ingreso deberá incluirse la comparación de los archivos autorizados de salida para comprobar la integridad de los datos.

10.007. Incidentes de seguridad informática. Un incidente de seguridad informática es un evento adverso en un sistema de computadoras, o red de computadoras, que compromete la confidencialidad, integridad o disponibilidad, la legalidad y confiabilidad de la información y los recursos tecnológicos. Puede ser causado mediante la explotación de alguna vulnerabilidad o un intento o amenaza de romper los mecanismos de seguridad existentes.

Se considera una parcial clasificación de CINCO (5) incidentes de seguridad informática, a los fines de facilitar su identificación:

a. Acceso NO Autorizado. Esta categoría comprende todo tipo de ingreso y operación no autorizado a los sistemas, tanto exitosos como no exitosos. Son parte de esta categoría:

- 1) Accesos no autorizados exitosos, sin perjuicios visibles a componentes tecnológicos.
- 2) Robo de información.
- 3) Borrado de información.
- 4) Alteración de la información.
- 5) Intentos recurrentes y no recurrentes de acceso no autorizado.
- 6) Abuso y mal uso de los servicios informáticos internos o externos que requieren autenticación.

b. Código malicioso. Esta categoría comprende la introducción de códigos maliciosos en la infraestructura tecnológica del instrumento Militar. Son parte de esta categoría los virus informáticos, troyanos y los gusanos informáticos.

c. Denegación del servicio. Esta categoría incluye los eventos que ocasionan pérdida de un servicio en particular. Los síntomas para detectar un incidente de esta categoría son:

- 1) Tiempos de respuesta muy bajos sin razones aparentes.
- 2) Servicio(s) interno(s) inaccesibles sin razones aparentes.
- 3) Servicio(s) externo(s) inaccesibles sin razones aparentes.

d. Escaneos, pruebas o intentos de obtención de información de la red o de un servidor en particular. Esta categoría agrupa los eventos que buscan obtener información de la infraestructura tecnológica del instrumento militar y comprende a los "Sniffers" (software utilizado para capturar información que viaja por la red) y la detección de vulnerabilidades (método de prueba y error).

e. Mal uso de los recursos tecnológicos. Esta categoría agrupa los eventos que atentan contra los recursos tecnológicos por el mal uso y comprende:

- 1) Mal uso y/o abuso de servicios informáticos internos o externos.
- 2) Violación de las normas de acceso a Internet.
- 3) Mal uso y abuso del correo electrónico institucional.
- 4) Violación de las políticas, normas y procedimientos de seguridad informática reglamentadas.

Los incidentes deben ser registrados y difundidos a los órganos de Inteligencia de su zona de responsabilidad, para su evaluación como accionar de sistemas de Inteligencia adversarios.

SECCION II

SEGURIDAD FÍSICA

10.008. Conceptos generales. La seguridad física brinda el marco para minimizar los riesgos de daños e interferencias a la información mediante la negación y/o neutralización de las amenazas de carácter físico en aquellos sectores y sistemas relacionados directa o indirectamente a la informática.

A fin de brindar la seguridad física a los sistemas de información (hardware y software) se deberá tener en cuenta lo establecido en el capítulo de “Medidas de Seguridad Física de las Instalaciones”, ampliándose con aquellos aspectos que por la especificidad de los efectos a proteger, se enumeran.

10.009. Provisión de energía. En toda instalación informática, especialmente las que cuenten con procesamiento en línea o tiempo real, el suministro de energía será fundamental. Debido a que normalmente, no será posible apoyar a todos los integrantes de la red, el correspondiente comando de la organización militar prestará especial atención, a los elementos de primera prioridad dentro de ella.

El suministro de energía deberá estar de acuerdo con las especificaciones del fabricante o proveedor de cada equipo. El equipamiento estará protegido con respecto a las posibles fallas en el suministro de energía u otras anomalías eléctricas. Para asegurar la continuidad del suministro de energía, se contemplarán las siguientes medidas de control:

- a. Disponer de múltiples enchufes o líneas de suministro para evitar un único punto de falla en el suministro de energía.
- b. Contar con un suministro de energía continua (UPS) para asegurar el apagado regulado y sistemático o la ejecución continua del equipamiento que sustenta las operaciones críticas del organismo. La determinación de dichas operaciones críticas, será el resultado del análisis de impacto realizado por el responsable de seguridad informática. Los planes de contingencia contemplarán las acciones que han de emprenderse ante una falla de la UPS. Los equipos de UPS serán inspeccionados y probados periódicamente para asegurar que funcionan correctamente y que tienen la autonomía requerida.
- c. Montar un generador de respaldo para los casos en que el procesamiento deba continuar ante una falla prolongada en el suministro de energía. Deberá realizarse un análisis de impacto de las posibles consecuencias ante una interrupción prolongada del procesamiento, con el objeto de definir que componentes será necesario abastecer de energía alternativa. Cuando el encendido de los generadores no sea automático, se asegurará que el tiempo de funcionamiento de la UPS permita el encendido manual de los mismos. Los generadores serán inspeccionados y probados periódicamente para asegurar que funcionen según lo previsto.

Asimismo, se procurará que los interruptores de emergencia se ubiquen cerca de las salidas de emergencia de las salas donde se encuentra el equipamiento, a fin de facilitar un corte rápido de la energía en caso de producirse una situación crítica. Se proveerá de iluminación de emergencia en caso de producirse una falla en el suministro principal de energía. Se implementará protección contra descargas eléctricas en todos los edificios y líneas de comunicaciones externas de acuerdo a las normativas vigentes.

10.010. Consideraciones en los cableados. El cableado de energía eléctrica y de comunicaciones que transporta datos o brinda apoyo a los servicios de información estará protegido contra interceptación o daño, mediante las siguientes acciones:

- a. Cumplir con las normas y requisitos técnicos vigentes de la República Argentina.
- b. Utilizar pisoducto o cableado embutido en la pared, siempre que sea posible, cuando corresponda a las instalaciones de procesamiento de información. En su defecto estarán sujetas a la siguiente protección alternativa: caños metálicos, bandejas pasacables y toda aquella protección acorde a las normas IRAM.
- c. Proteger el cableado de red contra interceptación no autorizada o daño, adoptando medidas de seguridad física particulares como: conductos especiales o evitando trayectos que atravesen áreas públicas.
- d. Separar los cables de energía de los cables de comunicaciones para evitar interferencias.

- e. Proteger el tendido del cableado troncal (backbone)* mediante la utilización de ductos blindados.

*Backbone: Se refiere a la principal conexión troncal de Internet. Es el subsistema vertical en una instalación de red de área local que sigue la normativa de cableado estructurado.

10.011. Sistemas de refrigeración. Los lugares destinados a la guarda de los sistemas informáticos o dispositivos de almacenamiento estarán ventilados, libres de la acción directa de los campos magnéticos de cualquier tipo, con temperaturas que oscilarán entre 5° y 30° C.

Para los centros de cómputos, será conveniente contar con temperaturas entre 15° y 22° C y con humedad relativa, entre 45% y 55%, mientras que el bulbo húmedo no debe exceder los 24° C.

Una sala de servidores (datacenter), incluye aspectos particulares en cuanto a refrigeración. En principio, los factores que permitirán apreciar una conclusión acertada, serán: la superficie de la sala, los tipos de servidores que allí operan, la infraestructura de las redes, la alimentación eléctrica redundada, sistema autónomo de alimentación (generador de gasoil), los aires acondicionados disponibles y los reguladores de temperatura y humedad. Todo ello, debe complementarse y mantener en lo posible, cifras cercanas a las expuestas y recomendadas para los centros de cómputos. Es ideal mantenerse por debajo de estos valores.

10.012. Prevención contra incendios. Los sensores de humo o calor que se instalen, deberán ser capaces de detectar los distintos tipos de gases, que desprendan los cuerpos en combustión.

Estos deberán instalarse en la sala de cómputos, junto al área de oficinas y en el perímetro físico de las instalaciones. Deberán estar conectadas con la alarma central del elemento o con el personal de guardia.

Los extintores y otros elementos utilizados para la lucha contra el fuego, se ubicarán en lugares de fácil acceso. Deberán estar cargados con el producto adecuado para instalaciones electrónicas. Estos medios se controlarán con regularidad, para asegurar su funcionamiento efectivo.

SECCION III

SEGURIDAD DE LOS SISTEMAS OPERATIVOS

10.013. Planificación y aprobación de sistemas

a. Planificación de la capacidad.

El oficial veedor de informática, el jefe o encargado del área informática y el personal de asesores que se designe conformarán un equipo de trabajo que evaluarán periódicamente la situación del sistema informático y asesorarán al jefe del organismo con el objeto de elaborar los programas y planes a fin de determinar las capacidades actuales de los sistemas operativos y proyectar las necesidades futuras a fin de garantizar el procesamiento y almacenamiento adecuado. Asimismo, aquellas novedades sobre la violación a las medidas de seguridad que se detecten serán informadas al escalón superior de forma de subsanar la vulnerabilidad, investigar y determinar responsabilidades y adoptar las medidas disciplinarias o legales que correspondan.

b. Aprobación de los sistemas.

El jefe o encargado del área informática, el oficial de comunicaciones, el oficial de medidas de seguridad de contrainteligencia y el personal de asesores que se designe evaluarán y sugerirán criterios de aprobación para nuevos sistemas o programas de información, actualizaciones y nuevas versiones, solicitando la realización de las pruebas necesarias antes de su aprobación definitiva y posterior empleo.

En todos los casos donde surgiere la necesidad de instalar sistemas o programas de información nuevos, actualizaciones o nuevas versiones se deberá solicitar autorización a los organismos de la Fuerza con responsabilidad sobre el área.

10.014. Intercambios o cesión de sistemas de información y software. Cuando se realicen acuerdos entre organismos, cualquiera fueran ellos, para el intercambio o cesión de sistemas de información y software, se especificarán el grado de sensibilidad de la información de la Fuerza involucrada y las condiciones de seguridad de la misma. Se deberán considerar todos aquellos aspectos plasmados en el capítulo "Medidas de Seguridad de Contrainteligencia referida a la documentación y material clasificado".

10.015. Los programas informáticos. Las debilidades en los programas representarán un riesgo sustancial y fundamental, para la seguridad del sistema. Se deberá partir de la premisa de que no se ha encontrado un sistema completamente seguro.

La seguridad de los programas pretende: restringir el acceso a los programas y archivos, verificar que se realice un empleo correcto de datos, archivos y programas, asegurar que no puedan modificarse los programas / archivos e impedir que puedan introducirse programas que produzcan efectos maliciosos, que lleven a la pérdida de información, a una denegación de servicio u otro efecto no deseado.

Será esencial identificar cuáles serán las debilidades de los programas, para lo cual se debe tener en cuenta los siguientes aspectos:

- a. Se confeccionará un listado de las debilidades existentes.
- b. Se realizará un inventario de las debilidades que no se hubieren identificado todavía, pero que sí se hubieren mencionado.
- c. Se probarán las debilidades existentes y potenciales, para verificar su existencia.
- d. Se definirá alguna forma de control, para cada debilidad.
- e. Se elaborará un plan de acción, para realizar los controles.

10.016. Sistema de transmisión de datos. Las redes de computadoras son, muchas veces, el medio más sencillo para la acción de personas que ingresan a los sistemas sin la debida autorización, la entrada de virus o la comisión de fraudes, de distinto tipo. Es así, como el ingreso de personas ajenas al sistema permitirá destruir o hurtar información propietaria de la organización o implantar virus, que iniciarán su acción destructiva, en determinado momento.

Los actores y los riesgos o amenazas que los mismos ocasionan a nuestro sistema, suele ser variados, de evolución permanente y con las aplicaciones de distinta naturaleza, imponiendo continuamente nuevas técnicas y procedimientos.

Es sumamente difícil prevenir, controlar o identificarlos. El problema de la seguridad es aún mucho mayor, en razón de que muchas veces, quien comete la acción es un integrante de la misma organización o un programador / usuario con habilidad y quizás, con alguna motivación para producir el caos en la red.

Por lo tanto, será esencial implementar medidas de seguridad tendientes a prevenir y neutralizar estas acciones, basándose en productos de seguridad y elementos que permiten proteger la transmisión de datos.

Las medidas de seguridad que pueden aplicarse, estarán conformadas en base a hardware, a software o una combinación de ambos y poseerán entre otras, alguna de las siguientes características:

- a. Seguridad jerárquica flexible.
- b. Encriptamiento / desencriptamiento automático.
- c. Códigos de identificación de usuario.
- d. Transmisiones seguras con enlaces PP, PMP, ya sean reales o virtuales, mediante túneles.
- e. Uso de dispositivos hardware externo, en combinación con software almacenado internamente.
- f. Software y hardware de detección y bloqueo de intrusiones (IDS, FIREWALLS, otros)
- g. Software y hardware de detección de programas malintencionados.
- h. Hardware de conectividad programable con capacidad de definir niveles de acceso.

SECCIÓN IV

SEGURIDAD DE LA INFORMACIÓN

10.017. Seguridad de la información documentada bajo formato digital. La seguridad de la información documentada se corresponderá a lo establecido en el capítulo “Medidas de Seguridad de Contrainteligencia referida a la información y material clasificado”.

10.018. Mantenimiento. Copia de resguardo de la información. El responsable del área Informática, el oficial veedor de informática del organismo y los propietarios de la información determinarán los requerimientos para resguardar cada información de acuerdo a su criticidad. En base a ello, si no existieran órdenes y procedimientos del escalón superior, se definirá y documentará un esquema de resguardo particular, de acuerdo a las características propias del área informática, el tipo y clasificación de la información y las particularidades del organismo.

Ese resguardo será una responsabilidad del área informática, quien además, deberá respetar los siguientes aspectos:

- a. Rotular los distintos soportes de guarda de la información para identificar cada una de ellas y administrarlas debidamente.
- b. Prever un esquema de reemplazo de los medios de almacenamiento de las copias de resguardo, una vez concluida la posibilidad de reutilizarlos.
- c. Almacenar en una ubicación remota copias recientes de información de resguardo junto con registros exactos y completos de las mismas y los procedimientos documentados de restauración, a una distancia suficiente como para evitar riesgos o amenazas al lugar de guarda principal.
- d. Los dispositivos de almacenamiento de información deberán guardarse y controlarse siguiendo las medidas y normas de seguridad establecidas en el capítulo “Medidas de Seguridad de Contrainteligencia referida a la información y material clasificado”.
- e. La protección de la información de resguardo deberá responder a los criterios establecidos en el capítulo “Medidas de Seguridad de Contrainteligencia referida a la información y material clasificado”.
- f. Se deberán retener al menos TRES (3) generaciones o ciclos de información de resguardo para la información y el software esenciales para el organismo.
- g. Se deberá verificar regularmente que los medios de resguardo sean útiles.
- h. Se verificará y probará periódicamente los procedimientos de restauración garantizando su eficacia y cumplimiento dentro del tiempo asignado a la recuperación en los procedimientos operativos.
- i. El período para llevar a cabo el resguardo dependerá de las características de cada organismo, el cual determinará y plasmará taxativamente en los documentos que fijen los procedimientos del área informática.

SECCIÓN V

SEGURIDAD DE LOS DISPOSITIVOS INFORMÁTICOS

10.019. Clasificación general. Los dispositivos informáticos son aquellos efectos físicos de material informático que conforman el hardware de un sistema.

10.020. Protección del equipamiento físico. Las debilidades de los equipos, sólo serán relevantes en las instalaciones consideradas como primera prioridad; por lo tanto será necesario identificarlas y determinar la manera de asegurar tales equipamientos. Deberá ser ubicado y protegido de tal manera que se reduzcan los riesgos ocasionados por amenazas y peligros ambientales, y las oportunidades de acceso no autorizado, teniendo en cuenta los siguientes puntos:

- a. Ubicar el equipamiento en un sitio donde se minimice el acceso innecesario y existan barreras de seguridad y controles de acceso adecuado.

- b. Ubicar los equipos de procesamiento y almacenamiento de información que manejan datos sensibles (información con alta clasificación de seguridad), en un sitio que permita la supervisión durante su uso.
- c. Aislar los elementos que requieren protección especial para reducir el nivel general de protección requerida.
- d. Adoptar controles adecuados para minimizar el riesgo de amenazas potenciales, por:
 - 1) Robo o hurto.
 - 2) Incendio.
 - 3) Explosivos.
 - 4) Humo.
 - 5) Inundaciones o filtraciones de agua (o falta de suministro).
 - 6) Polvo.
 - 7) Vibraciones.
 - 8) Efectos químicos.
 - 9) Interferencia en el suministro de energía eléctrica (cortes de suministro, variación de tensión).
 - 10) Radiación electromagnética.
 - 11) Derrumbes.

Esto deberá contemplarse y preverse su inclusión en un Manual de Operaciones de material informático particular, para el personal y/o elemento del cual es orgánico ese equipo.

10.021. Seguridad de terminales. El problema esencial referido a la seguridad de las terminales, será, principalmente, su uso indebido. Por lo tanto, el acceso a los servicios de información sólo será posible a través de un proceso de conexión seguro y estará diseñado para minimizar la oportunidad de acceso no autorizado.

Este procedimiento, debe divulgar la mínima información posible acerca del sistema, a fin de evitar proveer de asistencia innecesaria a un usuario no autorizado. Además se tendrá en cuenta la ubicación de las terminales, el acceso físico a ellas y el control sobre la operación no autorizada de la terminal, por medio de claves, códigos u otro método de restricción e identificación de operadores.

El equipo, los programas y otras verificaciones, deben garantizar el cumplimiento de los controles para los distintos tipos de dispositivos de almacenamiento, que se utilizaren para datos y programas.

Este control de accesos deberá:

- a. Mantener en secreto los identificadores de sistemas o aplicaciones hasta tanto se halla llevado a cabo exitosamente el proceso de conexión.
- b. Desplegar un aviso general advirtiendo que sólo los usuarios autorizados pueden acceder a la computadora.
- c. Evitar dar mensajes de ayuda que pudieran asistir a un usuario no autorizado durante el procedimiento de conexión.
- d. Validar la información de la conexión sólo al completarse la totalidad de los datos de entrada. Si surge una condición de error, el sistema no debe indicar que parte de los datos es correcta o incorrecta.
- e. Limitar el número de intentos de conexión no exitosos permitidos y registrar los intentos no exitosos.

- f. Impedir otros intentos de identificación, una vez superado el límite permitido. Desconectar conexiones de comunicaciones de datos.
- g. Limitar el tiempo máximo permitido para el procedimiento de conexión. Si este es excedido, el sistema debe finalizar la conexión.
- h. Desplegar la siguiente información, al completarse una conexión exitosa: Fecha y hora de la conexión exitosa anterior. Detalles de los intentos de conexión no exitosos desde la última conexión exitosa.

10.022. Accesos desde equipos terminales a un equipo central. Restricciones de equipamiento: para acceder (conectarse) a un equipo central, será preciso contar con una terminal de entrada / salida (generalmente de video) y con una línea de conexión, que resultaren compatibles, con dicho equipo central.

Restricciones para acceder al equipo central: los operadores de terminal tendrán restringido su acceso al equipo central mediante contraseñas o claves de acceso, las que deberán escribirse cada vez que debieren conectarse con dicho equipo.

Restricciones para acceder a una aplicación: las aplicaciones tendrán controles de acceso particulares, los que asegurarán, que sólo podrán conectarse con ellas, los operadores debidamente autorizados. Estos controles consistirán en una contraseña o clave de acceso personal para cada operador y diferente para cada aplicación.

También podrá restringirse, el grado de acceso de cada aplicación, referido en especial, al nivel de acceso a los archivos (podrá ver toda o parte de la información allí registrada) y al nivel de operación (podrá consultar los datos o también, modificarlos e incluso, borrarlos).

Autorizaciones centralizadas: un área propietaria para cada aplicación será la medida más conveniente a implementar en cada elemento. Esta será la dependencia interna que demanda la respectiva aplicación y que trabaja orgánicamente con la información y los datos que contiene.

Esta área propietaria será la única instancia habilitada para proponer, a la jefatura del elemento, las restricciones que se impondrán para acceder a su aplicación.

10.023. Centros de cómputos. La ubicación de los centros de cómputos será lo más alejada posible de las áreas de tránsito en gran escala. Deberán estar aislados, hasta donde fuere posible, de los sectores de alto riesgo de las instalaciones. Cuando compartieren el espacio con otros elementos, se los ubicará en el lugar que ofreciere menor riesgo. Según el nivel de información que administraren, serán clasificados, dentro de un área restringida o eventualmente, excluida.

Las conexiones entre estos centros de cómputos y las computadoras de una organización, deben contener las mismas medidas de seguridad, complementándose entre ambos subsistemas.

El acceso a los centros de cómputos, áreas de mantenimiento y depósito de elementos usados y para baja. En principio, serán definidos como áreas restringidas.

- a. Los controles de acceso no deberán variar durante las distintas horas del día; serán de particular importancia, los que se efectúen durante los cambios de turno del personal.
- b. Extender las barreras físicas necesarias desde el piso (real) hasta el techo (real), a fin de impedir el ingreso no autorizado y la contaminación ambiental, por ejemplo por incendio, humedad e inundación.
- c. Ingreso de personas ajenas a estos sectores.
 - 1) Deberán ser identificadas y registradas en forma adecuada.
 - 2) Se mantendrá un control permanente sobre ellas, durante su permanencia.
 - 3) El personal de mantenimiento, ajeno a la organización, no podrá permanecer solo, en ningún momento, cualquiera fuere la tarea a realizar.

10.024. Seguridad en computadoras personales. Conceptos generales. Las computadoras personales (PC) podrán estar conectadas o no a una red. En ambos casos se deberán cumplir las medidas de seguridad antes enunciadas para las terminales (Artículo 10.021), si cumpliesen esa función y para el acceso a un equipo central.

La información sensible que se procesa con medios informáticos y equipos de telecomunicaciones asociados, deberá ser protegida de los riesgos informáticos específicos de:

- a. Amenazas a los computadores.
 - 1) Pérdida de información.
 - 2) Lectura no autorizada de información.
 - 3) Modificación deliberada de la información, en tiempo de proceso.
 - 4) Acciones no autorizadas a memorias.
 - 5) Destrucción intencional.
 - 6) Contingencia.
- b. Amenazas a la seguridad de los archivos.
 - 1) Pérdida de información.
 - 2) Acceso no autorizado, a archivos.
 - 3) Incorrecta información en archivos.
- c. Amenaza a la seguridad en las telecomunicaciones.
 - 1) Empleo correcto de terminales.
 - 2) Conexiones no autorizadas.
 - 3) Conexiones indirectas.
- d. Amenazas a la privacidad de la información.
 - 1) Amenazas a información del personal.
 - 2) Amenazas a información, de la cual la organización es propietaria.

10.025. Protección de las computadoras

- a. Medidas de protección a nivel instalaciones.

Comprenderán aquellas medidas de carácter básicamente preventivo que se adoptarán para proporcionar a los equipos de procesamiento de datos, la seguridad relacionada con la restricción del acceso a los locales en donde se encontraren, a todo el personal no autorizado. A los conceptos ya expresados en el capítulo de "Medidas de Seguridad Física de Instalaciones" se deberá considerar, para aquellos locales con material informático, las siguientes medidas:

- 1) Los locales deberán poseer cerraduras adecuadas y armarios para guardar debidamente los accesorios, documentación y discos de trabajo.
- 2) En cada local donde se encontrare una computadora, deberá encontrarse en forma visible, un inventario actualizado de los componentes.
- 3) La sala de servidores será clasificada como ZONA EXCLUIDA.
- 4) Plan de evacuación. En caso de que un siniestro ponga en peligro la integridad física del recurso informático se deberán tener en cuenta las siguientes consideraciones para su evacuación:

- a) Prioridad 1 (Letra “A” – Triángulo Color Rojo): CPU(s) de servidores y computadoras personales, back up, documentación clasificada de sistemas y códigos fuente.
- b) Prioridad 2 (Letra “B” - Triángulo Color Amarillo): monitores, impresoras, elementos de conectividad y dispositivos de almacenamiento (disquetes, CD(s), discos Zip, cintas, torres de discos, etc.).
- c) Prioridad 3 (Letra “C” Triángulo Color Verde): teclados y resto de recursos.

b. Medidas de seguridad a nivel hardware.

Estas medidas serán especificadas en los equipos de computación, ya que se trata de capacidades técnicas de origen. Hay muchas y diversas formas de implementar barreras de protección y controles de acceso a través del hardware. Existen por ejemplo, ciertos dispositivos que se conectan a alguno de los pórticos exteriores de la computadora y/o periféricos y que al ser retirados, imposibilitan la operación de la máquina, dispositivos a base de tarjetas de proximidad o huellas digitales, que pueden utilizarse junto a un sistema de contraseñas para autenticar al usuario.

Existen sistemas de llaves removibles, para el bloqueo del acceso a unidades de disco, bloqueo de teclado, etc. Deberán asegurarse adecuadamente, las llaves u otros dispositivos de bloqueo, restringiendo la difusión de las palabras claves de acceso, de acuerdo con las medidas de seguridad establecidas.

c. Medidas de seguridad a nivel software.

Este tipo de protección se materializará a través de la restricción de acceso a los sistemas o módulos, mediante la asignación de uno o más códigos o palabras de acceso a los usuarios.

Conceptualmente, el sistema pedirá en forma interactiva, el ingreso del código, antes de permitir el acceso a cada usuario; a modo de una llave, que bloquea la entrada al sistema en forma global o bien, a módulos específicos.

d. Medidas de protección de documentación de sistemas.

La documentación a que se hace referencia, será exclusivamente la relacionada con los sistemas y que normalmente, se llevará en los centros de procesamiento de información. No se incluirá aquella, que podrá clasificarse como documentación de trabajo de cada usuario (la que se registrará, por las consideraciones de seguridad propias de cada caso). En esta categoría, entrarán aquellos documentos que se emplearán para el desarrollo, implementación y mantenimiento de los sistemas, a saber:

- 1) Carpeta de desarrollo del sistema (diagrama de sistemas, lógicos de flujos, cursogramas, códigos, definición de archivos, definición de pantallas, Etc).
- 2) Carpetas o manuales de procedimientos.
- 3) Carpeta de registro de modificaciones y actualizaciones.

La documentación tendrá la misma clasificación de seguridad, que la información de mayor clasificación a procesar.

e. Las medidas de protección a nivel procedimientos.

Constituirán la más eficaz barrera de protección, para la seguridad de la información en uso; una consciente disciplina de seguridad en la aplicación de los procedimientos, permitirá reducir las debilidades del sistema informático.

**RECUERDE: “EL USUARIO ES EL ESLABON
MAS DELGADO DEL SISTEMA DE SEGURIDAD”**

Algunos de los procedimientos a utilizar, serán:

- 1) Arranque: Todas las computadoras deberán tener en el disco de arranque, la siguiente secuencia de inicio:
 - a) Carga del procedimiento de detección preventiva de virus.
 - b) Mensaje de seguridad en pantalla generado por el archivo, Ej:

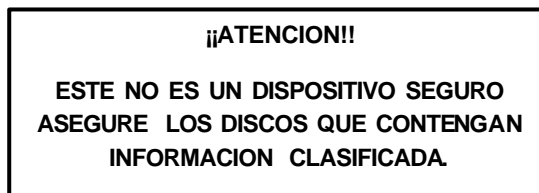


Figura 2

- 2) **Procedimientos de almacenamiento.** Quedará terminantemente prohibido, el almacenamiento de archivos que contuvieren información clasificada en unidades de disco rígido. Los mismos se almacenarán en diskettes, CD/DVD, pen drives, que serán convenientemente guardados en armarios de seguridad.

No se podrá almacenar información clasificada, en maquinas o dispositivos de almacenamiento removibles, de propiedad particular del personal.

- 3) Finalización del trabajo. Al finalizar el trabajo con información clasificada, deberá realizarse el apagado completo del sistema, antes de permitir a otro usuario continuar trabajando sobre la misma máquina. Deberá llevarse un "Registro de Operación" de acuerdo con el formato, que se indica en la figura 3

FORMULARIO DE REGISTRO DE OPERACIÓN DE COMPUTADORAS					
FECHA	HORA		OPERADOR	PROGRAMAS	OBS
	Desde	Hasta	Apellido y Nombre	UTILIZADOS	

Figura 3

Este registro podrá ser eliminado si el sistema tuviere capacidad de plasmar los usuarios que accedieron al dispositivo, la oportunidad en que lo hicieron y la posibilidad de que este registro este disponible para consulta en el equipo o desde el centro de Cómputo o administrador del sistema.

10.026. Dispositivos de almacenamiento removible. Medidas de protección. Los dispositivos de almacenamiento removibles (unidades de cinta, disco, diskette, CD, DVD, discos externos, USB, tarjetas de memoria, etc.) son un componente altamente vulnerables del sistema informático; sus reducidas dimensiones hacen que sean fáciles de ocultar y transportar; y si a lo expresado, le sumamos su enorme capacidad de almacenamiento, la magnitud del riesgo se incrementará. Estos dispositivos de almacenamiento deberán estar debidamente registrados y guardados, bajo normas estrictas sobre su manipuleo y utilización.

En cada dependencia, se llevará un registro permanente de los medios de almacenamiento que contuvieren información sensible, su distribución y los responsables. Cada uno de los dispositivos deberá estar identificado de acuerdo al siguiente detalle:

- a. Etiqueta: en ROJO con la leyenda: "Información CLASIFICADA".
- b. Oblea: será del color correspondiente a la clasificación del documento de mayor clasificación de seguridad almacenado.
- c. Nro: número de control permanente asignado al soporte y separado por una barra (/) seguido por los CUATRO (4) dígitos correspondientes al año de origen del documento (Ej: 23/2012).
- d. Dependencia: dependencia usuaria.

- 1) Contenido: breve descripción del contenido. En caso de ser extensa, hacer referencia al inventario que contiene el detalle.

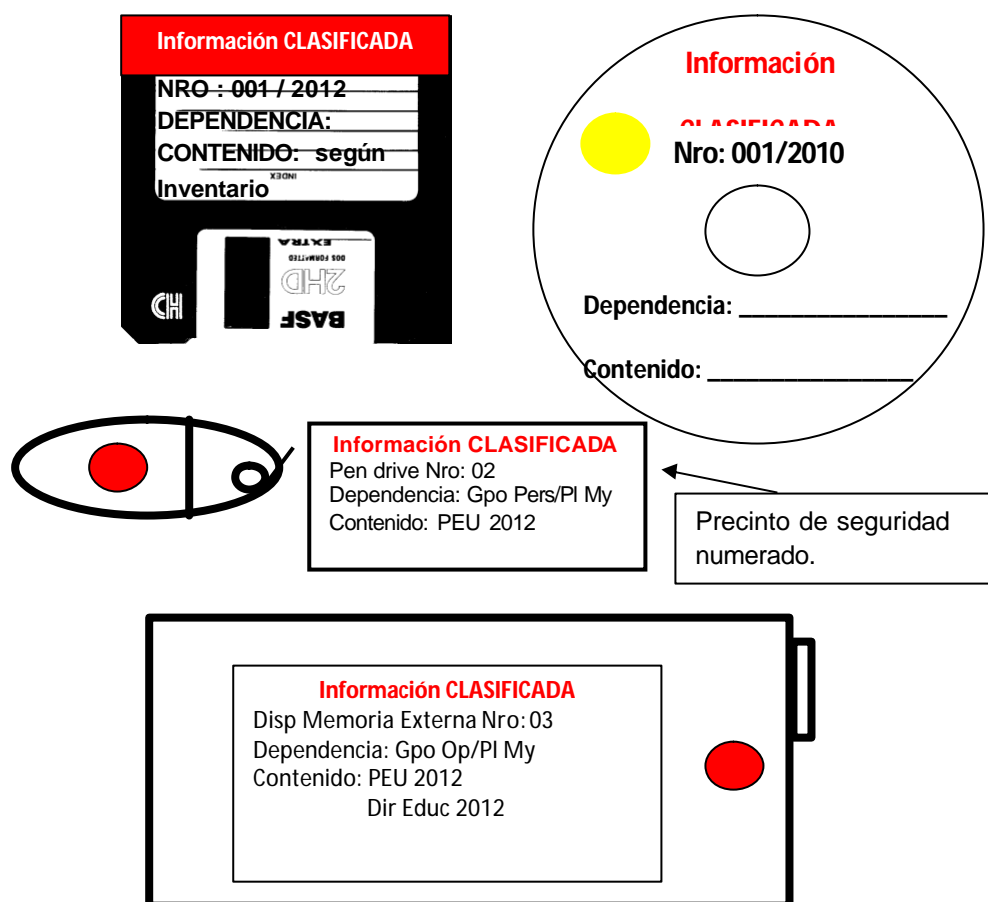


Figura 4

10.027. Destrucción y/o eliminación de información bajo formato digital. En el caso de que se debiere destruir información documentada bajo algún formato digital, se deberán utilizar distintos métodos.

La técnica empleada por el sistema operativo para el borrado de archivos y programas de disco rígido o diskettes, CD/DVD es un proceso reversible, en la mayoría de los casos. A través de ciertos métodos, será posible reconstruir en forma efectiva, la información borrada por lo que será necesario tomar ciertas precauciones.

Estas, consistirán en el borrado absoluto por "sobre-escritura"; a tal efecto, podrá emplearse alguno de los siguientes procedimientos:

- Empleo del programa FORMAT del sistema operativo.
- Empleo de programas como el WIPEDISK, ERASER, Etc.
- Empleo de dispositivos de desmagnetización.

En el caso de los Pen drives, se realizará un formateo de bajo nivel.

10.028. Destrucción y/o eliminación de dispositivos de almacenamiento en desuso. Los diskettes, CD/DVD, pen drives, discos rígidos y cualquier otro dispositivo inutilizados por defectos físicos deberán destruirse antes de su disposición definitiva, mediante procedimientos mecánicos comunes o bien, incinerándolos.

SECCION VI

SEGURIDAD DE USUARIOS

10.029. Conceptos generales. La seguridad de la información se basa en la capacidad para preservar su integridad, confidencialidad y disponibilidad, por parte de los elementos involucrados en su tratamiento: equipamiento, software, procedimientos, así como de los recursos humanos que utilizan dichos componentes.

En este sentido, es fundamental educar e informar al personal desde su ingreso y en forma continua, cualquiera sea su situación de revista, acerca de las medidas de seguridad que afectan al desarrollo de sus funciones y de las expectativas depositadas en ellos en materia de seguridad y asuntos de confidencialidad. De la misma forma, es necesaria la aplicación de sanciones en caso de incumplimiento.

La implementación de las medidas de seguridad referidas a la Informática tiene como meta minimizar la probabilidad de ocurrencia de incidentes. Es por ello que resulta necesario implementar un mecanismo que permita reportar las debilidades y los incidentes tan pronto como sea posible, a fin de subsanarlos y evitar eventuales repeticiones. Por lo tanto, es importante analizar las causas del incidente producido y aprender del mismo, a fin de corregir las prácticas existentes que no pudieron prevenirlo, y evitarlo en el futuro.

Por ello, es importante reducir los riesgos de error humano, la comisión de ilícitos, el uso inadecuado de instalaciones y de los recursos, y manejo no autorizado de la información.

Para esto, los usuarios deben estar al corriente de las amenazas e incumbencias en materia de seguridad, y encontrarse capacitados para cumplir las medidas de seguridad establecidas en el presente reglamento, en el transcurso de sus tareas normales.

10.030. Registro de usuarios. El responsable de la seguridad informática (SCD) junto con el responsable de las medidas de seguridad de contrainteligencia (oficial inteligencia) definirán un procedimiento formal de registro de usuarios para otorgar y revocar el acceso a todos los sistemas, bases de datos y servicios de información mono usuario y multiusuario, el cual debe comprender:

- a. Utilizar identificadores de usuario único, de manera que se pueda identificar a los usuarios por sus acciones evitando la existencia de múltiples perfiles de acceso para un mismo empleado. El uso de identificadores grupales sólo debe ser permitido cuando sean convenientes para el trabajo a desarrollar debido a razones operativas.
- b. Verificar que el usuario tiene autorización para el uso del sistema, base de datos o servicio de información.
- c. Verificar que el nivel de acceso otorgado es adecuado para el propósito de la función del usuario y es coherente con la política de seguridad establecida
- d. Entregar a los usuarios un detalle escrito de sus derechos de acceso.
- e. Requerir que los usuarios firmen declaraciones señalando que comprenden y aceptan las condiciones para el acceso.
- f. Garantizar que los proveedores de servicios no otorguen acceso hasta que se hayan completado los procedimientos de autorización.
- g. Mantener un registro formal de todas las personas registradas para utilizar el servicio.
- h. Cancelar inmediatamente los derechos de acceso de los usuarios que cambiaron sus tareas, o de aquellos a los que se les revocó la autorización, se desvincularon del organismo o sufrieron la pérdida/robo de sus credenciales de acceso.
- i. Efectuar revisiones periódicas con el objeto de cancelar identificadores, cuentas de usuarios redundantes, inhabilitar cuentas inactivas por más de 45 días y eliminar cuentas inactivas por más de 120 días. En el caso de existir excepciones, deberán ser debidamente justificadas y aprobadas.
- j. Garantizar que los identificadores de usuario redundantes no se asignen a otros usuarios.

- k. Adoptar medidas disciplinarias con todo aquel personal de la organización que intente acceder a los sistemas a los cuales sabe que no se encuentra autorizado. Esta actitud es claramente contraria al proceder normal y, a modo de prevención, debe ser corregida.

10.031. Administración de contraseñas de usuarios. La asignación de contraseñas se controlará a través de un proceso de administración formal, mediante el cual deben respetarse los siguientes pasos:

- a. Requerir que los usuarios firmen una declaración por la cual se comprometen a mantener sus contraseñas personales en secreto y las contraseñas de los grupos de trabajo exclusivamente entre los miembros del grupo.
- b. Garantizar que los usuarios cambien las contraseñas iniciales que les han sido asignadas la primera vez que ingresan al sistema. Las contraseñas provisionales, que se asignan cuando los usuarios olvidan su contraseña, sólo debe suministrarse una vez identificado el usuario.
- c. Generar contraseñas provisionales seguras para otorgar a los usuarios. Se debe evitar la participación de terceros o el uso de mensajes de correo electrónico sin protección (texto claro) en el mecanismo de entrega de la contraseña y los usuarios deben dar acuse de recibo cuando la reciban.
- d. Almacenar las contraseñas sólo en sistemas informáticos protegidos.
- e. Utilizar otras tecnologías de autenticación y autorización de usuarios, como ser la biométrica (por ejemplo verificación de huellas dactilares), verificación de firma, uso de autenticadores de hardware (como las tarjetas de circuito integrado), etc.
- f. Configurar los sistemas de tal manera que:
 - 1) Las contraseñas tengan 12 caracteres.
 - 2) Suspendan o bloqueen permanentemente al usuario luego de 3 intentos de entrar con una contraseña incorrecta (deberá pedir la rehabilitación ante quien corresponda).
 - 3) Solicitar el cambio de la contraseña cada 30 días.
 - 4) Impedir que las últimas 12 contraseñas sean reutilizadas.
 - 5) Establecer un tiempo de vida mínimo de 30 días para las contraseñas.

10.032. Administración de contraseñas críticas. En los diferentes ambientes de procesamiento existen cuentas de usuarios con las cuales es posible efectuar actividades críticas como ser instalación de plataformas o sistemas, habilitación de servicios, actualización de software, configuración de componentes informáticos y otros.

Dichas cuentas no serán de uso habitual (diario), sino que sólo serán utilizadas ante una necesidad específica de realizar alguna tarea que lo requiera y se encontrarán protegidas por contraseñas con un mayor nivel de complejidad que el habitual.

El responsable de la seguridad Informática definirá procedimientos para la administración de dichas contraseñas críticas que contemplen lo siguiente:

- a. Se definirán las causas que justificarán el uso de contraseñas críticas así como el nivel de autorización requerido.
- b. Las contraseñas seleccionadas serán seguras, y su definición será efectuada como mínimo por dos personas, de manera que ninguna de ellas conozca la contraseña completa.
- c. Las contraseñas y los nombres de las cuentas críticas a las que pertenecen serán resguardadas debidamente.
- d. La utilización de las contraseñas críticas será registrada, documentando las causas que determinaron su uso, así como el responsable de las actividades que se efectúen con la misma.
- e. Cada contraseña crítica se renovará una vez utilizada y se definirá un período luego del cual la misma será renovada en caso de que no se la haya utilizado.

- f. Se registrarán todas las actividades que se efectúen con las cuentas críticas para luego ser revisadas. Dicho registro será revisado posteriormente por el responsable de seguridad.

10.033. Revisión de derechos de accesos de usuarios. A fin de mantener un control eficaz del acceso a los datos y servicios de información, el responsable de seguridad Informática llevará a cabo un proceso formal, a intervalos regulares de 6 meses, a fin de revisar los derechos de acceso de los usuarios. Se deberán contemplar los siguientes controles:

- a. Revisar los derechos de acceso de los usuarios a intervalos de 6 meses.
- b. Revisar las autorizaciones de privilegios especiales de derechos de acceso a intervalos de 3 meses.
- c. Revisar las asignaciones de privilegios a intervalos de 6 meses, a fin de garantizar que no se obtengan privilegios no autorizados.

10.034. Responsabilidades del usuario - Contraseñas. Los usuarios deben seguir buenas prácticas de seguridad en la selección y uso de contraseñas. Las contraseñas constituyen un medio de validación y autenticación de la identidad de un usuario, y consecuentemente un medio para establecer derechos de acceso a las instalaciones o servicios de procesamiento de información. Los usuarios deben cumplir las siguientes directivas:

- a. Mantener las contraseñas en secreto.
- b. Pedir el cambio de la contraseña siempre que exista un posible indicio de compromiso del sistema o de las contraseñas.
- c. Seleccionar contraseñas de calidad, de acuerdo a las prescripciones informadas por el responsable de seguridad Informática, además se debe tratar que:
 - 1) Sean fáciles de recordar.
 - 2) No estén basadas en algún dato que otra persona pueda adivinar u obtener fácilmente mediante información relacionada con la persona, por ejemplo: nombres, números de teléfono, fecha de nacimiento, etc.
 - 3) No tengan caracteres idénticos consecutivos o grupos totalmente numéricos o totalmente alfabéticos.
- d. Cambiar las contraseñas cada vez que el sistema se lo solicite y evitar reutilizar o reciclar viejas contraseñas.
- e. Cambiar las contraseñas provisionales en el primer inicio de sesión ("log on").
- f. Evitar incluir contraseñas en los procesos automatizados de inicio de sesión, por ejemplo, aquellas almacenadas en una tecla de función o macro.
- g. Notificar de acuerdo a lo establecido, cualquier incidente de seguridad relacionado con sus contraseñas: pérdida, robo o indicio de pérdida de confidencialidad.

Si los usuarios necesitan acceder a múltiples servicios o plataformas y se requiere que mantengan múltiples contraseñas, se notificará a los mismos que pueden utilizar una única contraseña para todos los servicios que brinden un nivel adecuado de protección de las contraseñas almacenadas y en tránsito.

10.035. Equipos desatendidos en áreas de usuarios. Los usuarios deberán garantizar que los equipos desatendidos sean protegidos adecuadamente. Los equipos instalados en áreas de usuarios, por ejemplo estaciones de trabajo o servidores de archivos, requieren una protección específica contra accesos no autorizados cuando se encuentran desatendidos.

Se deberá concientizar a todo el personal, acerca de los requerimientos y procedimientos de seguridad, para la protección de equipos desatendidos, así como de sus funciones en relación a la implementación de dicha protección. Los usuarios cumplirán con las siguientes pautas:

- a. Concluir las sesiones activas al finalizar las tareas, a menos que puedan protegerse mediante un mecanismo de bloqueo adecuado, por ejemplo, un protector de pantalla protegido por contraseña.
- b. Proteger las computadoras o terminales contra usos no autorizados mediante un bloqueo de seguridad o control equivalente, por ejemplo, contraseña de acceso cuando no se utilizan.

SECCION VII

SEGURIDAD DE REDES INFORMÁTICAS

10.036. Conceptos generales. Cada organismo de la Fuerza establecerá un número determinado de redes según las características del mismo, disponibilidad de recursos y exigencias de las instalaciones, información a tramitar y conexiones de red necesarias, entre otros considerandos.

Como premisa fundamental de estas conexiones de red, se establece como una prohibición que las redes internas del organismo donde se encuentra información clasificada no deben estar enlazadas con redes públicas, bajo ningún concepto.

10.037. Control de acceso a la red. Las conexiones no seguras a los servicios de red pueden afectar a todo el organismo, por lo tanto, se controlará el acceso a los servicios de red tanto internos como externos. Esto es necesario para garantizar que los usuarios que tengan acceso a las redes y a sus servicios, no comprometan la seguridad de los mismos. Se otorgará el acceso a los servicios y recursos de red, únicamente, de acuerdo al pedido formal del titular de una organización que lo solicite para personal de su incumbencia. Este control es particularmente importante para las conexiones de red a aplicaciones que procesen información clasificada o aplicaciones críticas. Para ello, se desarrollarán procedimientos para la activación y desactivación de derechos de acceso a las redes, las cuales comprenderán:

- a. Identificar las redes y servicios de red a los cuales se permite el acceso.
- b. Realizar normas y procedimientos de autorización para determinar las personas y las redes y servicios de red a los cuales se les otorgará el acceso.
- c. Establecer controles y procedimientos de gestión para proteger el acceso a las conexiones y servicios de red.

10.038. Camino forzado. Las redes están diseñadas para permitir el máximo alcance de distribución de recursos y flexibilidad en la elección de la ruta a utilizar. Estas características también pueden ofrecer oportunidades para el acceso no autorizado a las distintas aplicaciones o para el uso no autorizado de servicios de información. Por esto, el camino de las comunicaciones será controlado.

Se limitarán las opciones de elección de la ruta entre la terminal de usuario y los servicios a los cuales el mismo se encuentra autorizado a acceder, mediante la implementación de controles en diferentes puntos de la misma. Algunos de estos criterios deberán ser tenidos en cuenta a la hora de su implementación:

- a. Asignar números o líneas, en forma dedicada.
- b. Establecer la conexión automática de puertos a gateways de seguridad o a sistemas de aplicación específicos.
- c. Limitar las opciones de menú o submenú de cada uno de los usuarios.
- d. Evitar la navegación ilimitada por la red.
- e. Imponer el uso de sistemas de aplicación y/o gateways de seguridad específicos para usuarios externos de la red.
- f. Controlar activamente las comunicaciones con origen y destino autorizados a través de un Gateway, por ejemplo utilizando firewalls.
- g. Restringir el acceso a redes estableciendo dominios lógicos separados, por ejemplo, redes privadas virtuales para grupos de usuarios dentro o fuera de la Fuerza.

10.039. Autenticación de usuarios para conexiones externas. Las conexiones externas son de gran potencial para accesos no autorizados a la información de la Fuerza. Por consiguiente, el acceso de usuarios remotos estará sujeto al cumplimiento de procedimientos de autenticación, algunos de los cuales brindan un mayor nivel de protección que otros. La autenticación de usuarios remotos puede llevarse a cabo utilizando:

- a. Un método de autenticación físico.
- b. Método de revocación de acceso del autenticador, en caso de compromiso de seguridad.
- c. Un protocolo de autenticación.

10.040. Autenticación de nodos. Una herramienta de conexión automática a una computadora remota podría brindar un medio para obtener acceso no autorizado a una aplicación de la Fuerza. Por consiguiente, las conexiones a sistemas informáticos remotos serán autenticadas. Esto es particularmente importante si la conexión utiliza una red que está fuera de control de la gestión de seguridad de la Fuerza.

10.041. Protección de los puertos (Ports) de diagnóstico remoto. Algunos equipos informáticos y sistemas de comunicación son instalados y administrados con una herramienta de diagnóstico remoto. Si no están protegidos, estos puertos de diagnóstico proporcionan un medio de acceso no autorizado, por consiguiente, deberán ser protegidos por un mecanismo de seguridad apropiado.

9.042. Subdivisión de redes. Para controlar la seguridad en una red, se podrán dividir en dominios lógicos separados. Para esto, se definirán y documentarán los perímetros de seguridad que sean convenientes. Estos perímetros se implementarán mediante la instalación de "gateways" con funcionalidades de "firewall" o redes privadas virtuales, para filtrar el tráfico entre los dominios y para bloquear el acceso no autorizado.

La subdivisión en dominios de la red tomará en cuenta criterios como los requerimientos de seguridad comunes de grupos integrantes de la red, la mayor exposición de un grupo a peligros externos, separación física, u otros criterios de aglutinamiento o segregación preexistentes.

10.043. Control de ruteo de red. En las redes compartidas, especialmente aquellas que se extiendan fuera de los límites del organismo, se incorporarán controles de ruteo, para asegurar que las conexiones informáticas y los flujos de información no violen las medidas adoptadas en lo referente a los controles de acceso. Estos controles contemplarán, mínimamente, la verificación positiva de direcciones de origen y destino. Adicionalmente, para este objetivo pueden utilizarse diversos métodos incluyendo, entre otros, la autenticación de protocolos de ruteo, ruteo estático, traducción de direcciones y listas de control de acceso.

10.044. Redes inalámbricas. Las redes inalámbricas deberán reunir estrictas condiciones de seguridad para su empleo. Entre las medidas a adoptar para instalar y usar este tipo de red, se deberán considerar:

- a. Sistemas de control de acceso y un canal seguro.
- b. Se deben montar protocolos de acceso y validación.
- c. Procesos de cifrado del canal.
- d. Uso de claves.
- e. Uso de RADIUS como punto central de validación.

10.045. Seguridad de los servicios de red. Se deberán fijar las pautas para garantizar la seguridad de los servicios de red de la Fuerza, tanto públicos como privados. Para ello, se tendrá en cuenta las siguientes consideraciones:

- a. Mantener instalados y habilitados sólo aquellos servicios que sean utilizados.
- b. Controlar el acceso lógico a los servicios, tanto a su uso como a su administración.
- c. Configurar cada servicio de manera segura, evitando las vulnerabilidades que pudieran presentar.

- d. Instalar periódicamente las actualizaciones de seguridad.
- e. Dicha configuración será revisada periódicamente.

SECCIÓN VIII

SEGURIDAD EN INTERNET

10.046. Conceptos generales. La red del internet es una red **NO SEGURA**, en ella conviven millones de usuarios y no todos con buenas intenciones. Conectarse a través de la red segura del Ejército (INTRANET) impone un riesgo que ha sido evaluado y convenientemente minimizado por medio de un esquema de seguridad (Firewall) en el cual USTED también forma parte IMPORTANTÍSIMA.

La forma más segura de poseer una conexión a internet es tener totalmente aislada la PC conectada a internet de manera tal que solo ella sea la que sufra las consecuencias de un ataque y se limite a su entorno, pudiendo reinstalar el sistema operativo y aplicaciones ante la contingencia. Se deberán cumplir las siguientes normas de seguridad:

- a. **Está prohibido acceder a internet vía módem desde una PC mientras esté conectada a la red LAN del elemento, se deberá desconectar físicamente de la boca de conexión a la red LAN. Esto, considerando que la computadora sólo guarda información del sistema operativo.**
- b. El acceso a internet será utilizado con propósitos autorizados o para el destino por el cual fue provisto.
- c. Se generara un registro de los accesos de los usuarios a internet, con el objeto de realizar revisiones de los accesos efectuados o analizar casos particulares.
- d. Se deberá restringir el acceso a:
 - 1) Correo electrónico.
 - 2) Sistemas de transferencia de archivos.
 - 3) Redes sociales y foros.
 - 4) Acceso a la red fuera del horario laboral.

Está prohibido el uso de redes sociales y sistemas similares de contactos personales, como sistemas de mensajería instantánea y foros, a través de Internet, en el ámbito de la Fuerza.

El criterio para la solicitud de una conexión a internet, debe atender los siguientes parámetros de seguridad:

- a. La máxima autoridad del elemento u organismo tendrá en cuenta que solo se justificará cuando la "necesidad de saber" del usuario autorizado así lo requiera y estará en relación directa con las funciones que desempeñe en su puesto de trabajo. Deberá considerar que cada acceso a Internet hará más vulnerable al sistema en general y a su propia red LAN en primera instancia. Además, se supone que toda la información necesaria la encontrará en la INTRANET (red segura) del Ejército.

Todo enlace a Internet se ejecutará a través del servidor de Internet del EMGE, siendo la Dir Sis Com Info el elemento auditor de los accesos a la red pública.

- b. Cualquier elemento que requiriera una conexión particular a Internet deberá documentar esa necesidad e informar/comunicar la misma, vía jerárquica, por nota el Director del Estado Mayor General (Dir Sis Com Info), especificando el proveedor del servicio, servicios contratados, puesto de trabajo o rol de combate y los fundamentos. Recibirá directivas particulares para la configuración de los accesos, filtros y registros para la auditoría del enlace.
- c. Deberá existir en el elemento u organismo una lista de los usuarios autorizados a tener acceso a Internet, siendo objeto de control por parte del responsable de la Seguridad Informática de que los usuarios de estas estaciones de trabajo posean un profundo conocimiento de las instrucciones sobre seguridad informática.

10.047. Sistemas de acceso público. Protección de la información publicada electrónicamente. Se tomarán recaudos para la protección de la integridad de la información publicada electrónicamente, a fin de prevenir la modificación no autorizada que podría dañar la reputación y la seguridad de la Fuerza. Todos los sistemas de acceso público como un servidor web, deberán prever que:

- a. La información se obtenga, procese y proporcione de acuerdo a la normativa vigente, en especial que no afecte de alguna forma a la seguridad de la Fuerza
- b. La información que se ingresa al sistema de publicación, o aquella que procesa el mismo, sea procesada en forma completa, exacta y oportuna.
- c. La información sensible sea protegida durante el proceso de recolección y su almacenamiento.
- d. El acceso al sistema de publicación no permita el acceso accidental a las redes a las cuales se conecta el mismo.
- e. Se registre al responsable de la publicación de información en sistemas de acceso público.
- f. La información se publique teniendo en cuenta las normas establecidas al respecto.
- g. Se garantice la validez y vigencia de la información publicada.

10.048. Control de software malicioso. Deben emplearse preventivamente, programas especiales, llamados genéricamente antivirus, para detectar en oportunidad la presencia de programas ocultos que pudieren tener por finalidad, dañar los datos almacenados en discos rígidos (virus informático). La mejor prevención contra este tipo de programas consistirá en prohibir el uso de dispositivos de almacenamiento extraíbles, de propiedad de particular del personal.

Se deberán utilizar programas antivirus, toda vez que se vaya a trabajar con un dispositivo de almacenamiento extraíble proveniente de otra computadora que no fuere la propia del operador. Normalmente, será necesario realizar controles periódicos tendientes a considerar el cumplimiento de las siguientes acciones:

- a. Prohibir el uso de software no autorizado por el elemento.
- b. Redactar procedimientos para evitar los riesgos relacionados con la obtención de archivos y software desde o a través de redes externas, o por cualquier otro medio, señalando las medidas de protección a tomar.
- c. Instalar y actualizar periódicamente software de detección y reparación de virus, examinado computadoras y medios informáticos como medida precautoria y rutinaria.
- d. Mantener los sistemas al día con las últimas actualizaciones de seguridad disponibles (probar dichas actualizaciones en un entorno de prueba previamente si es que constituyen cambios críticos a los sistemas).
- e. Revisar periódicamente el contenido de software y datos de los equipos de procesamiento que sustentan procesos críticos del elemento, investigando formalmente la presencia de archivos no aprobados o modificaciones no autorizadas.
- f. Verificar antes de su uso, la presencia de virus en archivos de medios electrónicos de origen incierto, o en archivos recibidos a través de redes no confiables.
- g. Concientizar al personal acerca del problema de los falsos virus (hoax) y de cómo proceder frente a los mismos.

CAPITULO XI

MEDIDAS DE SEGURIDAD EN APOYO A LAS OPERACIONES

SECCIÓN I

CONCEPTOS GENERALES

11.001. Conceptos generales. Las operaciones tácticas serán todas aquellas actividades que desarrollen las tropas cuando se las emplea ante la existencia de un enemigo, para el cumplimiento de una misión determinada ("Conducción para el Instrumento Militar Terrestre" - ROB-00-01 Cap V, Art 5.002).

Toda operación táctica encierra una idea o concepción con perfiles característicos, una técnica propia de ejecución y una finalidad que la tipifica y distingue. Las medidas de seguridad de Contrainteligencia que se deban llevar adelante en este tipo de operación deberán ser coordinadas en un tiempo y espacio determinado, exigirá precisos niveles de conducción, combinación de movimientos, maniobras e información a fin de lograr la seguridad del Instrumento Militar.

Es importante destacar que, a diferencia del campo de batalla pasado, los medios tecnológicos modernos, especialmente la denominada guerra de la información, impondrá ampliar las dimensiones y atender una naturaleza distinta del concepto de combate (hecho violento) y maniobra táctica.

11.002. Seguridad de las operaciones. La **seguridad** en las operaciones tácticas se logrará mediante la adopción de un conjunto de medidas relacionadas con el cumplimiento de la misión, la adopción de dispositivos, la organización de los elementos y la observancia de las medidas de control. Dichas medidas tenderán fundamentalmente, a proteger el poder de combate y/o instalaciones de una fuerza, brindando tiempo y espacio para demorar y/o neutralizar cualquier tipo de agresión y, en forma simultánea, posibilitar la reacción del propio elemento.

Asimismo, la ejecución de **medidas de seguridad de contrainteligencia** contribuirá al cumplimiento de la misión en las operaciones tácticas, proporcionando el conocimiento sobre la capacidad de inteligencia del enemigo en forma integral, asesorando sobre las medidas de seguridad a implementar en las operaciones y proponiendo la ejecución de las actividades de contrainteligencia necesarias.

11.003. Alcance de la aplicación de las medidas de seguridad de contrainteligencia. Las medidas de seguridad de contrainteligencia en operaciones tácticas comprende al conjunto de medidas referidas a la seguridad de personal, física de las instalaciones, de documentación y material clasificado, a las comunicaciones, a la informática y a la seguridad criptográfica con la particularidad de tener que preverse y aplicarse en el desarrollo de operaciones tácticas.

Además de las medidas de seguridad de contrainteligencia deberán considerarse otras acciones y procedimientos que, sin ser específicamente de Contrainteligencia, contribuirán al planeamiento y ejecución de la necesaria protección del Instrumento Militar.

Estas medidas o acciones que se considerarán complementarias son:

- a. Protección de la población. Consistirá en llevar a cabo medidas de seguridad que permitan proteger a la población civil de las operaciones militares propias o del oponente. Para lograr este cometido, se deberán instrumentar acciones que posibiliten identificar a la población civil diferenciándola del Instrumento Militar propio o enemigo y restringir sus desplazamientos evitando que se vean en riesgo o bajo amenaza en aquellas zonas donde se desarrollan o prevé el desarrollo de operaciones militares. La implementación de esta medida recaerá en los organismos estatales competentes, pudiendo quedar bajo responsabilidad del comandante del TO en caso de que la situación así lo imponga. Dentro del TO se deberá emplear, en la medida de lo posible, las fuerzas de seguridad o policiales agregadas, asignadas o puestas en apoyo del instrumento militar.
- b. Tratamiento de los prisioneros de guerra. Esta actividad se deberá llevar a cabo conforme al Derecho Internacional para los Conflictos Armados (DICA) y siguiendo todo otro protocolo y convenio internacional firmado por la Nación.

- c. Restricción y/o control de la información. Durante el desarrollo de operaciones militares habrá información acerca de las operaciones y recursos militares, de infraestructura de interés nacional y la propia población que deberá ser protegida de las acciones del oponente real. En este sentido, será necesario instrumentar una serie de acciones y protocolos que permita restringir el conocimiento de determinados temas que, diseminados en forma indebida y/o inoportuna, ponga en riesgo a la población y al Instrumento Militar designado para responder a aquellos actores que amenazan a los intereses nacionales establecidos en la Constitución Nacional. Esta actividad deberá responder a normativas debidamente aprobadas por los poderes estatales competentes en la materia y considerando cuidadosamente el período por el cual se extenderá. Asimismo, quienes deban instrumentar estos protocolos y procedimientos deberán contar con los recursos materiales necesarios y los medios humanos debidamente adiestrados.
- d. Control de zonas militares. Será una parte del territorio nacional, enclavada en la zona del interior que, en razón de su carácter e importancia desde el punto de vista de la defensa nacional, deberá estar sometida a la jurisdicción de la autoridad militar (ROB-00-01 – “Conducción para el Instrumento Militar”). Son aquellos espacios a ser protegidos de manera particular por el interés que representan para la Defensa y para la Nación, fuera de los TTOO. Será común asignar esta categoría a determinadas áreas, a los efectos de proporcionar la necesaria seguridad a la información o material clasificado y al personal muy importante o con funciones críticas, que en ellas se hallen. La constitución de toda zona militar deberá ser declarada por el Poder Ejecutivo Nacional y se deberá consignar taxativamente las atribuciones conferidas a la autoridad militar que allí se desenvuelva.
- e. Evacuación de zonas. Será aquel procedimiento que buscará proteger a la población de los efectos de las operaciones militares que se desarrollen. Esta medida será una responsabilidad de las autoridades estatales o podrá ser delegada al comandante del TO. Esta medida podrá adoptarse con el objeto de posibilitar las acciones militares necesarias, en el marco de los objetivos de nivel estratégicos que se hallan establecidos.
- f. Cooperación cívica – militar. Son aquellos recursos y acuerdos en que se apoya la mutua cooperación entre el comandante de un TO, las autoridades estatales, organizaciones no gubernamentales (nacionales e internacionales) y la población con el objeto de contribuir a proteger, preservar y sostener la vida de la población, el esfuerzo bélico y los otros recursos de la Nación que pudieran resultar vitales. Esta cooperación deberá establecerse a partir de normativas jurídicas y la responsabilidad recaerá en las más altas autoridades del Estado y, por delegación, en los organismos e instituciones involucradas.

11.004. Responsabilidades. La responsabilidad del planeamiento y ejecución de las medidas de seguridad de contrainteligencia recaerá, como responsabilidad de comando, en el comandante, director o jefe del elemento u organismo.

Durante el planeamiento, ejecución y supervisión de estas medidas, el comandante o jefe contará con la asistencia y asesoramiento del órgano de dirección del EM / PI My orgánico y con los órganos de ejecución propios y de los elementos de inteligencia orgánicos, agregados o en apoyo.

En este sentido, los elementos de inteligencia orientarán su apoyo para alcanzar el conocimiento acerca de las principales características de las Fuerzas del oponente, permitir la determinación de sus capacidades, facilitar la adopción de resoluciones sobre las de medidas de seguridad a adoptar y explotar sus debilidades.

SECCIÓN II

PLANEAMIENTO

11.005. Conceptos básicos. Independientemente de lo especificado en los distintos reglamentos operativos, deberá tenerse en cuenta, que el proceso para proporcionar una adecuada seguridad, incluirá una continua planificación, obtención de información, análisis de la información reunida, elaboración de informes y puesta en ejecución de las órdenes y directivas que se impartieren.

Tal como sucede con todas las tareas de planeamiento que se llevan a cabo en la Fuerza, el proceso de planificación que guiará la aplicación de las medidas de seguridad en las operaciones tácticas será el prescripto en el reglamento “Organización y Funcionamiento de los Estados Mayores” (ROD-71 – 01).

Consecuentemente, existirán en el método a aplicar fases, etapas y pasos que se deberán desarrollar con algunas consideraciones particulares para el caso de las medidas de seguridad de las operaciones, por tratarse de un aspecto específico comprendido por las medidas de seguridad de contrainteligencia y correspondiente al campo de la inteligencia.

11.006. Fase preliminar. Se deberá tener especialmente en cuenta que la continuidad y necesidad de anticipación que particulariza el trabajo de inteligencia, hará difícil determinar con precisión la oportunidad del inicio de las actividades de planeamiento para el oficial de inteligencia y su equipo de trabajo.

Normalmente, el inicio estará dado por una apreciación de inteligencia preliminar ("Inteligencia Táctica" – ROD-11-01, Cap VIII, Art. 8.002., b., 1er párrafo del cuadro y 1) d)).

Es importante destacar que la adopción de las medidas de seguridad de contrainteligencia estará presente en todos los pasos que relacionan el planeamiento general (PPC) con el planeamiento específico de inteligencia. Ambos procesos deberán estar integrados y se desarrollarán en forma paralela retroalimentándose.

Además, será precisamente a partir de los primeros momentos de la concepción de la operación, que el mantenimiento del secreto sobre la misma alcanza una importancia vital para negarle al enemigo la posibilidad de accionar o reaccionar de acuerdo con los planes propios.

11.007. Primera etapa del PPC "Determinación del plan general" (dentro de la fase preliminar)

a. Análisis de la misión por parte del Comandante.

Si el comandante distribuyere en forma anticipada la orden de operaciones del comando superior y se dispusiere de cierto tiempo previo a su orientación, el G-2 / S-2 con sus auxiliares deberán concentrar sus estudios y trabajos, atendiendo los siguientes aspectos:

- 1) Continuar con la carta de situación de medidas de seguridad de contrainteligencia, en la medida que la información disponible lo permita.
- 2) Estudiar el concepto de la operación del comando superior y analizar, a la luz de esto, las medidas de seguridad que se deban aplicar y cuales sean necesarias modificar.
- 3) Estudiar la probable zona de operaciones y las capacidades asignadas por el escalón superior al enemigo, con la finalidad de considerar los posibles requerimientos que el comandante de la GUC podrá formular al G2 para satisfacer sus necesidades de inteligencia, en función del análisis de la misión y su orientación. A partir de las capacidades, deberá establecerse cuales medidas deberán implementarse para oponerse a la acción enemiga.

Al respecto, el comandante podrá llegar a requerirle al oficial de inteligencia, asesoramiento relacionado con la identificación de los probables objetivos enemigos. Para ello, el G-2 / S - 2 deberá tener en cuenta que, si bien en ese nivel es totalmente factible referirse a efectos a alcanzar por parte del enemigo, en el nivel de conducción en el que está situado y apreciando el momento del análisis en que se encuentra, el asesoramiento se referirá, fundamentalmente, a especificar al comandante los probables objetivos materiales del enemigo.

Además, llegado el momento de proporcionar el asesoramiento, el G-2 / S-2 tendrá especialmente en cuenta, aclarar debidamente el grado de conocimiento que posee de la relación objetivo pretendido - capacidad disponible.

b. Reunión de información.

Si bien todo el EM / PI My participará en la reunión de información ordenada por el comandante, o de aquella necesaria para el planeamiento de cada campo de la conducción, el G-2 / S-2 será quien tendrá la responsabilidad primaria de esta actividad. En ese sentido, los resultados de su trabajo de inteligencia preliminar, se verán reflejados en dicho momento. Como ya se señaló, los adecuados estudios y las tareas previas desarrolladas, permitirán al G-2 /S-2 anticiparse a necesidades de Inteligencia que el comandante podrá requerir en este paso del planeamiento.

Mientras el comandante se encuentre preparando su orientación, el G2 / S-2 continuará con sus tareas y estudios preliminares dentro de esa apreciación de inteligencia preliminar. Al respecto, puede destacarse lo siguiente:

A medida que profundice su conocimiento sobre la zona de operaciones, la doctrina del enemigo, su OB y las AIRA (actividades importantes, recientes y actuales) procederá a redactar o actualizar la lista de indicios y, consecuentemente, los planes de obtención, exploración y vigilancia, de Contrainteligencia, etc. Debe quedar claro que ello no significará la culminación de la elaboración de estos planes en esta fase preliminar, pero sí la etapa de iniciación de la confección o actualización de los mismos.

Durante la realización de sus estudios, el oficial de inteligencia no deberá perder de vista que el enemigo estará activo. Por lo tanto, dentro de los estudios que se encuentra desarrollando, también deberá iniciar la consideración de todo lo vinculado con las actividades de Inteligencia del enemigo. Ello le proporcionará bases necesarias para proponer e implementar la adopción de medidas de seguridad inmediatas, para actualizar el plan de contrainteligencia. Esto último también tendrá influencia inmediata sobre las actividades de ejecución de inteligencia que se estuvieren desarrollando.

Finalmente, es necesario remarcar que, desde que el G-2 / S-2 comience su trabajo de análisis, nunca deberá dejar de considerar, que toda información actualizada que reciba relacionada con el enemigo, podrá ser producto de la implementación de un plan de engaño.

Antes de que el comandante imparta su orientación, podrá llegar a requerir una serie de exposiciones preliminares a su EM. En caso de que el G-2 / S-2 debiere exponer, prestará especial atención a que la finalidad de la misma será aquella que fija el reglamento de Organización y Funcionamiento de EEMM:

“...servirán al comandante para conformarle una idea general sobre los factores de éxito que podrá incluir en su orientación posterior...”. En consecuencia, para contribuir a que el comandante determine ciertos factores de éxito, el G-2 / S-2 deberá proporcionarle un cuadro de situación general del enemigo y de la zona de operaciones, poniendo énfasis en aquellos aspectos esenciales que afectan a la operación en un todo o en sus aspectos principales.

c. Orientación del comandante.

Se deberán considerar como aspectos sobresalientes vinculados a la seguridad en las operaciones:

- 1) Las capacidades asignadas al enemigo por el escalón superior
- 2) Los probables objetivos materiales del mismo
- 3) Asesoramiento respecto de algunas MSCI a tener especialmente en cuenta, según los estudios efectuados hasta el momento respecto de la situación que se está viviendo.

Se tendrá en cuenta que el enemigo ya está operando y por ende también realiza actividades de Inteligencia, razón por la cual resultará conveniente adoptar las medidas de seguridad de contrainteligencia necesarias y contemplar como parte de la apreciación de situación de inteligencia, los aspectos correspondientes a las MSCI, por medio de otra apreciación de situación de contrainteligencia a desarrollarse en forma simultánea con aquélla.

Durante este paso del PPC, se deberá prestar atención sobre aquellos requerimientos de seguridad que el comandante fije o sobre los cuales exprese un especial interés para, posteriormente, prever la(s) medida(s) de seguridad correspondiente(s).

d. La misión y análisis de la situación.

Al abocarse y realizar el análisis de la misión particular, el oficial de inteligencia podrá ir vislumbrando cual podría ser la manera en que el enemigo se opondría a la inteligencia propia, ampliando su estudio hacia las probables actividades de inteligencia a través de las cuales este podría afectar seriamente la misión.

Al analizar la situación intentará definir y precisar las capacidades de obtención de información del enemigo y determinar cuales son las necesidades de información esenciales para el enemigo con respecto al terreno, las condiciones meteorológicas y el Instrumento Militar propio, de forma de permitir planificar y ejecutar las medidas para negar información y proteger los propios recursos.

e. Elaboración de las capacidades y de los modos de acción.

Es necesario determinar las capacidades de obtención de información del enemigo y los efectos de las mismas sobre nuestros modos de acción. Además, se estudiará la eficacia de las medidas de seguridad de contrainteligencia ya implementadas, determinando la necesidad o no de adoptar otras medidas adicionales, en particular las relacionadas directamente con las operaciones tácticas.

f. Confrontación.

En la misma y a los efectos de determinar la factibilidad y aceptabilidad definitiva de cada modo de acción tentativo propio, el Of Icia deberá expresar las acciones que el enemigo es capaz de ejecutar en los distintos momentos de la operación a ejecutar. Por lo expresado, deberá enunciar tanto los aspectos que interesen a Inteligencia como aquellos a tener en cuenta desde el punto de vista de las medidas de seguridad durante las operaciones.

g. Proposición (conclusiones). Resolución.

El Of Icia expresará “conclusiones” acerca de:

- 1) Los efectos del terreno, condiciones meteorológicas y otros aspectos particulares de la zona de interés que influirán sobre las propias operaciones.
- 2) La capacidad más probable del enemigo y la capacidad más peligrosa que el mismo podrá adoptar. En este punto, convendrá que enuncie algunas precisiones relacionadas con las medidas de seguridad durante las operaciones a tener en cuenta por los elementos de combate, apoyo de combate y servicios para apoyo de combate, que contribuyan a proteger y asegurar la ejecución de las propias operaciones.
- 3) Las debilidades del enemigo.

11.008. Segunda etapa del PPC “Desarrollo del plan general”

a. Determinación y concreción de las suposiciones.

Una vez que el JEM hubiere fijado las suposiciones que se insertarán en el futuro plan, el G-2 verificará que las mismas se encuentren desarrolladas como EEI e incluidas en el plan de obtención, las que a su vez, podrán dar origen a nuevas medidas de seguridad de contrainteligencia.

b. Recopilación de información.

Reunión de información sobre las fuerzas enemigas y, particularmente, de los sistemas de inteligencia del enemigo que puedan interferir o favorecer directa o indirectamente la operación táctica en desarrollo y la obtención de información en forma indebida o la destrucción recursos humanos o materiales clasificados.

c. Composición de la maniobra táctica.

Si bien ello no será una responsabilidad del G-2 / S-2, éste intervendrá y asesorará sobre todos aquellos aspectos que le sean pertinentes, como por ejemplo, exploración, reconocimientos, seguridad, etc. Todo ello contribuirá a la confección de la matriz para el desarrollo del plan general.

d. Organización de la fuerza.

Propondrá las relaciones de comando y funcionales de los elementos de inteligencia que dispondrá la GUC/GUB.

Tendrá en cuenta que la organización para el combate influirá en la decisión sobre cuáles serán los medios de reunión disponibles de la Fuerza.

e. Asignación de tareas.

El oficial de inteligencia propondrá las tareas a cumplir por los elementos de inteligencia, exploración y vigilancia y de toda aquella organización que por sus funciones y misiones puedan contribuir con la ejecución de las medidas de seguridad de contrainteligencia.

f. Coordinación del plan general.

Para las actividades que afectaren solamente elementos que ejecutarán actividades contenidas en los planes de apoyo, la coordinación quedará registrada, únicamente, en dichos planes.

Cuando se trate de integrar un plan de apoyo (ejemplo: plan de vigilancia de combate) con otras operaciones de apoyo en función de un todo (plan general), el G-2 intervendrá en lo que se refiere a inteligencia, en la confección de la matriz para el desarrollo del plan general.

Relación e integración de los planes de contrainteligencia.

Al finalizar el paso de integración de planes, también habrá concluido la preparación de los documentos de trabajo que emplee el oficial de inteligencia, como por ejemplo el plan de obtención, el plan de contrainteligencia, plan de exploración y vigilancia, etc.

11.009. Tercera etapa del PPC “Elaboración de la orden”. El Oficial de Inteligencia tendrá responsabilidad primaria en la redacción del Anexo Inteligencia a las órdenes y planes, en donde lo relativo a las medidas de seguridad de contrainteligencia se deberá incluir medidas concretas y particularizadas según las características del ambiente operacional.

Para arribar a esta etapa y poder elaborar el documento de contrainteligencia, con los detalles y la solidez suficiente, resulta necesario haber realizado los estudios, según lo permitan el tiempo y los medios disponibles, que hagan posible incorporar en dicha orden o plan las medidas de seguridad que se aprecien como mínimas y apropiadas para brindar una aceptable protección a la operación en curso.

11.010. Cuarta etapa del PPC “Supervisión de la acción”. El oficial de inteligencia deberá desarrollar un programa de control y supervisión que le permita evaluar y verificar el desarrollo de las acciones de Inteligencia y de sus resultados.

Este programa, cuya confección se iniciará durante la coordinación del plan general en la segunda etapa del planeamiento, se apoyará en los planes del campo de inteligencia y en los documentos de trabajo confeccionados por el oficial de inteligencia. En ellos determinará los objetivos o metas que deberán reflejar la inteligencia y contrainteligencia requerida por el comandante o jefe, para el cumplimiento de la misión.

El programa de control permitirá detectar la desviación en oportunidad para su corrección, tener prevista medidas correctivas aptas, factibles y aceptables en función de la situación en desarrollo y, de esta forma, negar o disminuir la acción del enemigo y sus sistemas de Inteligencia sobre el propio instrumento militar.

Este programa exigirá contar con un mínimo de medios y de autoridad para poder desarrollarlo.

11.011. Dirección. El reglamento “Organización y Funcionamiento de los Estados Mayores” (ROD-71-01) define a la dirección como la actividad básica de la conducción, por la cual se guiarán los medios a disposición, según los planes en ejecución, asegurando juiciosa, metódica y racionalmente, los sucesivos pasos previstos, dentro de las alternativas posibles, para el cumplimiento de la misión.

El oficial de inteligencia no tendrá autoridad de comando. Impartirá órdenes en nombre del comandante o jefe, de acuerdo con las normas que éste hubiere establecido.

Los miembros del EM / PI My, adecuadamente orientados, podrán adoptar decisiones dentro del grado de autoridad delegado por el comandante o jefe, aliviando su actividad y relevándolo de las decisiones menores.

Dada las características de las actividades del oficial de inteligencia, la impartición de las órdenes deberá ser coordinada con el oficial de operaciones.

Entre las órdenes sobre las que el oficial de inteligencia tendrá incumbencia, se mencionan aquellas que hayan recibido los medios cuyas funciones, actividades y tareas se relacionan, directa o indirectamente, con las necesidades de inteligencia y contrainteligencia para satisfacer las necesidades del comandante o jefe y el cumplimiento de la misión. A modo de ejemplo, se puede mencionar:

- a. La impartición de órdenes relativas a las medidas de seguridad de contrainteligencia, con énfasis en aquellas de carácter táctico.
- b. Órdenes relativas al tratamiento de los PPGG.
- c. Restricción y/o control de la información que permita brindar seguridad.
- d. Ejecución del plan de medidas de seguridad de contrainteligencia.

11.012. Secuencia para la determinación y aplicación de las medidas de seguridad en las operaciones. Con el objeto de operativizar el planeamiento y establecer una secuencia para la determinación y aplicación de las medidas de seguridad en las operaciones, y considerando la necesidad de subdividir el proceso en pasos relacionados al método de planeamiento general, se establece la siguiente integración:

Fase preliminar	<p><u>Primer paso.</u> Identificar la amenaza de obtención de información, por parte de los sistemas y elementos de Inteligencia del enemigo.</p> <p>La información específica necesaria incluirá los elementos de Inteligencia del enemigo, dirigidos contra la propia Fuerza, entre otros:</p> <ul style="list-style-type: none"> - Unidades (subunidades) de Inteligencia del enemigo. - Misiones de dichos elementos. - Despliegue táctico (método de despliegue para cumplir su misión). - Capacidades de dichos elementos. - Procedimientos utilizados para la transmisión de la información. - Tiempo de reacción. - Debilidades de los elementos de Inteligencia del enemigo. <p>El despliegue de los medios de Inteligencia del enemigo deberá materializarse en calcos sobre la carta. A medida que los propios medios confirmen las ubicaciones de los mismos, los calcos deberán actualizarse. Estos calcos serán utilizados para ubicar los elementos de la propia Fuerza, de acuerdo con los planes previstos.</p> <p>La información sobre los medios de reunión del enemigo se obtendrá de los escalones superiores y de los informes que se recibieren de los escalones en contacto con el enemigo.</p>
<p>1ra Etapa "Determinación del plan preliminar".</p> <ul style="list-style-type: none"> - Análisis de la misión por parte del comandante. - Reunión de información. - Orientación del comandante. 	<p><u>Segundo paso.</u> Identificar los perfiles de la propia Fuerza y recomendar los Elementos Esenciales de Información relacionados con las MSCI.</p> <p>Comprenderá la identificación de las partes componentes de diagramas de perfiles y esquemas (procedimientos normales). Será un proceso conjunto de los oficiales de inteligencia y operaciones.</p> <p>1) Diagramas. Los diagramas (señales) son la característica distintiva de una unidad, que resultan de la presencia de la misma, en la zona de operaciones. Los diagramas se dividen en:</p> <ul style="list-style-type: none"> - Imágenes (visual, foto, infrarroja). - Electromagnética. - Acústica. <p>Las señales se detectan debido a que las diferentes unidades tienen distintos equipos, dimensiones diferenciadas, sus señales electromagnéticas son diferentes, producen ruidos distintos y olores asociados con ellos. La detección de dichas señales podrá ser utilizada por los analistas enemigos, para ubicar unidades, determinar actividades, etc.</p>

	<p>2) Esquemas. Serán acciones que habitualmente ocurrirán ante una serie dada de circunstancias. Estas se basarán en el concepto de la operación de las órdenes de operaciones, procedimientos operativos normales, además de la manera en que las unidades en consideración, han cumplido tradicionalmente, con una misión determinada.</p> <p>Estos esquemas ocurrirán para casi todos los tipos de operación, ya que los mismos ayudarán a las unidades, a conducir una operación determinada, con un mínimo grado de dificultad. Los esquemas y señales no son básicamente malos, a menos que revelen un EEIP (elemento esencial de inteligencia propio) o proporcionen al enemigo, un indicio que le permita descubrir un EEIP.</p> <p>3) Perfiles. El siguiente es un procedimiento para la determinación de un perfil de la propia fuerza.</p> <p>a) Obtener la organización de las tareas determinadas en el planeamiento y dividir cada una de las unidades mayores, en la organización de las tareas (R1, R2, R3, Art, B Com, etc.), en los siguientes aspectos: inteligencia, operaciones, comando y comunicaciones, apoyo logístico y administrativo.</p> <p>b) Determinar la señal física y electrónica de las unidades más importantes, en cada una de las áreas mencionadas. Estas señales son desarrolladas a partir de fichas de despliegue histórico, manuales de doctrina, etc.</p> <p>c) Se compilarán los perfiles de unidades individuales, para desarrollar el perfil de la unidad mayor. Por ejemplo, el perfil de una brigada incluirá todos los perfiles de unidades, dentro de la zona de responsabilidad de la GUC, más las señales de aquellas que concurrirán para apoyar la operación. El perfil de la Brigada permitirá determinar exactamente, qué unidades están haciendo qué, dónde y cuándo.</p> <p>d) Este perfil deberá ser analizado en profundidad y deberán mostrar las interrelaciones de comando, apoyo y maniobra. Esta interrelación es crítica debido a que las señales y esquemas de un Regimiento, en forma individual, pueden poner en evidencia un EEIP (por ejemplo, la ubicación de su posición defensiva inicial), sin embargo, podrá indicar como está apoyado por elementos de ingenieros, logísticos, etc.).</p> <p>e) Los perfiles se examinarán para ver cómo se relacionan con la misión y concepto de la operación, cuál será el que podrá poner en evidencia información crítica, para el éxito de la operación.</p> <p>f) El oficial de operaciones y de inteligencia desarrollan el EEIP, basados en el concepto de la operación, la orientación del comandante sobre lo que él piensa, que es esencial para el éxito de la operación, los estudios del estado mayor, las evaluaciones de debilidades y los análisis de riesgos.</p> <p>Estos EEIP demostrarán cuáles perfiles e indicadores específicos deberán ser examinados, para adoptar las medidas de seguridad correspondientes</p>
<p>1ra Etapa "Determinación del plan preliminar".</p> <p>- La misión y análisis de la situación.</p>	<p><u>Tercer paso.</u> Identificar las debilidades de la propia fuerza.</p> <p>Las debilidades son aquellos perfiles que descubren indicios de procedimientos operativos o de planeamiento de la unidad, los cuales, a menos que se pongan en ejecución medidas de seguridad, serán detectados por medios de reunión del enemigo. Si fuera reunida esta información, podría comprometer el EEIP de la unidad, poniendo en peligro el éxito de la operación. Las debilidades podrán incluir cualquier actividad llevada a cabo, por una unidad militar.</p> <p>1) Las vulnerabilidades se determinarán comparando el perfil de la propia fuerza, con la amenaza de las actividades de reunión del enemigo.</p> <p>2) Existirá una vulnerabilidad, cuando el enemigo tuviere la capacidad de reunir información sobre nuestras fuerzas (fecha, hora, ubicación y tipo de unidad)</p>

	<p>o actividad) y procesar la información a tiempo, para reaccionar de modo tal, que pudiese afectar el resultado de la operación.</p> <p>Las unidades podrán ser vulnerables, sólo si el enemigo pudiese obtener ubicaciones precisas. Aquí, es donde el proceso de la información y el tiempo de reacción entran en juego. Aunque el enemigo reúna información precisa, si le llevare tres horas procesarla y la propia tropa se hubiere movido, no existirán vulnerabilidades.</p> <p>3) Como una ayuda a esta evaluación de vulnerabilidad, las técnicas de la apreciación gráfica de inteligencia se aplican a esquemas y señales de la propia fuerza, por lo que nos podemos ver a nosotros mismos, como nos verían los sistemas de reunión de enemigos.</p> <p>Por ejemplo, utilizando lo determinado en los pasos 1 y 2, que muestran las ubicaciones de las unidades de la propia fuerza y la ubicación y capacidades de los elementos de reunión del enemigo, cada perfil propio puede compararse a la amenaza.</p> <p>Cuando este proceso se completa, existe un listado inicial de vulnerabilidades. Luego, el analista debe identificar, dónde, cuándo y con qué, el enemigo tendrá la capacidad de reunir información, sobre los indicadores identificados. Cada vulnerabilidad estará listada con la amenaza específica, para ayudar al analista en el listado de vulnerabilidades y su posterior uso, durante el análisis de riesgo.</p> <p>Agregada a esta lista, irá una evaluación de la credibilidad de la fuente de información (para el enemigo) y un listado de cada vulnerabilidad, de acuerdo con su importancia para el éxito de la operación y la susceptibilidad para la reunión (número, tipo y validez de los medios de reunión enemigos, enfrentados a cada vulnerabilidad).</p>
<p>1ra Etapa "Determinación del plan preliminar".</p> <ul style="list-style-type: none"> - Elaboración de las capacidades y de los MMAA. - Confrontación. 	<p><u>Cuarto paso.</u> Análisis de riesgo y selección del EEIP.</p> <ol style="list-style-type: none"> 1) El análisis de riesgo es el proceso mediante el cual, se determinarán los riesgos de las operaciones, cuando no se aplicaren medidas de seguridad para proteger las vulnerabilidades propias de las actividades de obtención de información, por parte del enemigo y la comparación de estos riesgos, con el costo de poner en ejecución las medidas de seguridad (en términos de tiempo, equipo, fondos y/o efectivos militares) y su probable efectividad. 2) Cada vulnerabilidad enumerada en la lista del paso anterior se examinará, para determinar el posible impacto de la obtención de información enemiga, en el resultado de la operación. Las pérdidas potenciales de tiempo, equipo y efectivos serán consideradas. 3) Para determinar el factor de riesgo, se considerarán las actividades normales, así como las acciones pasadas y la doctrina enemiga. Los riesgos asociados a cada vulnerabilidad, se agregarán a la lista. 4) Los costos de poner en ejecución varias medidas de seguridad, se compararán con los beneficios (en término de reducción de riesgos) que pudieren dar. 5) El resultado del análisis de riesgo incluye la selección por parte del oficial de operaciones de aquellos EEIP, que fueren lo suficientemente críticos, como para garantizar la aplicación de medidas de seguridad. 6) Un aspecto esencial de este análisis será la identificación del EEIP crítico, que no podrá ser protegido por contramedidas, a fin de asesorar sobre la conveniencia de realizar operaciones de engaño. 7) En este paso, se realizarán los estudios necesarios para reducir la lista de EEIP establecidos en el segundo paso. Los EEIP deberán limitarse a aquellos aspectos críticos de la operación, que deberán protegerse para asegurar el éxito de la misión.

<p>1ra Etapa "Determinación del plan preliminar".</p> <p>- Proposición (conclusiones). Resolución.</p>	<p><u>Quinto paso.</u> Proposición de medidas de seguridad.</p> <ol style="list-style-type: none"> 1) Basado en la información obtenida en el paso anterior, el oficial de inteligencia propondrá las medidas de seguridad al oficial de operaciones, con el propósito de reducir las vulnerabilidades. 2) Las medidas de seguridad variarán de acuerdo con la situación, la importancia del EEIP, así como la eficacia de las medidas a adoptar. 3) Las medidas de seguridad podrán dividirse, en las siguientes categorías: <ol style="list-style-type: none"> a) Medidas de contra-vigilancia. Son utilizadas para prevenir las actividades de observación del enemigo sobre las propias operaciones. Incluyen entre otras, al enmascaramiento, las actividades de patrullas, las técnicas de operaciones electrónicas, etc. b) Contra medidas. Son todas aquellas acciones tomadas para anular el sistema de reunión de información. Las contramedidas emplean dispositivos o técnicas, con el objetivo de dañar la eficacia de las actividades de detención del enemigo. c) Engaño. Este se prepara para confundir al enemigo, mediante la manipulación, distorsión o falsificación de la información, obligándole a actuar de tal forma, que resulte perjudicial para sus intereses. 4) Para asesorar al oficial de operaciones y al comandante, el oficial de inteligencia presentará las proposiciones sobre las medidas de seguridad que debieran adoptarse, para neutralizar las vulnerabilidades propias.
<p>2da Etapa "Desarrollo del plan general" y 3ra Etapa "Elaboración de la orden".</p>	<p>f. <u>Sexto paso.</u> Selección de las medidas de seguridad.</p> <ol style="list-style-type: none"> 1) La selección de las medidas de seguridad se basará en su eficacia para ocultar el EEIP, ala actividad de obtención del enemigo. El problema será competencia del oficial de operaciones. Generalmente, existen cinco opciones, para quien debe tomar la decisión. <ul style="list-style-type: none"> - No se necesitan medidas de seguridad (se acepta el riesgo de la detección). - Se aplican una o más de las medidas de seguridad. - Se detiene la actividad. - Se utiliza el engaño. - Se cambia la operación. 2) La no selección de medidas de seguridad deberá estar basada en: <ul style="list-style-type: none"> - Si fuere detectada, la actividad soportará el plan de engaño. - El comandante desea aceptar los riesgos relacionados con la detección, por parte del enemigo. 3) Las medidas de seguridad de contrainteligencia estarán volcadas en un documento específico de contrainteligencia, de una orden de operaciones.
<p>4ta Etapa "Supervisión de la acción".</p>	<p><u>Séptimo paso.</u> Puesta en ejecución de las medidas de seguridad.</p> <ol style="list-style-type: none"> 1) Determinadas las medidas de seguridad a adoptarse, el oficial de operaciones establecerá qué elementos deberán utilizarse, para su implementación. 2) La decisión se basará en el tipo de medida, los recursos disponibles y la misión de cada elemento. Una apropiada aplicación de las mismas, permitirá que se desarrollen las actividades esenciales, al mismo tiempo que se reducen las probabilidades, para que el enemigo pudiese detectar las actividades o interpretar correctamente su significado. 3) El oficial de operaciones deberá considerar siempre, la destrucción de las capacidades de obtención de información del enemigo, como una contramedida importante. <p><u>Octavo paso.</u> Control de la implementación de las medidas y su evaluación.</p>

	<p>1) Este paso se controlará el cumplimiento de las MSCI implementadas e intentará evaluar el éxito de las mismas. El personal designado controlará que las medidas de seguridad de contrainteligencia se cumplan de acuerdo al plan de contrainteligencia ordenado y evaluará si las mismas han sido efectivas. Esta efectividad será evaluada en términos de la protección que la medida diere al EEI.</p> <p>Podrá variar desde el control de una sola medida (control del enmascaramiento de un elemento), por un miembro del comando, hasta la constitución de equipos de expertos.</p> <p>2) Durante la selección de prisioneros de guerra enemigos y refugiados, el personal de contrainteligencia determinará los requerimientos de la inteligencia enemiga y verificará la efectividad de las medidas de seguridad.</p> <p>3) Si cualquier acción indicare un posible compromiso de información esencial, los datos deberá ser informados al oficial de inteligencia, para el análisis de la información descubierta y los riesgos a los que podría estar sometido el comando.</p> <p>Ejemplo de datos que deberán ser informados:</p> <ul style="list-style-type: none"> a) Divulgación de EEI. b) Violaciones de procedimientos de seguridad establecidos. c) Indicios de que el enemigo tuviere conocimientos anteriores, de una operación propia. <p><u>Noveno paso.</u> Propositiones para reajustar las medidas de seguridad.</p> <p>1) Basados en los resultados del paso anterior, el personal de operaciones y de inteligencia, en forma conjunta, realizarán ajustes a las medidas de seguridad en ejecución.</p> <p>2) Cuando fuere necesario, se propondrán nuevos EEI y cambios de las medidas de seguridad.</p> <p>3) Los informes posteriores a las operaciones, se realizarán para permitir el análisis de las medidas de seguridad y determinar los cambios necesarios, para mejorar la seguridad del comando y del elemento.</p> <p>4) Las prácticas de planeamiento de medidas de seguridad serán realizadas, para asegurar que una planificación futura considere las debilidades presentes, al desarrollar las medidas de seguridad para operaciones.</p>
--	---

SECCION III

EVALUACIONES DE SEGURIDAD EN ACTIVIDADES EN CAMPAÑA

11.013. Conceptos básicos. La evaluación de seguridad es un control de la efectividad de las medidas de seguridad en vigor. Esta evaluación puede dar lugar a la modificación o a la supresión de las medidas en aplicación o a la puesta en vigencia de otras.

Los métodos de evaluación serán seleccionados y aplicados, dependiendo de las misiones del elemento, de las disponibilidades de personal y de la vulnerabilidad anticipada a los esfuerzos de reunión del sistema y los elementos de Inteligencia del enemigo.

11.014. Objeto de las evaluaciones. Será determinar el éxito, fracaso o falta de medidas de seguridad, aplicadas a una operación o actividad en campaña. Todas estarán diseñadas para proporcionar información completa y exacta, sobre cómo se están aplicando las medidas de seguridad. En operaciones, se buscará identificar debilidades y amenazas, las evaluaciones se realizarán en respuesta a objetivos inmediatos.

11.015. Fases de la evaluación. Cada evaluación será única, dado que cada una reflejará la operación o actividad que estará siendo evaluada y analizada. Sin embargo, existen ciertos procedimientos comunes a todas las evaluaciones. Estos procedimientos comunes dividen una evaluación, en tres fases identificables. PLANEAMIENTO - EVALUACION EN EL TERRENO -INFORMES A ELEVAR.

11.016. Planeamiento. Este dependerá de la naturaleza y complejidad de la operación o actividad a ser evaluada; normalmente, las acciones de planeamiento incluyen:

- a. Determinación del propósito de la evaluación.
- b. Selección de los equipos de evaluación.
- c. Reunión de antecedentes.
- d. Revisión de los EEIP.
- e. Inteligencia disponible sobre los medios de reunión del enemigo.
- f. Conocimiento de la operación o actividad a ser evaluada.
- g. Desarrollo de esquemas funcionales.
- h. Anuncio de la evaluación.

Un paso importante durante la fase de planificación será la reunión de datos necesarios, para obtener un conocimiento lo más amplio posible del elemento a evaluar. Esta reunión de datos se llevará a cabo, a través de una revisión de las directivas, PON(s) y planes que tuvieran relación con el elemento y sus actividades.

Esta revisión familiarizará al equipo con la misión, el objetivo y los procedimientos operativos de la unidad y otros elementos con los cuales pudiere estar conectado funcionalmente. Como mínimo, deberán obtenerse los siguientes tipos de documentos e información:

- a. Conocimiento de la misión. Proporcionará una visión, sobre la razón de ser del elemento y la importancia de todos sus planes. También podrá proporcionar información sobre otras unidades, planes o programas, que dependieren de la unidad evaluada para apoyo.
- b. Planes del elemento. Estos especificarán el propósito y los objetivos de los diversos procedimientos en la unidad y generalmente, contendrán cursos de acción prescriptos para contingencias dadas. El estudio de estos documentos familiarizará al equipo de evaluación, con el carácter general de la unidad y sus operaciones.
- c. Datos orgánicos. Estos identificarán al personal considerado clave en la organización y mostrará relaciones de comando y comunicaciones, que se establecerán entre los diversos elementos de la unidad en cuestión. Del estudio de la misma, surgirá cuáles de esos elementos serán los más rentables, como blanco de los elementos de reunión del enemigo.
- d. Listado de los EEIP. Una inspección de la lista de los EEIP del propio elemento identificará aquellos aspectos de valor de Inteligencia, que el comandante o jefe considere de significativa importancia, para la seguridad.
- e. Conocimiento sobre los medios de Inteligencia del enemigo.

Deberán obtenerse datos sobre:

- 1) Actividades de los medios de reunión del enemigo, en el área a evaluarse.
- 2) Capacidades de observación.
- 3) Capacidades de espionaje.
- 4) Capacidad de explotación de fuentes abiertas.
- 5) Capacidades del enemigo de reunión de información por radar y comunicaciones.

6) Sistemas móviles tales como satélites, camiones, aviones, barcos, Etc.

- f. Conocimiento de la operación o de la actividad a evaluar. Requiere una revisión de los planes de operaciones y otras directivas que tengan relación con la operación o actividad. Los miembros del equipo de evaluación revisarán la misión, el concepto de la operación, objetivos, estructura de la organización y relaciones de comando.

La confección de una lista de verificación proporciona a los miembros del equipo evaluación, una herramienta básica. Las listas de verificación son generales y muchos aspectos serán agregados, como resultado de las entrevistas realizadas en el terreno y de la observación; deberá especificarse la ubicación de cada miembro del equipo, el personal que ha de ser entrevistado, procedimientos a ser controlados y los tipos de datos que deberán reunirse.

El paso final de la fase planificación será el anuncio a los interesados, que el oficial de operaciones remitirá a los jefes de elementos, especificando:

- 1) Propósito y alcance de la evaluación.
- 2) Miembros del equipo y autorizaciones.
- 3) Informaciones requeridas.
- 4) Tiempo de evaluación.
- 5) Apoyo administrativo requerido.
- 6) Apoyo de comunicaciones.

11.017. Evaluación en el terreno. Comprende, en general, un informe inicial, instrucciones del comando del elemento u organismo evaluado, evaluación propiamente dicha y un informe final. Durante el desarrollo de operaciones tácticas, se llevan a cabo los informes e instrucciones, si la situación lo permitiere.

- a. Informe inicial. Puede ser formal o informal y será presentado por el jefe de equipo. Contendrá:

- 1) Objetivo y alcance de la evaluación.
- 2) Dirección de la evaluación.
- 3) Resumen de la evaluación de las capacidades del enemigo y de las vulnerabilidades propias. En las situaciones tácticas, se reciben comentarios del personal del elemento u organismo evaluado, para actualizar la situación.
- 4) Evaluaciones previas sobre la seguridad, si así correspondiere.

- b. Instrucciones del comando. Le permitirá al equipo de evaluación tener una idea general de la operación, desde el punto de vista del elemento u organismo.

- c. Evaluación. Durante la evaluación propiamente dicha, se reunirán datos a través de la observación de actividades, reunión de documentos y entrevistas personales. La obtención de datos es la parte fundamental de la etapa de evaluación en el terreno. La selección de los tipos de datos a reunir, dependerá del o de los tipos de amenaza a los cuales, el comando apoyado, se sabe o se supone que estará expuesto.

A modo de ejemplo, se presenta una guía para las actividades de reunión de datos, según se refiera a cada uno de los tipos básicos de amenaza.

- 1) Contra amenazas de personas.
 - a) Plan de seguridad.
 - b) Planes de emergencia.
 - c) Normas para el acceso a la documentación.
 - d) Programas de educación de medidas de seguridad de contrainteligencia.

- e) Procedimientos para la guarda de la documentación clasificada.
 - f) Procedimientos para la identificación del personal, control de los movimientos.
 - g) Sistemas de iluminación y de alarma.
 - h) Barreras.
 - i) Medidas especiales para la protección de equipos e instalaciones críticas.
- 2) Contra la amenaza de comunicaciones y de electrónica.
- a) De acuerdo con lo establecido, en el reglamento "Conducción de Comunicaciones".
- 3) Contra la amenaza de equipos que captan imágenes.
- a) Control de los equipos fotográficos no autorizados.
 - b) Medidas para evitar la penetración (infiltración óptica).
 - c) Uso correcto del enmascaramiento.
 - d) Uso innecesario de signos de guías y otros aspectos, que proporcionarán información.
 - e) Procedimientos para el encubrimiento de las marcas de equipos.
 - f) Medidas para evitar fotografías infrarrojas.
 - g) Almacenamiento al aire libre, de equipos especiales y abastecimientos.

La observación verificará el suceso, la secuencia y el momento oportuno de los hechos, durante una operación. Las entrevistas agregan elementos adicionales de información, indispensables para completar la interpretación. Las listas de control deben revisarse antes y después de las entrevistas, para confirmar si se han cubierto todos los puntos correspondientes.

La información específica sobre cómo, cuándo y dónde la gente cumple con sus tareas y cómo se relacionan estas tareas, con la secuencia observada y planificada de los hechos, se registrará, a fin de documentar las actividades, en una secuencia lógica. Los hechos registrados durante o inmediatamente después de la entrevista, generalmente incluirán:

- a. Identificación y objetivo de la entrevista.
- b. Descripción de la posición ocupada por la persona que es entrevistada.
- c. Detalles de cómo, cuándo, dónde y qué tareas realiza el individuo (operativas y de seguridad).
- d. Si sus actividades reflejan el conocimiento de la amenaza de reunión de los medios de Inteligencia del enemigo.

Cada uno de los miembros del equipo deberá estar familiarizado con las listas de verificación, utilizados por los otros integrantes y deberá estar alerta a la información que pudiere afectarlos. A medida que se acumulen datos, mediante observación y entrevistas, su incorporación al perfil funcional básico, cambiará la lista original de los eventos, proyectados en una lista de hechos reales.

Las ideas originales se transformarán ahora en un registro cronológico de todo cuanto hubiere sucedido en realidad: dónde, quién, cómo y por qué fue hecho. Este cuadro, también deberá reflejar una evaluación de la vulnerabilidad de cada evento, a la amenaza de los medios de inteligencia enemigos, conocidos o supuestos.

A medida que se continúa con la reunión de datos, comenzará a surgir información provisional; la misma deberá ser confirmada y documentada en todo lo posible; si se considerare importante, deberá darse a conocer, al comandante o jefe responsable de la operación, para que se adoptaren las medidas correctivas.

Dadas las características de las operaciones o la magnitud del elemento u organismo a evaluar, el método más apropiado para determinar cómo emplear el equipo de evaluación, será la reunión diaria del jefe del equipo con todos sus integrantes, para evaluar el progreso, comparar los datos y coordinar la dirección de la evaluación.

La comparación de los datos dará lugar a nuevas directivas de investigación y requerimientos sobre su obtención, suministrando pautas de corto plazo, para el empleo del equipo.

La duración de la etapa de evaluación en el terreno, se establecerá en la fase de planeamiento; su duración exacta dependerá de la situación táctica y de la rapidez con que se obtuvieren los datos de evaluación.

El análisis de las medidas de seguridad será un procedimiento para identificar las debilidades en la protección de los EEIP; el resultado final del proceso de análisis será la identificación de las vulnerabilidades en la seguridad del comando analizado.

Una vez finalizado el proceso de análisis, se sacarán las conclusiones, en cuanto a los aspectos de las medidas de seguridad que se consideraren débiles y los procedimientos vulnerables a las actividades de Inteligencia del enemigo. Estas estarán incluidas, en el informe final, conjuntamente con las proposiciones para eliminarlas totalmente o minimizarlas.

Cada debilidad, seleccionada para incluir en el informe final, deberá estar relacionada con la amenaza e identificada claramente.

Las proposiciones que acompañan a cada una de las mismas deberán tener en consideración la factibilidad y el costo de implementación, la dificultad de la misión del comando y el grado de riesgo presentado a los EEIP en cuestión.

11.018. Informe final. Sin perjuicio de los problemas presentados al comandante o jefe del elemento u organismo evaluado durante el desarrollo de la misma, al término de la evaluación deberá presentarse un informe final. La finalidad del mismo será comunicar los resultados generales y los aspectos más importantes detectados.

- a. Cada miembro del equipo de evaluación obtendrá los datos relacionados con su área en particular. Estos datos serán una cronología, acerca de quién estuviere haciendo qué, dónde y su delimitación en tiempo.
- b. Correlacionando los diagramas operativos separados, comenzará a surgir la cronología de eventos de la operación o actividad en su totalidad.
- c. La finalidad de construir los diagramas funcionales tendrá una adecuada aplicación, si el equipo fuere capaz de:
 - 1) Describir el período dividido en etapas, que surgiere de la operación o actividad.
 - 2) Establecer la manera por la cual los distintos comandos, organizaciones y actividades, interactuarán y cumplirán con su rol, en la operación o actividad.
 - 3) Seguir el flujo de información, a través de las facilidades de comunicaciones.
- d. La descripción cronológica de eventos que tuvieron lugar en la operación o actividad evaluada, suministrará una base para el análisis e identificación, de las debilidades. También podrán identificarse, las fuentes que podrán explotar los medios de reunión del enemigo. Las debilidades y las fuentes se conectarán con la información que pudiere utilizarse para degradar la eficacia de la operación, en la actualidad o en el futuro.

Esto se relacionará directamente con los EEIP, que serán en el verdadero sentido, la información clave que deberá negarse al enemigo y que hubieren sido identificados antes de la evaluación.
- e. Las debilidades serán identificadas, partiendo desde el punto de vista enemigo, con relación a la actividad u operación evaluada.

- f. El equipo de evaluación deberá reconocer la existencia de más de un enemigo y que el descubrimiento por sí solo, no indicará necesariamente una vulnerabilidad. Si el enemigo no tuviere la capacidad de procesar y reaccionar frente a la información, con el tiempo suficiente y de la forma adecuada, para degradar la eficacia de un elemento determinado.

La capacidad del equipo para emitir estos juicios, requerirá un amplio conocimiento del enemigo. Los criterios básicos para identificar una vulnerabilidad, serán la existencia de una amenaza y que la información derivada de la misma, fuere realmente un EEIP.

CAPÍTULO XII

PLANEAMIENTO, SUPERVISIÓN Y CONTROL DE LAS MEDIDAS DE SEGURIDAD DE CONTRAINTELIGENCIA

SECCIÓN I

PLANEAMIENTO DE LAS MSCI

12.001. Aspectos generales. El enfoque para desarrollar las medidas de seguridad de contrainteligencia para los organismos y elementos del Instrumento Militar se basa en un proceso continuo y sistemático que genera un sistema de protección integrado destinado a determinar las previsiones que deberán adoptarse a fin de proteger los recursos de la Fuerza de aquellos actores que representan un riesgo o amenaza a la seguridad.

El planeamiento de las medidas de seguridad de contrainteligencia partirá de la base de una apreciación de situación de contrainteligencia en la cual deberá plasmarse, de la forma más detallada posible, cual es la situación de los propios recursos y cuales son los riesgos y amenazas a la seguridad del Instrumento Militar.

12.002. Planeamiento estratégico militar conjunto y específico. El EMCFFAA es el responsable del planeamiento a nivel estratégico militar, determinando las responsabilidades para los distintos integrantes del Instrumento Militar.

Sobre la base de los documentos de contrainteligencia de nivel estratégico militar, la Fuerza deberá realizar el planeamiento correspondiente y emitir las directivas específicas sobre las medidas de seguridad de contrainteligencia.

12.003. Planeamiento a nivel operacional y táctico. Los comandos deberán efectuar el planeamiento de contrainteligencia, a fin de lograr un nivel de seguridad compatible con sus requerimientos específicos.

Se deberán basar para ello en las directivas, normas o procedimientos operativos normales que reciban del escalón superior, y en las conclusiones extraídas de su propia apreciación de contrainteligencia.

12.004. Recurrencia de los planes. El planeamiento y posterior ejecución de las acciones necesarias para proteger los recursos del Instrumento Militar resulta una actividad compleja y muy amplia. Los planes deberán ser sometidos a una recurrencia dinámica a fin de que las medidas de seguridad que se apliquen resulten eficaces.

12.005. Responsabilidades. Planificar las medidas de seguridad de contrainteligencia es una responsabilidad de todos los niveles de comando, por lo que cada comandante, director o jefe deberá desarrollar las directivas, órdenes, programas y planes que posibiliten lograr un adecuado grado de responsabilidad.

Lo expresado exigirá del comandante, director o jefe adopte las previsiones específicas, en relación con la situación imperante, contemplando los siguientes aspectos:

- a. Adecuación al nivel de seguridad requerido para el elemento, el que será fijado por el escalón superior o en su defecto, establecido por el responsable del mismo, sobre la base de la misión y el contexto imperante.
- b. Análisis previo, en detalle, del plan de medidas de seguridad de contrainteligencia en vigencia y la eficacia de su implementación, respecto a los objetivos previstos, conforme a la legislación vigente.
- c. Determinación de las debilidades existentes en la seguridad de la información y material clasificado, particularmente las deficiencias del planeamiento preexistente.
- d. Verificación de las condiciones para el cumplimiento de las medidas de seguridad de contrainteligencia (medios humanos, posibilidades tecnológicas, etc.).

La planificación de MSCI requerirá del asesoramiento del órgano de inteligencia del nivel que se trate, en su carácter de especialista en la materia.

SECCIÓN II

INFORMACIÓN DOCUMENTADA DE CONTRAINTELIGENCIA

12.006. Conceptos generales. El proceso de planeamiento, ejecución y posterior supervisión y control de las operaciones y actividades de contrainteligencia que desarrolla el Instrumento Militar exige implementar un conjunto de documentos que regulen acciones y plasmen órdenes, directivas y distinta información que posibilite configurar una situación a fin de facilitar la adopción de resoluciones por parte del comandante, director o jefe.

12.007. Apreciación de situación de contrainteligencia. La apreciación de situación de contrainteligencia consistirá en un estudio descriptivo y analítico de las medidas de seguridad de la Fuerza y el ambiente operacional en la que el Instrumento Militar debe desarrollar sus actividades, especialmente, del enemigo u oponente.

La apreciación de situación de contrainteligencia es un procedimiento de trabajo que busca analizar distintos aspectos que conforman la situación, con el objeto de obtener conclusiones acerca de:

- a. La influencia del ambiente operacional en la protección de los recursos propios.
- b. Las capacidades del Instrumento Militar propio a proteger.
- c. Evaluación de las vulnerabilidades y debilidades propias.
- d. Los riesgos y amenazas a la seguridad de la Fuerza.
- e. Las capacidades del enemigo u oponente y la probabilidad de adopción.

La apreciación de situación de contrainteligencia se preparará y mantendrá actualizada en todos los escalones de la Fuerza. Constituirá una responsabilidad del oficial de inteligencia del organismo.

Estará supeditada a numerosas variables. Un cambio importante en cualquiera de ellas impondrá su revisión, a fin de determinar si se mantendrán o no las conclusiones establecidas anteriormente.

Deberá estar en condiciones de exponerse en cualquier momento, dado que el proceso de análisis nunca termina, lo que implicará la necesidad de su permanente actualización.

Esta apreciación constituirá una base de trabajo a partir de la cual se podrán llevar a cabo planes y programas de trabajo.

12.008. Bases de trabajo para el desarrollo de la apreciación de situación de contrainteligencia. Lograr una adecuada apreciación de situación de contrainteligencia requerirá evaluar en detalle y en oportunidad todos los aspectos que, desde el punto de vista de medidas de seguridad de contrainteligencia afectan a la seguridad del Instrumento Militar.

Entre los documentos que servirán de base a la apreciación de situación de contrainteligencia y que deberán ser analizados detalladamente, se deberá considerar:

- a. Estudios de seguridad.
- b. Inspecciones de seguridad.
- c. Informes de inspecciones y supervisiones relacionadas con las MSCI.
- d. Programa de educación del organismo.
- e. Hechos y acciones que afectaron a la seguridad de la Fuerza.
- f. Organización y estructura del enemigo u oponente a fin de determinar las capacidades y vulnerabilidades de sus sistemas de Inteligencia.
- g. Ambiente geográfico.

12.009. Plan de obtención de contrainteligencia. El plan de obtención de contrainteligencia es un documento de trabajo del campo de inteligencia en el cual se materializará la dirección del esfuerzo de obtención, y se confeccionará para coordinar e integrar la actividad de los medios de obtención.

12.010. Plan de medidas de seguridad de contrainteligencia. El plan de medidas de seguridad de contrainteligencia es el documento que permitirá organizar las actividades y tareas referidas a las medidas de seguridad que deberán considerarse, estableciendo:

- a. Medidas de seguridad a enfatizar.
- b. Medidas adicionales que deben adoptarse.
- c. Unidades u organismos que deben implementarlas.
- d. Oportunidad.
- e. Lugar, sector o área.

Constituirá la base fundamental para la preparación de requerimientos de contrainteligencia. Tendrá por finalidad la elaboración por parte del oficial de inteligencia, de un listado completo y detallado de las medidas de seguridad de contrainteligencia necesarias para proporcionar la seguridad de una operación o actividad de los organismos del Instrumento Militar.

Se preparará simultáneamente con el planeamiento de la operación o actividad prevista, e incluirá tanto los aspectos relacionados a fin de obtener un nivel de seguridad adecuado y proporcionar libertad de acción al comandante o jefe. Estas medidas ampliarán o complementarán las incluidas en el PON de contrainteligencia.

Deberá ser detallado y flexible, para lograr un apoyo oportuno de contrainteligencia.

No será un documento de difusión a nivel táctico. Se instrumentará mediante:

- a. El Plan de contrainteligencia a nivel estratégico operacional.
- b. Párrafo 6 del Anexo inteligencia de una orden de operaciones.
- c. Apéndice al Anexo de inteligencia de una orden de operaciones.
- d. Órdenes y requerimientos.
- e. Directivas, órdenes especiales, PON(s), etc.

12.011. Carta de hechos que afectan a la fuerza (desde el punto de vista de las medidas de seguridad de contrainteligencia). Constituirá el registro gráfico georeferenciado de la información relativa a los hechos que afectan a la Fuerza desde el punto de vista de las medidas de seguridad de contrainteligencia.

La finalidad de la carta de situación acerca de los hechos de violaciones a las medidas de seguridad de contrainteligencia que afectan a la Fuerza, será el registro gráfico para facilitar la comprensión de la situación por parte del Cte, Dir o J, mediante una rápida visión de conjunto.

12.012. Carta de situación de ataques cibernéticos. Constituirá el registro gráfico georeferenciado de la información relativa a los lugares, equipos, actores, procedimientos y programas a través de los cuales se ha atacado a los sistemas informáticos propios.

Este tipo de documento deberá desarrollarse a partir de la identificación de este tipo de ataque. Por lo general, se desarrollará en los más altos niveles desde donde se administran las distintas redes que conforman el sistema informático del Ejército.

SECCIÓN III

SUPERVISIÓN DE LAS MEDIDAS DE SEGURIDAD DE CONTRAINTELIGENCIA

12.013. Conceptos generales. Definición. La supervisión de las medidas de seguridad de contrainteligencia es la verificación continua de la evolución de la situación de seguridad, a fin de comprobar si coincide con la prevista, para proponer las modificaciones necesarias.

La supervisión es una responsabilidad de todos los niveles de la conducción, y consistirá en el registro sistemático del funcionamiento de las medidas implementadas en el área de su responsabilidad. Los registros permitirán, a priori, conformar una imagen de la eficacia de la medida que se trate y, a la vez, facilitar la comparación de información cuando se desarrollen los análisis tendientes a conformar estudios de seguridad.

Dado que la aplicación de las medidas se imponen a través de directivas, instrucciones, procedimientos operativos normales, u otros tipos de órdenes, todos ellos deben contemplar la forma de ejecutar los registros compatible con las medidas aplicadas y los responsables intervinientes.

Los registros adoptarán el formato necesario derivado del tipo de tecnología que involucre a la medida o conjunto de ellas que se vinculen para lograr un efecto determinado, así serán libros de entrada y salida de áreas controladas, videos sistemáticamente obtenidos, resúmenes de centrales telefónicas, etc.

Es conveniente que existan sistemas de seguridad con responsabilidad cruzada y redundante para ser más consistentes la acción de protección y a la vez facilitar la supervisión mutua.

12.014. Control de las MSCI. El control de las MSCI consiste en las acciones tendientes a verificar el cumplimiento de las mismas y producir las correcciones necesarias, incluyendo su anulación, modificación, reemplazo, etc., a partir de diagnosticar las causas que llevan al incumplimiento, y determinar que aspectos pueden o deben ser mejorados para lograr un mayor cumplimiento.

El control de las medidas de seguridad de contrainteligencia podrá ser ejercido por delegación de autoridad del responsable de la organización, por el órgano de inteligencia de la misma o, a su requerimiento, el órgano del escalón superior, a través de inspecciones periódicas y aperiódicas.

Escalones superiores podrán asumir la necesidad de ejecutar controles de medidas de seguridad de contrainteligencia en los elementos bajo su responsabilidad.

El instrumento para efectivizar el control será la inspección de seguridad.

Los estudios de seguridad e inspecciones tendrán clasificación de seguridad: "CONFIDENCIAL".

CAPÍTULO XIII

ESTUDIOS E INSPECCIONES DE SEGURIDAD

SECCIÓN I

CONCEPTOS GENERALES

13.001. Conceptos generales. Todo elemento deberá tener en cuenta que el enemigo u oponente apelará a todos los recursos disponibles para superar las barreras que se le opusieren. Deberá, asimismo, entenderse que NO existirán barreras invulnerables, que aseguren totalmente contra el accionar indebido (daño, robo, hurto, agresión u otros) al objetivo o a la fuente que interesare, por parte de quien llevar a cabo una actividad de Inteligencia contra un elemento de la Fuerza.

Lo expresado obligará al comandante o jefe del elemento a adoptar provisiones específicas en relación con la situación imperante, teniendo en cuenta que estas deberán contemplar los siguientes aspectos:

- a. Su adecuación al nivel de seguridad necesario del elemento. Dicho nivel deberá ser fijado por el comandante o jefe en relación con la misión impuesta al elemento que comandare.
- b. El análisis previo, en detalle, del plan de medidas de seguridad de contrainteligencia elaborado por el elemento, así como, la vigencia de las medidas derivadas de su aplicación.
- c. La determinación de las debilidades existentes en la seguridad, relacionadas particularmente con deficiencias en el planeamiento y en la adopción de las medidas consecuentes.
- d. La verificación del grado de cumplimiento de las medidas de seguridad de contrainteligencia.

Todo ello impondrá el desarrollo de procesos descriptivos y analíticos que configurarán verdaderas apreciaciones de situación de seguridad y que se denominan "estudios e inspecciones de seguridad". Generalmente, su clasificación de seguridad (en ambos documentos) será "CONFIDENCIAL".

13.002. El estudio de seguridad. Definición. Es la apreciación de la situación de seguridad, desde el punto de vista de contrainteligencia, sobre instalaciones y/o sectores determinados en los que existan información, medios y/o materiales por proteger.

En este documento descriptivo, que contempla todos los aspectos funcionales a la aplicación de las medidas de seguridad de contrainteligencia, se recopilará información relacionada con el tema específico y se formularán conclusiones y proposiciones acerca del estado de seguridad actual de un elemento y de las medidas que deberán adoptarse para disminuir o neutralizar las actividades de Inteligencia del enemigo.

13.003. La inspección de seguridad. Definición. Es una técnica de contrainteligencia que consistirá en la fiscalización de la adopción de las medidas de seguridad y de su cumplimiento, a fin de verificar el grado de seguridad existente, la eficacia de las medidas y su vigencia. Esta técnica, a su vez, permitirá determinar la conveniencia o la necesidad de adoptar, modificar o derogar las medidas en uso, en forma total o parcial, y/o tomar las medidas disciplinarias o jurídicas, que se derivaren de las transgresiones que se detectaren.

13.004. Responsabilidades. Alcance. Todo comandante, director o jefe de un elemento u organismo militar, será responsable de adoptar las acciones necesarias tendientes a mantener e incrementar un nivel de seguridad adecuado que le permita desarrollar sus actividades, minimizando los aspectos que generen riesgos y/o amenazas a la información, sus recursos humanos y materiales.

Las tareas derivadas de la ejecución de un estudio o una inspección de seguridad, serán responsabilidad del oficial de inteligencia de ese elemento (G-2/S-2), quien planificará, dirigirá y comprobará el cumplimiento de las medidas de seguridad acordes con la situación particular de la organización a la cual pertenece.

Cuando el nivel de seguridad requerido, supere las propias capacidades del elemento, se solicitará al escalón superior personal técnico de inteligencia para ese cometido, siendo aspecto prioritario de los especialistas la ejecución de inspecciones de seguridad.

SECCIÓN II

ESTUDIOS DE SEGURIDAD

13.005. La oportunidad de ejecución. Los estudios de seguridad se efectuarán por orden del jefe del Elemento o comando del cual dependieren. Se podrá ejecutar en forma total o parcial. Generalmente, se ordenarán cuando:

- a. Se organizare o creare un nuevo elemento.
- b. Se reactivare un elemento.
- c. Se introdujeren modificaciones sustanciales en la misión, efectivos, organización o instalaciones de un elemento.
- d. Se comprobaren deficiencias, debilidades o negligencias en el cumplimiento de las medidas de seguridad de contrainteligencia que indiquen la necesidad de una revisión completa del sistema existente.
- e. Cuando la evolución de una situación de riesgo y/o amenaza así lo aconseje.
- f. Cuando no se hubieren efectuado hasta el momento estudios de seguridad.
- g. Cuando se cambie el emplazamiento de ese elemento o parte de sus fracciones orgánicas.

La actualización del estudio de seguridad se llevará a cabo en forma periódica. Corresponderá, como mínimo, hacer una por cada semestre.

Este documento de actualización siempre será un complemento del documento original, será conveniente anexar esta actualización a este.

13.006. Planeamiento. Desarrollar el plan de actividades que facilitará la ejecución de este trabajo particular implica considerar sus exigencias temporales y cumplir detalladamente lo establecido. El planeamiento del estudio de seguridad demandará el cumplimiento de tres fases diferenciadas:

- a. Fase previa.
- b. La ejecución del estudio en sí.
- c. La formulación del informe correspondiente.

Cada una de estas fases se materializará a través de un conjunto de tareas que deberán ser realizadas respetando un orden lógico establecido. Este orden deberá seguirse tanto en la confección de la guía para realizar el estudio de seguridad como en su ejecución y en la elaboración del informe correspondiente.

En principio, todo estudio de seguridad exigirá la confección de un plan de trabajo, el cual incluirá la ejecución de tareas previas al estudio, así como las que se derivaren de este.

- a. Tareas previas al estudio de seguridad.

- 1) Entrevista inicial. Será realizada por el responsable del estudio al comandante, director o jefe del elemento u organismo, a fin de exponer el plan de trabajo. Se lo orientará sobre las tareas que deberán llevarse a cabo, si dicha autoridad estuviere de acuerdo, se impartirán las órdenes pertinentes.

Se le recabará la cooperación necesaria y la coordinación con el personal del elemento que resultare necesario.

- 2) Selección del personal para integrar el equipo. Las características del elemento sobre el cual deberá realizarse el estudio determinará qué personal deberá integrar el equipo de trabajo.

- 3) Revisión del archivo de Inteligencia del elemento. Será realizada con la finalidad de:

- a) Verificar la existencia de estudios de seguridad anteriores, a fin de comprobar el tiempo transcurrido desde su ejecución y estudiar el informe producido.
 - b) Estudiar, en el caso de que se hubieren efectuado, los informes de inspección de seguridad.
 - c) Verificar y estudiar los casos en que se hubieren violado medidas de seguridad de contrainteligencia.
 - d) Reunir información e inteligencia referente a la zona de interés.
- 4) Determinación del material necesario. Surgirá como consecuencia de la consideración de las características generales y particulares del organismo. En caso necesario, podrá solicitarse a la unidad de inteligencia material altamente tecnificado.
 - 5) Preparación de la guía de comprobación. Una guía de comprobación es un documento en donde se enuncian, en forma ordenada y agrupados por ítems, todos aquellos hechos, cosas o personas que deberán controlarse durante el desarrollo de un estudio de seguridad.

Para su elaboración se tendrá en cuenta lo establecido en el Anexo 16, teniendo en cuenta que cada situación presentará características distintas y que dicha guía deberá adecuarse a cada caso particular.

b. Ejecución del estudio de seguridad.

Se procederá a la ejecución del estudio siguiendo la guía confeccionada a tal efecto, la cual solo dará una idea general de lo que deberá estudiarse. Algunos aspectos no serán tocados y otros serán incluidos si en ella no estuvieren consignados.

Resultará conveniente que los estudios de seguridad que se realicen fuesen filmados en su totalidad, en la medida de lo posible, dado que ello permitirá:

- 1) Fundamentar sólidamente las recomendaciones por efectuarse.
- 2) Reflejar en forma exacta la situación de seguridad del organismo.
- 3) Ratificar, rectificar y/o completar aspectos incluidos en el informe escrito.
- 4) Complementar la descripción que se realizare sobre topografía, zonas críticas, barreras u otros aspectos particulares.
- 5) Facilitar el estudio de los informes producidos con anterioridad.

c. Informe de estudio de seguridad.

Una vez efectuado el estudio, se procederá a la confección de un informe (Anexo 17) en el cual se volcará en forma detallada y objetiva:

- 1) Una descripción de los hechos, cosas o personas que se hubieren controlado, de acuerdo con la lista de comprobación, sin emitir juicio alguno.
- 2) Conclusiones sobre el estado de seguridad que presentaren los aspectos antes descriptos y en relación con el nivel de seguridad deseado u ordenado.
- 3) Recomendaciones para la adopción de nuevas medidas de seguridad, cambios por introducir, completamientos u otro tipo de decisión.

El informe contendrá las partes enunciadas, a fin de ser expuesto en forma verbal o, normalmente, por escrito, a la autoridad que lo hubiere ordenado. Tanto las conclusiones como las recomendaciones podrán ser adelantadas verbalmente, a fin de facilitar la adopción de medidas que permitirán subsanar fallas advertidas en la seguridad.

También será necesario considerar una apreciación presupuestaria inicial que facilite al jefe de elemento u organismo, contar con elementos reales de juicio para adoptar una resolución desde el punto de vista de la adquisición de efectos, bienes u otros (Apéndice 1 al Anexo 17).

Para un mayor esclarecimiento, será conveniente incluir imágenes (fotos) en el cuerpo del informe y agregarse esquicios, cartas, gráficos integrados con dibujos y fotografías (incluso con referencia a filmaciones) como anexos de este.

d. Limitaciones.

Las tareas específicas que se indiquen necesarias, derivadas de la seguridad laboral e higiene ocupacional, no se encuentran bajo la órbita de personal especialista de inteligencia; serán solo una apreciación, desde el punto de las medidas de seguridad de contrainteligencia, la recomendación de aplicación de tales acciones.

13.007. Estudios de seguridad especiales. Estos estudios estarán referidos a aspectos que exigirán el trabajo de personal técnico específico. Generalmente, serán realizados por personal especialista en electrónica, a fin de asegurarse que las instalaciones u otros locales concretos, donde se tratare información clasificada, estuvieren libres de equipos técnicos para la reunión de información (internos o externos al lugar) o bien, cuenten con los medios electrónicos acordes con la seguridad que dicho espacio requiere.

Estos estudios serán solicitados a la dirección/comando del cual dependiere ese organismo que posee al personal especialista.

Durante la realización del estudio de seguridad de un elemento, al que se considerare crítico en lo concerniente a la seguridad, el estudio de los siguientes aspectos podrá ser agregado a aquel como un anexo.

a. Alcance del estudio.

- 1) Búsqueda y comprobación de modificaciones no autorizadas en los equipos existentes.
- 2) Búsqueda de equipos electrónicos no autorizados.
- 3) Incremento de medios electrónicos que alerten o potencien un sector determinado (sensores, alarmas, cámaras).

b. Estudio.

- 1) Entrada y salida de conductores eléctricos.
- 2) Inspección de la superficie del suelo, paredes y techos para determinar la existencia de cualquier anomalía.
- 3) Inspección de cajas de salidas eléctricas, lámparas, aparatos de TV, dispositivos de intercomunicación, teléfonos, computadoras, etc.
- 4) Control de todos los cables en toda su extensión, a fin de determinar la existencia de objetos extraños o no, los que deberán ser controlados y analizados.
- 5) Revisación cuidadosa de muebles, puertas, ventanas, aberturas, etc.
- 6) Movimiento de todos los muebles, para romper los cables que pudieren estar fijos a los mismos.
- 7) Control de cables telefónicos.
- 8) Revisión de los orificios, respiraderos u otros lugares críticos.
- 9) Comprobación de los dispositivos de comunicaciones, para descubrir la presencia de cualquier señal que posibilite la reunión de información, por parte de un oponente real/potencial.
- 10) Auditoria integral del sistema informático del elemento.

c. Limitaciones.

La eficacia del estudio, necesariamente, dependerá de la disponibilidad de personal idóneo y equipos técnicos.

d. Informe.

Se confeccionará en la forma establecida para los estudios de seguridad y se adjuntará como anexo al cuerpo principal del informe del estudio de seguridad (en el caso que así fuese ejecutado). En el caso de ser un informe único, debe caratularse "Informe del Estudio de Seguridad Especial N°..."

SECCIÓN III

INSPECCIONES DE SEGURIDAD

13.008. Consideraciones básicas. Las inspecciones de seguridad tendrán un alcance más restringido que el estudio y se llevarán a cabo cuando el comando correspondiente deseara comprobar el sistema de seguridad adoptado por un elemento.

No serán periódicas, sino que se realizarán de acuerdo con la situación y, por lo menos, dos veces al año a cada elemento dependiente. Existen dos tipos de inspecciones de seguridad:

a. Anunciada.

Es aquella cuya realización será conocida por todo el personal interesado y, por lo tanto, podrán llevarse a cabo los preparativos necesarios. Será completa, formal y tendrá como objeto asegurarse de que el nivel de seguridad fuere el adecuado. Podrá ser ejecutada por personal del elemento o, bien, especialista del área de inteligencia.

b. No anunciada.

Su ejecución no será conocida por el personal del elemento. En algunos casos, podrá conocerla su jefe. Este tipo de inspección podrá abarcar aspectos parciales o totales por comprobar durante una inspección (mediante una guía) o solamente podrá manifestarse mediante un intento sutil de vulneración de barreras (por ejemplo, penetración de determinadas barreras para comprobar sus debilidades).

Estos dos tipos podrán utilizarse en forma separada o sucesiva, con respecto a un determinado elemento u organismo.

13.009. Responsabilidades. Las inspecciones de seguridad, normalmente, serán ordenadas por el comandante, director o jefe del cual dependiere el elemento por fiscalizar. Su ejecución estará a cargo de personal orgánico de dicho comando o jefatura, y podrá contar con el apoyo especializado de la unidad de Inteligencia orgánica si fuere necesario.

Anualmente, el comandante, director o jefe del elemento ordenará al órgano de dirección de inteligencia la ejecución de inspecciones de seguridad en las dependencias del mencionado organismo, con la finalidad de disponer de un conocimiento más detallado de la situación de seguridad de ciertas instalaciones de la organización que comanda.

A tal efecto, el responsable de área de inteligencia confeccionará su plan anual de inspecciones, el cual deberá respetar y elevar los informes consecuentes al jefe del elemento u organismo. Al menos, una vez al año, las dependencias con material y/o documentación clasificada deben ser inspeccionadas.

13.010. Ejecución de la inspección de seguridad

Las actividades y tareas que abarca una inspección de seguridad serán las mismas que abarcarán los estudios de seguridad. Puede señalarse como diferencia que podrá o no haber una entrevista inicial y esbozar recomendaciones si la situación así lo impusiere.

Como tarea previa, será necesario estudiar todo lo relacionado con el sistema de seguridad existente; a tal efecto, será conveniente adelantar al elemento u organismo por inspeccionar una hoja de avanzada, previa a la visita, solicitando todos aquellos antecedentes (documentos, planos, PON(s) y gráficos) que facilitarán un conocimiento más detallado.

Por similitud al planeamiento para la ejecución del estudio de seguridad, es conveniente la preparación de una guía de inspección de seguridad (Anexo 16).

El informe se confeccionará siguiendo los lineamientos generales del correspondiente a un estudio de seguridad (Anexo 17).

CAPÍTULO XIV

EDUCACIÓN E INSTRUCCIÓN DE MEDIDAS DE SEGURIDAD DE CONTRAINTELIGENCIA

SECCIÓN I

CONCEPTOS GENERALES

14.001. Conceptos generales. El personal integrante del Instrumento Militar tendrá, en mayor o menor grado, participación en las actividades de inteligencia, referidas en particular a la obtención de información y a la contrainteligencia, y su eficiencia estará en relación directa con el grado de educación e instrucción recibida.

La educación e instrucción referida a la contrainteligencia tiene como objeto lograr una actitud mental permanente en todo el personal, a fin de crear una real y efectiva “**Conciencia de inteligencia y contrainteligencia**”. Esto es, alcanzar un cambio en la conducta de los integrantes de la Fuerza para aprehender las órdenes, directivas y procedimientos de inteligencia y contrainteligencia de forma consiente y aplicarlas voluntariamente, a fin de lograr el grado de seguridad adecuado que posibilite proteger los propios recursos.

14.002. Definiciones de interés

a. Educación militar.

Acción y efecto de desarrollar y perfeccionar las facultades y aptitudes técnico profesional y militares del personal, a través de los sistemas educativos de las Fuerzas Armadas y del Estado Mayor Conjunto, a efectos de satisfacer las necesidades que las exigencias del servicio imponen en la paz y en la guerra (PC-00-02).

b. Instrucción.

Conjunto de actividades esencialmente prácticas destinadas a alcanzar los niveles adecuados de conocimiento y habilidades necesarios para el desempeño eficaz de las funciones y tareas militares (PC-00-02).

c. Instrucción militar.

Es el conjunto de actividades esencialmente prácticas que integran el proceso de formación militar, con la finalidad inmediata de promover la adquisición de conocimientos, destrezas, habilidades, técnicas y tácticas necesario para el logro eficaz de las tareas y funciones militares (PC-00-02).

El proceso educativo sobre MSCI se materializa en la transmisión de valores que producen los cambios intelectuales, emocionales y sociales de los integrantes del Instrumento Militar a fin de crear la primera barrera sistémica al accionar de la inteligencia extranjera sobre la información y medios protegidos. Esta base será la que, en definitiva, alentará la respuesta eficiente para el objetivo de las medidas de seguridad de contrainteligencia que dará todo integrante del Instrumento Militar al verse expuesto a la acción directa o indirecta de los sistemas de Inteligencia del enemigo u oponente.

Los valores fundamentales que se incluirán serán:

“Disciplina del Secreto”

y

“Necesidad de Saber”

La instrucción, tal como lo define la PC 00-02, es el conjunto de actividades, esencialmente prácticas, destinadas a alcanzar los niveles adecuados de conocimiento y habilidades necesarios para el desempeño eficaz de las funciones y tareas militares.

Vinculada a las medidas de seguridad de contrainteligencia, la instrucción se presenta como una actividad permanente aun cuando materializa especialización y progresividad, que puede determinar pasos, etapas y niveles.

La instrucción permite reducir el riesgo tanto del error posible en la acción individual, que ponga en peligro lo que se debe proteger, como en la sistematización del control orientada a la detección temprana de cualquier anomalía (PC-12-04, Capítulo 9).

SECCIÓN II

PLANEAMIENTO

14.003. El planeamiento de educación e instrucción de las medidas de seguridad de contrainteligencia. El planeamiento de las acciones educativas relacionadas con las medidas de seguridad de contrainteligencia tiene por objeto lograr la programación coordinada de actividades y tareas educativas que posibiliten capacitar al personal para cumplimentar con eficiencia sus responsabilidades respecto de la observancia de las medidas de seguridad.

Tales acciones educativas orientarán su propósito a lograr una adecuada "Conciencia de Contrainteligencia" en el personal y una mejor situación de seguridad para una organización.

SECCIÓN III

RESPONSABILIDADES

14.004. Responsabilidad en la educación e instrucción del personal. La educación e instrucción en las medidas de seguridad de contrainteligencia será responsabilidad de todo comandante, director o jefe, con el asesoramiento del organismo de inteligencia del elemento.

Su finalidad última es la de incorporar como valor, en todo el personal, cualquiera fuere su función o jerarquía, la conciencia de la importancia de la aplicación constante de las MSCI, último resguardo frente a las diferentes contingencias que pueden exponer a la información el personal y los materiales clasificados.

Si bien la educación militar incluye, en las etapas de formación y perfeccionamiento, objetivos sobre las medidas de seguridad de contrainteligencia, la incidencia que su aplicación tiene para alcanzar niveles adecuados de protección, respecto de información y materiales clasificados, hace que se requiera un esfuerzo adicional de todo responsable de una organización militar, cualquiera fuere su nivel (PC-12-04).

Todo comandante, director o jefe deberá establecer los objetivos mínimos requeridos para cada función crítica por ser desarrollada en su organización, expresados en contenidos y horas aplicadas para alcanzarlos. Esto incluirá al entrenamiento que proporcionará la adecuación del personal a nuevos materiales o funciones, y al mantenimiento de la capacidad para la función.

El oficial de inteligencia del elemento u organismo tendrá responsabilidad de asesoramiento sobre aquellos aspectos referidos a las medidas de seguridad de contrainteligencia. Durante el planeamiento de la educación, deberá participar con el oficial de operaciones, a fin de:

- a. Proponer los temas de contrainteligencia que se incluirán en el plan de educación y en la integración con las demás materias.
- b. Coordinar con el oficial de operaciones el desarrollo y control de la educación de contrainteligencia.
- c. Coordinar con los restantes miembros del elemento de asesoramiento y asistencia la integración de la educación de contrainteligencia en la correspondiente a otros aspectos de educación.
- d. Asesorar a los responsables de impartir la educación de contrainteligencia sobre los medios, ayudas de instrucción e instructores necesarios para alcanzar los objetivos de educación fijados para la contrainteligencia.
- e. Proporcionar a los elementos y organismos ayudas de instrucción e instructores capacitados para desarrollar temas de contrainteligencia.

SECCIÓN IV

OBJETIVOS EDUCATIVOS

14.005. Objetivo de la educación e instrucción. Se deberá tener como meta que el personal comprenda y aprehenda acerca de las medidas de seguridad de contrainteligencia de forma que modifique la conducta de los integrantes de la Fuerza y se concrete en el acabado cumplimiento de la disposiciones establecidas fruto de una aprehensión de los valores y no del efecto de la acción coercitiva (PC-12-04).

En conjunto, la educación e instrucción orientada a las MSCl tendrán como objetivo inculcar al personal tres ideas fundamentales:

- a. Las MSCl son de carácter permanente y requieren una continua actualización.
- b. Las MSCl conforman un sistema integrado.
- c. El cumplimiento de la aplicación de las MSCl es una responsabilidad de todos los integrantes de las Institución, sin excepción.

14.006. Consideraciones generales

Las medidas de seguridad de contrainteligencia exigen un grado de completa integración y coordinación para lograr el máximo de efectividad. Esta integración y coordinación es lo que crea el efecto sinérgico del sistema, sobre el que recae la protección de la información y materiales clasificados.

Por ello, la educación e instrucción deben hacer hincapié en que un sistema necesita de todos sus componentes para realizar su función correctamente. Si un componente falla, todo el sistema lo hará.

La seguridad de la información, personal y material, proporcionada por el sistema de MSCl, será tan fuerte como el más débil de sus componentes; es por ello que se debe orientar a inculcar que las medidas que se adopten son un esfuerzo integral del conjunto del Instrumento Militar.

En el ámbito de las MSCl, no hay conducta individual sin consecuencias. Si bien la implementación de las medidas de seguridad es una responsabilidad de comando, el cumplimiento de estas es obligatorio para todos los integrantes del Instrumento Militar, incluso para quienes que sin pertenecer a ella, ingresan, toman contacto o se relacionan de alguna forma con este.

Es por ello que todo el personal debe cumplir y hacer cumplir las medidas de seguridad de contrainteligencia impuestas, deberá informar en caso de detectar o sospechar de infracciones a estas o situaciones anormales.

La consigna por transmitir debe ser clara: "Las MSCl son de cumplimiento obligatorio para todos, SIN EXCEPCIONES".

ANEXOS

LEGISLACIÓN VINCULADA AL SECRETO MILITAR

1. DECRETO Nro 9390/63.

BUENOS AIRES, 11 de octubre de 1963.

Visto lo propuesto por el señor Ministro Secretario en el Departamento de Defensa Nacional en Expediente N° 15231/59; y,

CONSIDERANDO:

Que el Código Penal de la Nación en sus artículos 222 y 223, prevé y reprime la revelación del "Secreto Militar".

Que dentro de la legislación positiva, existe el Decreto N° 34023/44, que reglamenta la aplicación de las normas jurídicas de referencia;

Que el tiempo transcurrido desde la promulgación del Decreto N° 34023/44, la evolución sufrida por la legislación extranjera sobre la materia durante ese lapso, así como la experiencia recogida en la aplicación del mencionado decreto aconsejan su reforma y actualización.

EL PRESIDENTE DE LA NACIÓN ARGENTINA

DECRETA:

Art. 1° - "Secreto Militar" es toda noticia, informe, material, proyecto, obra, hecho, asunto que deba, en interés de la seguridad nacional y de sus medios de defensa, ser conocido solamente por personas autorizadas y mantenido fuera del conocimiento de cualquier otra.

Art. 2° - A los efectos de la aplicación del presente decreto, la "seguridad nacional" es la situación en la que los intereses vitales de la Nación se hallan a cubierto de interferencias y perturbaciones substanciales, y "defensa nacional", es el conjunto de medidas que el Estado adopta para lograr la seguridad nacional.

Art. 3° - La denominación de personas autorizadas a que se hace referencia en el Art. 1°, comprende a los funcionarios y empleados de la administración pública, a los agentes del gobierno ya las personas que en razón de su profesión, oficio y/o empleo de carácter privado, o por autorización especial emanada de autoridad competente, tengan conocimiento, permanente o transitorio, de los asuntos definidos en el Art. 1°.

Art. 4° - Sin perjuicio de lo expuesto en el Art. 1°, se considera "secreto militar" a los asuntos que se enumeran en el anexo especificativo (Apartado II - Enumeración taxativa), así como aquellos que resulten de su actualización por la autoridad competente.

Art. 5° - El Ministro de Defensa Nacional es la autoridad competente responsable de la actualización del contenido del anexo especificativo (Apartado II - enumeración taxativa), ajustándose para ello a las normas para la Calificación del Secreto Militar (Apartado I del mismo Anexo). Asimismo, en la reglamentación que dicte al efecto, deberá determinar dentro de cada Ministerio o Repartición, las autoridades y funcionarios, que por su jerarquía y competencia están facultados para calificar como "secreto militar" los casos concretos que se planteen.

Art. 6° - El Ministerio de Defensa Nacional tiene también a su cargo el estudio y resolución de todas las consultas que por casos concretos de aplicación del presente decreto, pudieran suscitarse en los distintos organismos de la administración nacional, provincial o municipal.

Art. 7°, 8° y 9° - De forma.

APARTADO I DEL ANEXO AL DECRETO N° 9390/63 - "NORMAS PARA LA CALIFICACIÓN DEL SECRETO MILITAR".

- 1) En los casos concretos no previstos en el Apartado II del presente Anexo y para imponer o no la calificación de "secreto militar" a un determinado asunto, se tendrán en cuenta siempre dentro del espíritu de la definición del art. 1° del presente decreto, los siguientes elementos de juicio:

- a) Naturaleza del asunto, en relación con su aplicación, uso y/o empleo para fines específicamente militares.
 - b) Origen y procedencia del asunto y si ha sido concebido, proyectado, redactado, fabricado o adquirido, bajo caución de secreto.
 - c) Interés militar del asunto, aunque éste no haya existido con anterioridad, o se prevea que desaparecerá después de transcurrido cierto lapso.
 - d) Accesibilidad del asunto por su uso, emplazamiento o función, que haga presumir la imposibilidad de mantener el secreto.
 - e) Conveniencia de calificar de "secreto" solamente a aspectos parciales y bien definidos del asunto, por la imposibilidad de mantener la reserva para todo el conjunto.
 - f) El factor tiempo debe ser considerado especialmente en relación con la posibilidad de poder mantener el secreto durante lapsos determinados.
- 2) Las normas contenidas en los incisos a) a f) del párrafo 1), no están expresadas en orden de importancia y pueden ser concurrentes o excluyentes.
- 3) Las normas contenidas en los incisos a) a f) del párrafo 1), se aplicarán también, pero con sentido contrario para los casos en que la calificación de "secreto militar" impuesta con anterioridad a un asunto determinado, deba ser dejada sin efecto.

APARTADO II DEL ANEXO AL DECRETO Nº 9390/63 - "ENUMERACIÓN TAXATIVA DE LOS ASUNTOS CONSIDERADOS SECRETO MILITAR".

- 1) Cuando resulten de importancia fundamental para la preparación y empleo de las fuerzas armadas:
- a) Estado moral, material y grado de instrucción y/o eficiencia de las fuerzas armadas.
 - b) Los planes de las fuerzas armadas. Datos atinentes a las reservas de las mismas. Causas y efectos accidentes militares.
 - c) Estudios, reconocimientos, proyectos, ejercicios, maniobras de las fuerzas armadas.
 - d) Organización, distribución, composición, funcionamiento, efectivos, armamento, material y dotación de los comandos, unidades, bases aeródromos, aeropuertos, organismos, destacamentos, fábricas militares, arsenales, polvorines y servicios de las fuerzas armadas.
 - e) Movimiento y transporte de tropas, material y ganado de las fuerzas armadas, cuando los mismos se realicen para participar en operaciones probables o inminentes.
 - f) Estudios, proyectos, planes de desarrollo, pruebas, experiencias, ejercicios e invenciones.
 - g) Características fundamentales de las partes constitutivas, o de las modificaciones técnicas que se introduzcan en: vehículos, naves, aeronaves, armamentos, proyectiles, explosivos, establecimientos, fortificaciones y obras militares, combustibles, materiales de guerra, medios y aparatos técnicos, telefónicos, telegráficos, radioeléctricos, acústicos, ópticos y electrónicos.
 - h) Datos referentes a movilización y desmovilización.
 - i) Adquisiciones, fabricaciones, construcciones y lo relativo a negociaciones y trámites.
- 2) La política de la nación, de interés militar. Los planes de defensa nacional.
- 3) Cuando resulten de importancia vital para la defensa nacional:

- a) Datos referentes a la movilización y desmovilización de los recursos nacionales en todos sus aspectos y los relativos a capacidad de transformación y producción.
 - b) Características, cantidad y rendimiento de las redes y medios técnicos (experimentales o en uso) de las vías y medios de comunicaciones. Ubicación de los centros de distribución telefónicos, telegráficos, radioeléctricos y de teletipos oficiales y privados.
 - c) Planes, proyectos, modificaciones y estudios referentes a las características especiales y de explotación de la red ferroviaria mejoras de rendimiento, detalles técnicos y capacidad de transformación de obras de arte, depósitos de combustibles, talleres, usinas y sistemas de tracción.
 - d) Características de la red vial y detalles técnicos especiales de sus obras de arte.
 - e) Características y detalles técnicos especiales, relativos a la construcción, rendimientos, capacidad y transformación de puertos, canales, diques, obras hidroeléctricas, represas, acueductos, gasoductos y oleoductos.
 - f) Los códigos, claves, documentos y material criptográfico para comunicaciones.
 - g) Trámites y ejecución de operaciones comerciales que en virtud de la legislación vigente, deben mantenerse secretas.
 - h) Datos relativos a materiales críticos.
 - i) Cartografía y relevamiento de cualquier tipo o clase.
 - j) Estudios analíticos.
- 4) Toda documentación que por su contenido pueda permitir la divulgación parcial o total de asuntos que hayan sido calificados de "secreto militar".

2. LEY 26.394 - CÓDIGO DE DISCIPLINA DE LAS FUERZAS ARMADAS.

- 1) Anexo IV - TÍTULO II Faltas disciplinarias – CAPITULO I- Faltas Graves:

ARTÍCULO 10.- Tipos de faltas graves.

Las siguientes conductas se considerarán faltas graves:

... INC 19. El militar que permitiere la revelación de un secreto por negligencia.

- 2) Anexo IV - TÍTULO II Faltas disciplinarias – CAPITULO III - Faltas gravísimas:

ARTÍCULO 13.- Tipos de faltas gravísimas.

Constituyen faltas gravísimas sólo las siguientes:

...INC 22. *Infidelidad en el servicio.* El militar que revelare una orden reservada o secreta o cualquier otra información que pueda poner en peligro a otros militares o hiciere peligrar el éxito de las tareas encomendadas a él o a otros militares.

3. CÓDIGO PENAL DE LA NACIÓN.

ARTÍCULO 156.- Será reprimido con multa de pesos mil quinientos a pesos noventa mil e inhabilitación especial, en su caso, por seis meses a tres años, el que teniendo noticia, por razón de su estado, oficio, empleo, profesión o arte, de un secreto cuya divulgación pueda causar daño, lo revelare sin justa causa.

ARTÍCULO 157.- Será reprimido con prisión de un (1) mes a dos (2) años e inhabilitación especial de un (1) a cuatro (4) años, el funcionario público que revelare hechos, actuaciones, documentos o datos, que por ley deben ser secretos.

ARTÍCULO 222.- Será reprimido con reclusión o prisión de uno (1) a seis (6) años, el que revelare secretos políticos, industriales, tecnológicos o militares concernientes a la seguridad, a los medios de defensa o a las relaciones exteriores de la Nación.

En la misma pena incurrirá el que obtuviere la revelación del secreto. Será reprimido con prisión de uno a cuatro años el que públicamente ultrajare la bandera, el escudo o el himno de la Nación o los emblemas de una provincia argentina.

Si la revelación u obtención FUESE COMETIDA POR UN MILITAR, en el ejercicio de sus funciones el mínimo de la pena se elevará a tres (3) años y el máximo de la pena se elevará a diez (10) años.

ARTÍCULO 223.- Será reprimido con prisión de un mes a un año e inhabilitación especial por doble tiempo, el que por imprudencia o negligencia diere a conocer los secretos mencionados en el artículo precedente, de los que se hallare en posesión en virtud de su empleo u oficio.

ARTÍCULO 255.- Será reprimido con prisión de un mes a cuatro años, el que sustrajere, alterare, ocultare, destruyere o inutilizare en todo o en parte objetos destinados a servir de prueba ante la autoridad competente, registros o documentos confiados a la custodia de un funcionario público o de otra persona en el interés del servicio público. Si el autor fuere el mismo depositario, sufrirá además inhabilitación especial por doble tiempo.

4. LEY 25.164. MARCO DE REGULACIÓN DEL EMPLEO PÚBLICO NACIONAL.

ARTÍCULO 3. — La presente normativa regula los deberes y derechos del personal que integra el Servicio Civil de la Nación. Este está constituido por las personas que habiendo sido designadas conforme lo previsto en la presente ley, prestan servicios en dependencias del Poder Ejecutivo, inclusive entes jurídicamente descentralizados.

Quedan exceptuados de lo establecido en el párrafo anterior:

- a) El Jefe de Gabinete de Ministros, los Ministros, el Secretario General de la Presidencia de la Nación, los Secretarios, Subsecretarios, el Jefe de la Casa Militar, las máximas autoridades de organismos descentralizados e instituciones de la Seguridad Social y los miembros integrantes de los cuerpos colegiados...
- c) El personal militar en actividad y el retirado que prestare servicios militares.

Artículo 23. —Los agentes tienen los siguientes deberes, sin perjuicio de los que en función de las particularidades de la actividad desempeñada, se establezcan en las convenciones colectivas de trabajo:

- f) Observar el deber de fidelidad que se derive de la índole de las tareas que le fueron asignadas y guardar la discreción correspondiente o la reserva absoluta, en su caso, de todo asunto del servicio que así lo requiera, en función de su naturaleza o de instrucciones específicas, con independencia de lo que establezcan las disposiciones vigentes en materia de secreto o reserva administrativa.

5. LEY 25.188. ÉTICA EN EL EJERCICIO DE LA FUNCIÓN PÚBLICA.

ARTÍCULO 2.- Los sujetos comprendidos en esta ley se encuentran obligados a cumplir con los siguientes deberes y pautas de comportamiento ético:

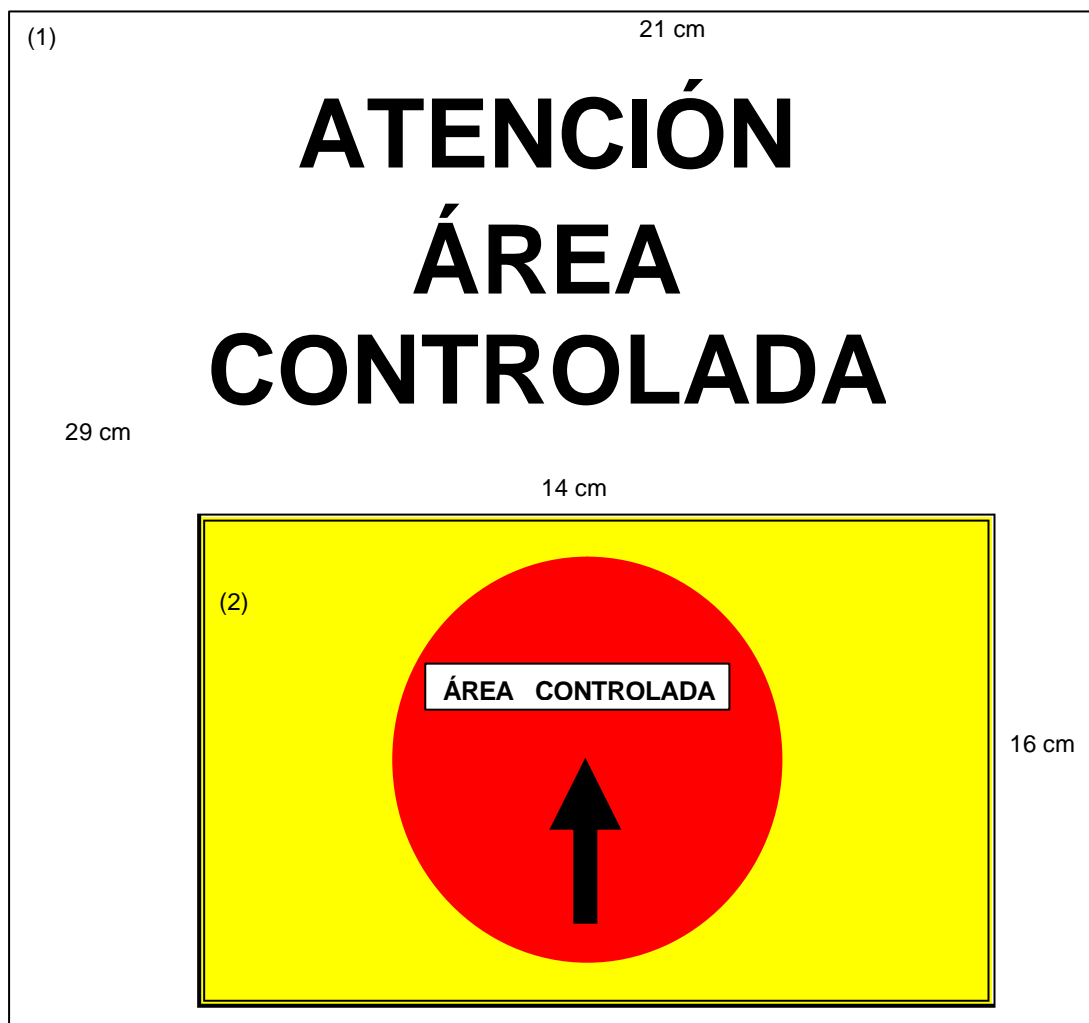
- f) Proteger y conservar la propiedad del Estado y sólo emplear sus bienes con los fines autorizados. Abstenerse de utilizar información adquirida en el cumplimiento de sus funciones para realizar actividades no relacionadas con sus tareas oficiales o de permitir su uso en beneficio de intereses privados;

6. DECRETO Nro 41/99 - CÓDIGO DE ÉTICA DE LA FUNCIÓN PÚBLICA.

ARTÍCULO 19.- DISCRECIÓN. El funcionario público debe guardar reserva respecto de hechos o informaciones de los que tenga conocimiento con motivo o en ocasión del ejercicio de sus funciones, sin perjuicio de los deberes y las responsabilidades que le correspondan en virtud de las normas que regulan el secreto o la reserva administrativa.

ARTÍCULO 30.- USO DE INFORMACIÓN. El funcionario público debe abstenerse de difundir toda información que hubiera sido calificada como reservada o secreta conforme a las disposiciones vigentes. No debe utilizar, en beneficio propio o de terceros o para fines ajenos al servicio, información de la que tenga conocimiento con motivo o en ocasión del ejercicio de sus funciones y que no esté destinada al público en general.

MODELO DE CARTELES PARA LA IDENTIFICACIÓN DE ÁREAS DE SEGURIDAD



Referencias:

- (1) Fondo blanco, letras en negro.
- (2) Fondo amarillo, círculo en rojo, flecha y letras en negro.

* Las distancias impuestas serán similares para las distintas áreas. El tamaño corresponde a una hoja tipo A 4.

(1)

ATENCIÓN
ÁREA
RESTRINGIDA

(2)



Referencias:

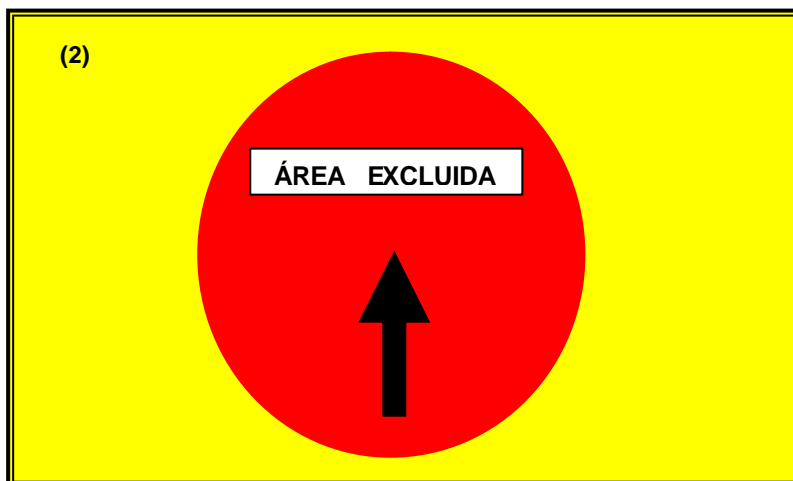
(1) Fondo blanco, letras en azul.

(2) Fondo amarillo, círculo en rojo, flecha y letras en negro.

(1)

ATENCIÓN
ÁREA
EXCLUIDA

(2)



Referencias:

- (1) Fondo blanco, letras en rojo.
- (2) Fondo amarillo, círculo en rojo, flecha y letras en negro.

MODELO DE CREDENCIAL DEL ORGANISMO

5,5 cm

EJÉRCITO ARGENTINO	
B Com 604	
Fotografía 4x4 Frente y fondo blanco	ALVAREZ
	RAUL
	Cbo 1ro
	Dir Pers - EMGE
Tarjeta de Identificación Nro 19	

CREDENCIAL DE IDENTIFICACION INTERNA
ZAPALA,de.....de
Vence:..... de.....de.....
SELLO Jefe Militar del organismo
En caso de extravío informar de inmediato al teléfono: (0391 -)

Notas:

Será tarjeta plastificada y su color será determinado por las autoridades del organismo y podrá ser cambiado si así se lo considerare necesario por razones de seguridad, en lapsos aperiódicos.

Este es un documento que deberá ser llevado permanentemente por su poseedor, de manera que en cualquier circunstancia pueda controlarse su identidad.

MODELO DE FICHA DE CONTROL DE TRÁNSITO DE PERSONAL EN INSTALACIONES MILITARES

Ejército Argentino
Guarnición Militar

FICHA DE CONTROL DE TRÁNSITO DE PERSONAL EN INSTALACIONES MILITARES

Ficha control Nro: A	Ficha control Nro: B
(Permanece en la Guardia de Prevención)	(Acompaña a la persona) (Talón para archivo definitivo)
Apellido y nombres:	Apellido y nombres:
Documento de Identificación: (Tipo): DNI-Pasaporte Nro:	Documento de Identificación: (Tipo): DNI-Pasaporte Nro:
Nacionalidad: Fecha de nacimiento:	Nacionalidad: Fecha de nacimiento:
Lugar de nacimiento: Prov/Región:	Lugar de nacimiento: Prov/Región:
Domicilio particular:	Domicilio particular:
Profesión / Actividad laboral:	Profesión / Actividad laboral:
Empresa o razón social que representa:	Empresa o razón social que representa:
Domicilio laboral:	Domicilio laboral:
Unidad u organismo que visita:	Unidad u organismo que visita:
Persona o dependencia que visita:	Persona o dependencia que visita:
Fecha de ingreso:	Fecha de ingreso:
Hora de ingreso: Hora de egreso:	Hora de ingreso: Hora de egreso:
Hora inicio entrevista: Hora finaliza entrevista:	Hora inicio entrevista: Hora finaliza entrevista:
Acompaña:	Firma (Persona entrevistada) Aclaración
Observaciones:	
Ingresa con vehículo Marca: Modelo:	Ingresa con vehículo Marca: Modelo:
Patente: Tarjeta identificación del vehículo Nro:	Patente: Tarjeta identificación del vehículo Nro:
Carga que transporta:	Carga que transporta:
Entra con material-documentación clasificada:	Entra con material-documentación clasificada:
Carga: (detallar si carga portafolio, paquetes, bultos)	Carga: (detallar si carga portafolio, paquetes, bultos)
Deja en depósito:	Deja en depósito:
Observaciones:	Observaciones:
Jefe de Guardia Oficial de Servicio Firma y aclaración Firma y aclaración	Jefe de Guardia Oficial de Servicio Firma y aclaración Firma y aclaración
Oficial Icia Un visitada Observaciones: Firma y aclaración	Oficial Icia Un visitada Observaciones: Firma y aclaración

27 cm

INSTRUCCIONES:

1. El jefe de guardia procederá a llenar ficha en ambos formularios con los datos del visitante.
2. Separará las fichas A y B.
3. El talonario A quedará bajo su custodia en la Gu Prev junto con los documentos de identidad del visitante.
4. El talonario B deberá portar en forma visible la persona que se encuentre transitando la unidad.
5. La persona entrevistada completará la parte del documento que le corresponda y se la entregará al entrevistado.
6. El entrevistado entregará el talonario debidamente completo y recibirá los documentos de identidad que hubiere dejado en la Gu Prev.
7. A relevo de servicio se entregará el talonario A al oficial de inteligencia de la unidad visitada y el talonario B al J Seg Cu (en caso de que las instalaciones se conformen con más de una unidad) o también se entregará al Of Icia para su posterior destrucción.

MODELO DE TARJETA DE CIRCULACIÓN

<div data-bbox="336 405 791 674"><p>C (2)</p><p>AUTORIZA A DESPLAZARSE EXCLUSIVAMENTE POR PISO (1)</p><p>Nro 4</p></div>	<p>(3) Firma</p> <p>JEFE AGR CDO SER (EMGE) OBSERVACIONES: AL ENTREGAR LA PRESENTE CREDENCIAL SE DEVOLVERÁ EL DOCUMENTOS DE IDENTIDAD (2)</p>
(Anverso)	(Reverso)
<div data-bbox="336 853 791 1122"><p>M (2)</p><p>AUTORIZA A DESPLAZARSE EXCLUSIVAMENTE POR PISO (1)</p><p>Nro 13</p></div>	<p>(3) Firma</p> <p>JEFE AGR CDO SER (EMGE) OBSERVACIONES: AL ENTREGAR LA PRESENTE CREDENCIAL SE DEVOLVERÁ EL DOCUMENTO DE IDENTIDAD (2)</p>
(Anverso)	(Reverso)

Nota:

Serán tarjetas plastificadas y sus colores podrán modificarse si así se lo considerase necesario por razones de seguridad en lapsos aperiódicos.


Referencias:

- (1) Letras rojas.
- (2) Letras negras.
- (3) Sello del organismo.

MODELO DE FICHA DE CONTROL DE CIRCULACIÓN DE PERSONAL EN INSTALACIONES MILITARES

Ejército Argentino
Guarnición Militar CÓRDOBA

FICHA DE CONTROL DE TRÁNSITO DE PERSONAL EN INSTALACIONES MLITARES

Ficha control Nro: A (Permanece en la Guardia Prevencion)	Ficha control Nro: B (Acompaña a la persona) (Talón para archivo definitivo)
Apellido y nombres: José ESTIGARRIBIA	Apellido y nombres: José ESTIGARRIBIA
Documento de Identificación: (Tipo): DNI Nro: 4.292.314	Documento de Identificación: (Tipo): DNI Nro: 4.292.314
Nacionalidad: argentina Fecha de nacimiento: 01 Ene 1945	Nacionalidad: argentina Fecha de nacimiento: 01 Ene 1945
Lugar de nacimiento: Tinogasta Prov/Región: CATAMARCA	Lugar de nacimiento: Tinogasta Prov/Región: CATAMARCA
Domicilio particular: Av 25 de Mayo 1275	Domicilio particular: Av 25 de Mayo 1275
Profesión / Actividad laboral: vendedor	Profesión / Actividad laboral: vendedor
Empresa o razón social que representa: Librería San José	Empresa o razón social que representa: Librería San José
Domicilio laboral: calle 9 de Julio 769 – AIMOGASTA – LA RIOJA	Domicilio laboral: calle 9 de Julio 769 – AIMOGASTA – LA RIOJA
Unidad u organismo que visita: RI Parac 22	Unidad u organismo que visita: RI Parac 22
Persona o dependencia que visita: My Mariano CHAZARRETA	Persona o dependencia que visita: My Mariano CHAZARRETA
Fecha de ingreso: 28 Feb 2012	Fecha de ingreso: 28 Feb 2012
Hora de ingreso: 1030 Hs Hora de egreso: 1320 Hs	Hora de ingreso: 1030 Hs Hora de egreso: 1320 Hs
Hora inicio entrevista: 1050Hs Hora finaliza entrevista: 1200 Hs	Hora inicio entrevista: 1050Hs Hora finaliza entrevista: 1200 Hs
Acompaña: SV Javier MONTIEL de la Aytía 2do RI se apersona para acompañarlo hasta la oficina del 2do J Un.	My MARIANO CHAZARRETA 2do J RI Parac 22
Observaciones: - -	 Firma (Persona entrevistada) Aclaración
Ingresa con vehículo Marca: FIAT Modelo: SIENA FIRE	Ingresa con vehículo Marca: FIAT Modelo: SIENA FIRE
Patente: AKC 047 Tarjeta identificación del vehículo Nro: 27	Patente: AKC 047 Tarjeta identificación del vehículo Nro: 27
Carga que transporta: efectos generales particulares	Carga que transporta: efectos generales particulares
Entra con material-documentación clasificada: No	Entra con material-documentación clasificada: No
Deja en depósito: No	Deja en depósito: No
Observaciones: entre las 1200 Hs y las 1300 Hs no se puede determinar donde estuvo. A las 1300 Hs fue interrogado por el Sarg ARÍSTIDES, quien lo condujo hasta la Gu Prev.	Observaciones: entre las 1200 Hs y las 1300 Hs no se puede determinar donde estuvo. A las 1300 Hs fue interrogado por el Sarg ARÍSTIDES, quien lo condujo hasta la Gu Prev.
Subof Pr ALDO CUCCIARO J Gu / Cu UNIÓN	Subof Pr ALDO CUCCIARO J Gu / Cu UNIÓN
Tte 1ro PEDRO ESCURRA Of Ser / Cu UNIÓN	Tte 1ro PEDRO ESCURRA Of Ser / Cu UNIÓN
Cap CARLOS ZURITA Oficial Icia / RI Parac 22	Cap CARLOS ZURITA Oficial Icia / RI Parac 22
Observaciones: Incluir recomendaciones próxima orden del día.	Observaciones: Incluir recomendaciones próxima orden del día.

INSTRUCCIONES:

1. El jefe de guardia procederá a llenar ficha en ambos formularios con los datos del visitante.
2. Separará las fichas A y B.
3. El talonario A quedará bajo su custodia en la Gu Prev junto con los documentos de identidad del visitante.
4. El talonario B deberá portar en forma visible la persona que se encuentre transitando la unidad.
5. La persona entrevistada completará la parte del documento que le corresponda y se la entregará al entrevistado.
6. El entrevistado entregará el talonario debidamente completo y recibirá los documentos de identidad que hubiere dejado en la Gu Prev.
7. A relevo de servicio se entregará el talonario A al oficial de inteligencia de la unidad visitada y el talonario B al J Seg Cu (en caso de que las instalaciones se conformen con más de una unidad) o también se entregará al Of Icia para su posterior destrucción.

**MODELO DE FICHA DE CONTROL DE CIRCULACIÓN DE PERSONAL EN
INSTALACIONES MILITARES CON MUCHA CIRCULACIÓN**

(Comandos u otros organismos de mucha circulación)

Ejército Argentino
Estado Mayor del Ejército

FICHA DE CONTROL DE TRÁNSITO DE PERSONAL (Talonario A)

Ficha Registro Nro:

Tarjeta Circulación Nro:

Apellido y nombre:

Doc Identificación (Tipo):

DNI Nro:

Fecha nacimiento:

Lugar de nacimiento:

Prov/Región:

Domicilio particular:

Profesión / Actividad laboral:

Empresa o razón social que representa:

Domicilio laboral:

Vehículo Marca:

Modelo:

Patente:

Entra con el material- documentación clasificada:

Deja en depósito:

Fecha:

Hora de entrada:

Hora de salida:

Observaciones:

21
cm

CABA, de

de 2.013

Jefe del Servicio de Seguridad
Firma y aclaración

FICHA DE CONTROL DE TRÁNSITO DE PERSONAL (Talonnario B)

Ficha Registro Nro:

Tarjeta Circulación Nro:

Piso	Dependencia	Local	Atendido por Grado - Apellido	Hora Entrada - Salida	Obs	Firma y aclaración del personal entrevistado.

CABA, de de 2.013

Jefe del Servicio de Seguridad

.....

Firma y aclaración

Notas:

(1) Queda en las instalaciones.

(2) Con el personal que visita.

MODELO DE FICHA ÍNDICE DE DOCUMENTOS EN CUSTODIA

Índice de documentos que contiene la Caja de Seguridad N° Marca..... Ubicada en..... Área.....		
Procedencia del documento		Síntesis del documento
Código	Registro	

Lugar y fecha, de de 2.012

Enc XXXXX
Firma y aclaración

Of XXXXXX
Firma y aclaración

MODELO DE REGISTRO DE SEGURIDAD DE MANIPULACIÓN DE INFORMACIÓN DOCUMENTADA CLASIFICADA

Ejército Argentino
Batallón de Arsenales 608

REGISTRO DE SEGURIDAD DE MANIPULACIÓN DE INFORMACIÓN DOCUMENTADA CON CLASIFICACIÓN X X X X X X X

Dependencia:	Registro Nro:	Fecha:	Desde:	Hasta:
--------------	---------------	--------	--------	--------

Nro	Nro o Código de referencia	Clasif Seg	Copia Nro	Documento (Tipo, Anx, Nro de páginas, Referencia sobre archivo, GFH del Doc).	Entregado por:	Retirado por:	Devuel to por:	Recibido por:	Obs
01	ZXZ 132	EyC	77	OE JEMGE 188 (Seguridad de IIEE)	(*1)	(*1)	(*1)	(*1)	
02	YYS 979	S	77	MM A 109 (Seguridad de la Fuerza en OMP).	(*1)	(*1)	(*1)	(*1)	
03									

RIO MAYO, de de 2.011

Enc Área XXXX
Firma y aclaración

Of XXXXXX
Firma y aclaración

Of Icia
Firma y aclaración

J PI My
Firma y aclaración

REFERENCIAS:

(*1) Rol – Rúbrica - Código de Guarismo

ACLARACIONES:

1. La documentación se conformará diariamente, por área responsable de la guarda y custodia de información clasificada.
2. En caso de no manipularse información, el documento no se confeccionará.

**MODELO DE RECIBO DE AUTORIZACIÓN DE INGRESO O EGRESO DE
DOCUMENTACIÓN Y MATERIAL CLASIFICADO DEL ELEMENTO U
ORGANISMO**

Ejército Argentino
B Ing M 22

**RECIBO DE AUTORIZACIÓN DE INGRESO O EGRESO
DE DOCUMENTACIÓN Y MATERIAL CLASIFICADO**

REGISTRO N

Expediente Nro
Clasificación de Seguridad:

INGRESO / EGRESO (1)

Se certifica que el portador de la presente, (Grado)

Nombre..... Apellido:

Doc Identidad: (Tipo) Nro

(1) **clasificado**, transportado en:

DOCUMENTACION

MATERIAL

INGRESA CON

EGRESA CON

Tipo (portafolio, caja, bulto, paquete, bolsa, e tc.)	Cantidad	Identificación Nro	Obs

Lugary Fecha:.....

.....

Oficial de Inteligencia / B Ing M 22

Referencias:

- (1) Tachar lo que no corresponde.
- (2) Cantidad: número de portafolios, cajas, paquetes, e tc.
- (3) Portafolios, cajas, paquetes, etc.

ACTA DE ELIMINACIÓN DE DOCUMENTOS (boletines, documentos de todo tipo clasificados o sin clasificar, etc.)

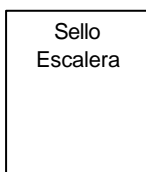
Ejército Argentino
Regimiento de Infantería de Monte

ACTA DE ELIMINACIÓN DE DOCUMENTOS

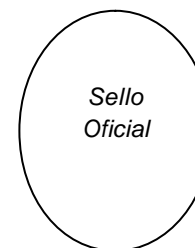
REGISTRO N°

DESTRUCCIÓN DE DOCUMENTOS (Clasificación)			(Organismo)		(Código de la Unidad)	(Lugar) (Fecha)	
Nro	Nro o código de referencia	Cantidad de hojas	Cant. Copias	Documento (Nombre – Cantidad de anexos – fecha – etc.)	Organismo de Origen	Destinatario	Obs
Preparé los documentos a eliminar.			Fecha	Grado, nombre y apellido del responsable de su guarda.		Firma	
Presenció la preparación de los documentos a eliminar.			Fecha	Grado, nombre y apellido del responsable de su guarda.		Firma	
Eliminé los documentos.			Fecha	Grado, nombre y apellido de la persona que efectúa la eliminación.		Firma	
Presenció la eliminación.			Fecha	Grado, nombre y apellido de la persona que presencia la eliminación		Firma	

Lugar y fecha.....



Capitán ANGEL GALLARDO
S-2 –RC BI 28

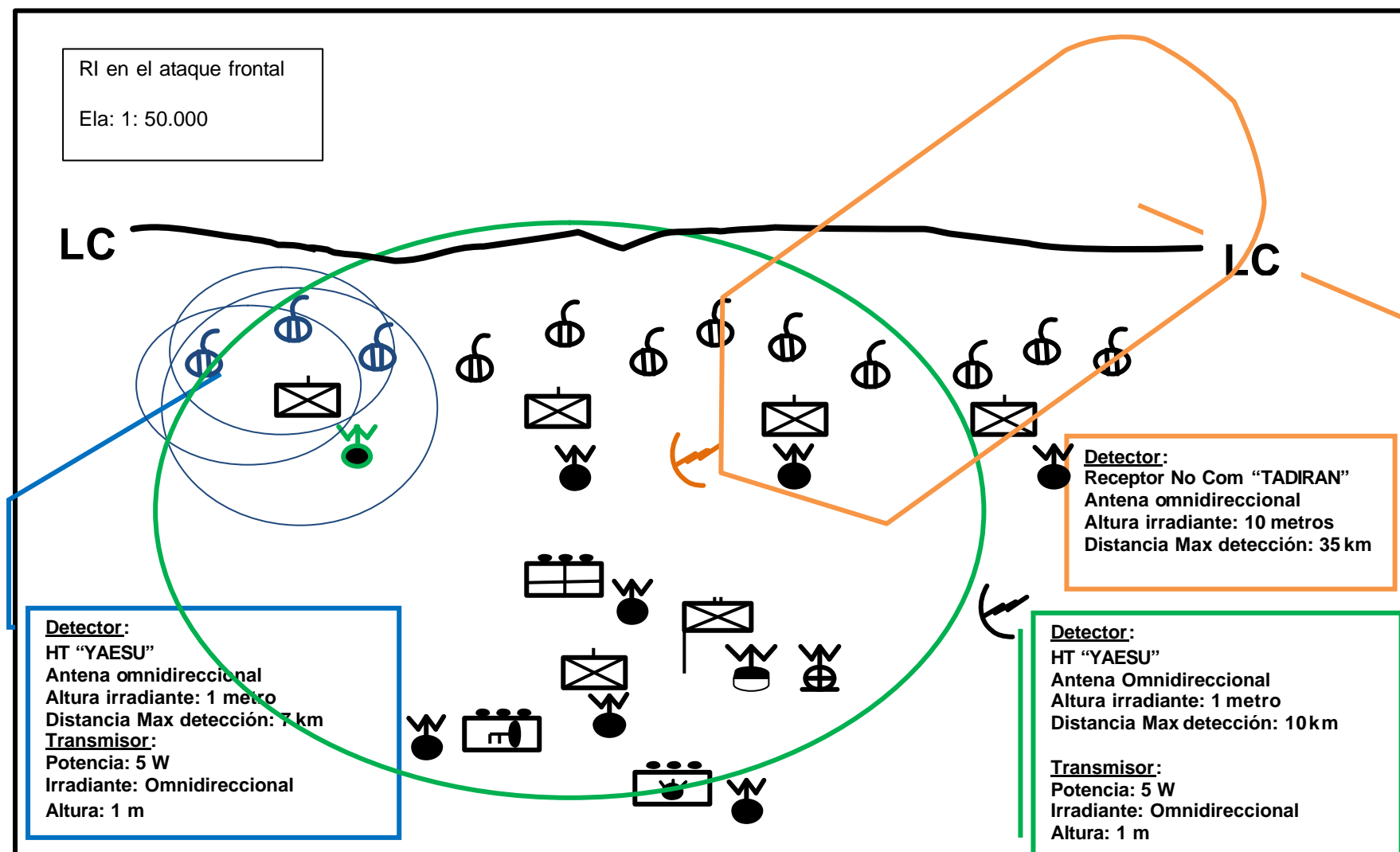


Teniente Coronel EFRAIN SEVILLA
JEFE DEL REGIMIENTO DE CABALLERÍA 28

NOTA: Si la documentación tuviere clasificación RESERVADA o mayor, firmará el Oficial. Si la documentación tuviere una clasificación menor, firmará el Oficial de Personal



GRAFICACIÓN DE LOS LÓBULOS DE EMISIÓN



OBSERVACIONES:

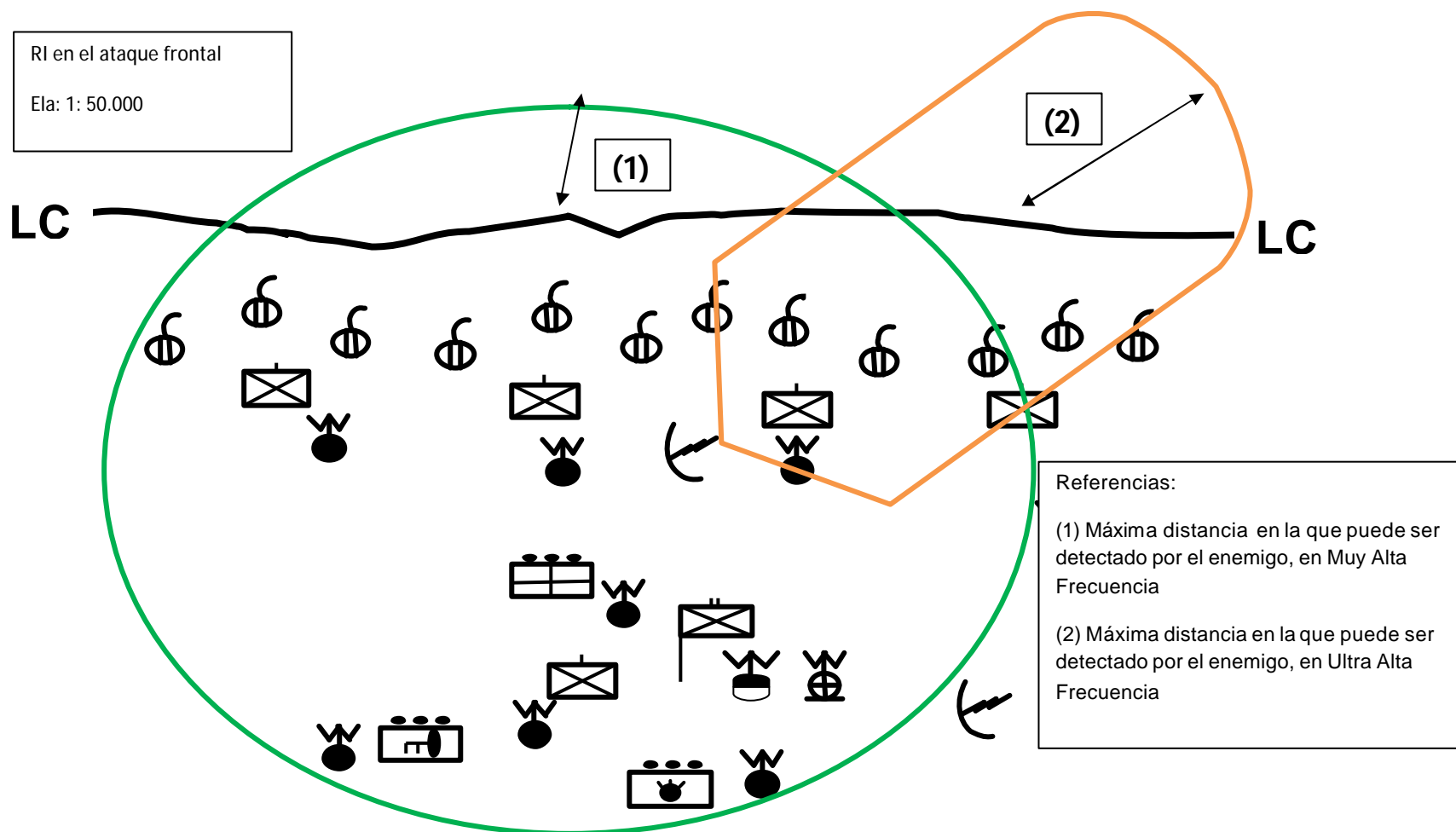
La graficación es esquemática a los fines de ejemplificarla. No deberán tomarse como reglamentarias la distribución de los elementos ni los emisores representados.

Los símbolos empleados corresponden a lo establecido en el ROD-05-05 "Conducción de Comunicaciones", Anexo 51 y RFD-99-02 "Escritura en Campaña".

Para facilitar el trazado de los lóbulos de irradiación, se les asignará un color a cada fracción, de acuerdo con el nivel en que se trabaje. Ejemplo: Si se trabaja a nivel unidad, a cada subunidad se le asigna un color diferente.

Para este ejemplo, se trazaron los lóbulos de solo algunos de los elementos, a los fines de ilustrar el procedimiento de confección.

GRAFICACIÓN DEL PEEM DEL ELEMENTO EN CONSIDERACIÓN



CARTEL DE ADVERTENCIA SOBRE LA VULNERABILIDAD DE LOS SISTEMAS DE COMUNICACIONES

ATENCIÓN
ESTE APARATO ES VULNERABLE A LA
INTERFERENCIA ENEMIGA.
NO SE DEBE TRANSMITIR INFORMACIÓN CLASIFICADA.

MODELO DE APRECIACIÓN DE SITUACIÓN DE MEDIDAS DE SEGURIDAD DE CONTRAİNTELIGENCIA

APRECIACIÓN DE SITUACIÓN DE MEDIDAS DE SEGURIDAD DE CONTRAİNTELIGENCIA Nro 00/0000

SECRETO

Copia Nro:
Unidad u organismo.
Lugar.
Oportunidad.
Clave de identificación.

UNIDAD U ORGANISMO: (Nombre y designación completa del elemento inspeccionado).

Referencias: cartografía, calcos u otros documentos útiles.

1. MISIÓN.

Enunciación de la misión asignada (o autoimpuesta) a la Fuerza.

2. CARACTERÍSTICAS DE LA ZONA.

a. Condiciones meteorológicas.

1) Situación existente:

Se volcarán los datos sobre la luz y un pronóstico o informe meteorológico.

2) Efectos sobre las actividades de inteligencia del enemigo u oponente.

Se tratarán los efectos de las condiciones meteorológicas sobre las actividades de inteligencia del enemigo (exploración aérea, patrullas, paracaidistas, exploración y vigilancia del campo de combate, etc.).

3) Efectos sobre las actividades de contrainteligencia propias.

Se indicarán las restricciones que impondrán a las actividades de contrainteligencia propias. Se determinarán sus efectos sobre la eficacia de las medidas adoptadas.

b. Terreno.

1) Situación existente.

Se determinarán las características fundamentales que presenta el terreno: cursos de agua, cultivos, obras de arte, zonas pobladas, etc., a fin de facilitar la posterior consideración de sus efectos.

2) Efectos sobre las actividades de inteligencia del enemigo.

Se indicarán sus efectos favorables y desfavorables en cuanto a ocultamiento, desplazamientos nocturnos y diurnos, transitabilidad, blancos rentables para las acciones de inteligencia que puedan desarrollar las organizaciones del enemigo u oponente, etc.

3) Efectos sobre las actividades de contrainteligencia propias.

Se señalarán los efectos que originarán condiciones favorables y desfavorables sobre las actividades de contrainteligencia propias, restando eficacia a las medidas adoptadas.

3. SITUACIÓN DE INTELIGENCIA DEL ENEMIGO.

Este párrafo contendrá toda información disponible sobre los medios de inteligencia del enemigo u oponente, que permitirá desarrollar posteriormente sus capacidades y extraer las conclusiones referidas a la probabilidad de adopción de cada una de ellas.

a. Composición.

Se determinarán las organizaciones o agrupamientos a los que pertenecen los medios enemigos disponibles, sus vinculaciones con las Fuerzas Armadas, sus dependencias, etc.

b. Efectivos y eficiencia.

Señalarán los efectivos conocidos y/o apreciados indicando procedimientos empleados, técnicas y la eficiencia demostrada.

c. Dispositivo.

Se indicarán los emplazamientos y actividades.

d. Actividades importantes, recientes y actuales.

Se resumirán los hechos que afectan a la Fuerza producidos.

e. Logística.

Posibilidades y medios de apoyo disponibles.

f. Refuerzos.

Se indicarán los medios disponibles y sus características referidas, fundamentalmente, al personal.

g. Peculiaridades y debilidades.

Se señalarán aquellas que puedan concretarse en vulnerabilidades explotables.

Ellas serán desarrolladas en los aspectos que sean necesarios y convenientes, tales como: personal inteligencia, logística, personalidades, etc.

4. CAPACIDADES DE INTELIGENCIA DEL ENEMIGO

a. Enumeración de las capacidades.

Se determinarán las capacidades de los sistemas de inteligencia del enemigo.

b. Análisis de las capacidades.

Se señalarán los indicios que indiquen la relativa probabilidad de adopción de cada capacidad.

5. CONCLUSIONES.

a. Relativa probabilidad de adopción de las capacidades de inteligencia del enemigo.

b. Efectos de las capacidades de inteligencia del enemigo.

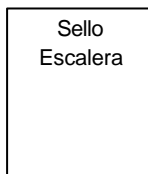
1) Efectos sobre la propia misión.

Se expresarán los efectos que ejercerán sobre el cumplimiento de la propia misión las actividades y operaciones de inteligencia del enemigo u oponente.

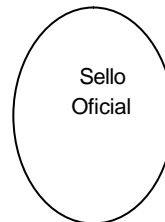
2) Efectos sobre las actividades de contrainteligencia propias.

Se deberá indicar el grado de eficiencia de las medidas prescriptas en los procedimientos operativos normales (PON), los efectos sobre las operaciones de contrainteligencia y las medidas que se deberán incrementar para contrarrestar la acción del enemigo u oponente.

AGREGADOS:



Lugar y fecha



Firma y aclaración

DISTRIBUIDOR:

GUÍA PARA CONFECCIONAR UN INFORME SOBRE UN ESTUDIO O INSPECCIÓN DE SEGURIDAD

SECRETO

Copia Nro
Unidad u organismo
Lugar
Oportunidad
Clave de identificación

INFORME SOBRE ESTUDIO / INSPECCIÓN DE SEGURIDAD Nro 00/0000

UNIDAD U ORGANISMO: (Nombre y designación completa del elemento inspeccionado).

SECCIÓN I

ANTECEDENTES RELACIONADOS CON EL ESTUDIO DE SEGURIDAD

1. **Grado de seguridad impuesto y deseado.** Determinar si el grado de seguridad impuesto es adecuado a la información, personal o material que debe proteger.
2. **Estudios de seguridad.** Evaluar los estudios de seguridad que se toman como base de estudio preliminar para determinar su valor como tal.
3. **Inspecciones de seguridad.** Evaluar las inspecciones de seguridad que se toman como base de estudio preliminar para determinar su valor como tal.
4. **Otros antecedentes básicos existentes.** Se citarán los hechos ocurridos en el elemento que hubieren afectado la seguridad, consignándolos por separado, según estuvieren relacionados con la seguridad física de la información, documentos y material clasificados, de los sistemas de comunicaciones y de las personas y del sistema informático.
5. **Hechos que afectaron la seguridad de la Fuerza en el elemento u organismo bajo estudio o inspección.** Determinar cuáles fueron los hechos que se detectaron y analizaron. Determinar si los procedimientos fueron los correctos, qué medidas aplicaron para subsanar la situación, cómo se produjo la violación de la o las medidas de seguridad. Aclarar cuáles fueron las causas y determinar qué modificaciones se hicieron para corregir las normas y procedimientos de seguridad.

SECCIÓN II

CARACTERÍSTICAS DEL ÁREA EXTERIOR

1. CARACTERÍSTICAS DEL ÁREA EXTERIOR.

a. Características topográficas periféricas.

Observar las características o accidentes del terreno en la periferia de la instalación.

- 1) Determinar si estas características tienen un efecto perjudicial para la seguridad de la instalación.
- 2) Determinar si estas características pueden ser utilizadas para disuadir a quienes pretendan entrar subrepticamente.
- 3) ¿Qué medidas adicionales de seguridad son necesarias para que las características del terreno puedan servir de barreras?
- 4) Determinar si alguna persona ajena al elemento puede usar las características del terreno como protección.

- 5) ¿Qué medidas serán necesarias para impedir el aprovechamiento de estas características del terreno por parte del enemigo?

b. Características naturales y antrópicas de las áreas inmediatas que representen riesgos o amenazas para la seguridad actual o en el futuro inmediato.

- 1) Características naturales de las áreas inmediatas que representen riesgos o amenazas para la seguridad actual o en el futuro inmediato.
- 2) Características antrópicas de las áreas inmediatas que representen riesgos o amenazas para la seguridad actual o en el futuro inmediato.
- 3) Áreas inmediatas.
 - a) Se solicitará a las fuerzas policiales, de seguridad u organismo competente que proporcionen aquellas características de las áreas inmediatas a la instalación (que les son pertinentes por la misión específica de los mismos), que pudieran llegar a constituir factores críticos para la seguridad y mantengan informado al elemento de los posibles cambios que se produzcan al respecto.
 - b) El personal de inteligencia afectado al estudio de seguridad del elemento tendrá responsabilidad primaria en el análisis de las características topográficas adyacentes al elemento desde el punto de vista de la seguridad.

c. Riesgos o amenazas informáticas.

De acuerdo con el tipo de organización y la misión, podrá haber elementos u organismos en los que la incidencia del ciberentorno podrá afectar directa o indirectamente su funcionamiento.

SECCIÓN III

CARACTERÍSTICAS DEL PERÍMETRO Y ZONA PERIMETRAL

2. CARACTERÍSTICAS DEL PERÍMETRO Y ZONA PERIMETRAL.

a. Zona perimetral.

- 1) Barreras perimétricas. Describa en detalle, según sea posible, cómo se desarrolla el sistema de barrera por sectores. El perímetro comprende tres componentes claramente diferenciados: la zona despejada interior, la barrera misma y la zona despejada exterior.

Se deberán dejar establecidos claramente y en detalle los siguientes aspectos:

a) Zona despejada interior.

Describa con detalle la extensión (ancho) de esta zona, ubicación de obstáculos, responsabilidad del mantenimiento, periodicidad con que se efectúan los trabajos necesarios, sectores iluminados, sectores sin iluminación, clase y altura o despeje de la vegetación existente, transitabilidad, determinar si corresponde a un sector público, privado o propio, tipo y cantidad de personas que habitualmente transitan, etc.

- ¿Han sido preparadas zonas despejadas lindando con la cerca? En caso afirmativo:

- ¿Qué ancho tiene la zona despejada exterior?
- La zona despejada exterior ¿está libre de obstáculos que impidan la observación?
- ¿Qué tiempo máximo de retardo proporciona la zona despejada exterior? ¿Cómo fue determinado?
- ¿Cuál es el ancho de la zona despejada interior?

- La zona despejada interior, ¿está libre de obstáculos que impidan la observación?
- ¿Qué tiempo mínimo de retardo proporciona la zona despejada interior? ¿Cómo fue determinado?
- ¿Existen algunos puntos a lo largo de la cerca donde la existencia de edificios, instalaciones, material almacenado, etc. reduzca el ancho de la zona despejada a menos del mínimo normal? Si es así, ¿ha sido aumentada la altura de la cerca para impedir la entrada? Se han adicionado otras medidas como iluminación, etc. para disminuir el riesgo.
- ¿Quién está a cargo del mantenimiento de la zona despejada? ¿Con qué frecuencia se inspecciona?
- ¿Cuál es el estado general de la zona despejada?
- Describa el terreno de la zona despejada, incluyendo el tipo de suelo, vegetación y contraste al que da lugar esta zona.
- ¿Hay algún camino conducente a la zona despejada?
- ¿Existen edificios, árboles, construcciones de cualquier tipo o material próximo a la línea de la cerca que puedan servir de ayuda para escalarla? En caso afirmativo, ¿ha sido aumentada la altura de la cerca?
- ¿Se usan torres de centinelas complementadas con la cerca del perímetro? En caso afirmativo:
- ¿Cuántas torres existen y dónde están ubicadas?
- Describa las torres para centinela, en detalle.
- Describa las posibilidades de observación de cada torre. ¿Existen obstáculos que impidan al centinela observación de toda el área que tiene asignada?
- ¿Qué medidas han sido tomadas como protección contra el acceso de personas ajenas al elemento y el fuego de armas portátiles?
- ¿Cuál es la distancia media entre las torres? Si la distancia entre dos de ellas cualesquiera fuere mayor que 100 metros, explique la razón e indique las medidas que hayan sido tomadas para controlar el área entre ellas.
- ¿Están las torres equipadas con proyectores? Describa en detalle.
- ¿Qué sistema hay para que las torres puedan comunicarse entre sí y cada torre con la guardia de prevención?

b) Zona despejada exterior.

Describa con detalle la extensión (ancho) de esta zona, ubicación de obstáculos, responsabilidad del mantenimiento, periodicidad con que se efectúan los trabajos necesarios, sectores iluminados, sectores sin iluminación, clase y altura o despeje de la vegetación existente, etc.

c) Barreras naturales.

- (1) Obstáculos en el perímetro exterior. Describa en detalle cuáles son los accidentes topográficos que se desarrollan próximos al perímetro exterior del elemento u organismo y que sirven como barrera. Se deberán considerar cursos o espejos de agua, vegetación, zanjas, mamelones, etc.

(2) Obstáculos en el perímetro interior. Describa en detalle cuáles son los accidentes topográficos que se desarrollan próximos al perímetro exterior del elemento u organismo y que sirven como barrera. Se deberán considerar cursos o espejos de agua, vegetación, zanjas, mamelones, etc.

d) Barreras artificiales.

Describa en detalle cada una de las estructuras y sistemas componentes de las barreras artificiales que se desarrollan en las instalaciones en estudio.

(1) Cercas. Tipo de material, características de su construcción, altura, etc.

- La instalación o actividad ¿está encerrada dentro de un perímetro cercado? En caso afirmativo:
 - ¿Dónde está ubicada la cerca?
 - Describa la cerca en detalle, incluya el tipo y altura, ancho, ángulo y dirección del voladizo, número de alambres y espacio entre los alambres del voladizo.
 - Señale claramente el estado, fallencias detectadas y grado de mantenimiento.
 - Describa la construcción de esta cerca, incluyendo:
 - Tipo y tamaño de los postes.
 - Distancia entre los postes y métodos para fijarlos en la tierra.
 - Tipo y características del alambre de la cerca y espacio entre los alambres.
 - Sistema empleado para fijar alambres a los postes y anclajes al piso.
 - Sistema empleado para fijar el voladizo a la cerca.
 - Proximidad de la cerca al suelo y tipo de terreno o construcción debajo de la misma.
 - Si se utilizan varias cercas, descríbalas a todas según se indicó anteriormente, incluyendo la distancia entre ellas, tipo de terreno entre las cercas y características que presenta.
 - Indique en qué lugares se hallan y describa los túneles, alcantarillas, zanjas y otras aberturas de la cerca, y en qué forma se evita que puedan ser vulnerables para pasar a través de la cerca.
 - Si pasa a través de la cerca algún arroyo, río, riachuelo, etc., explique qué medidas han sido tomadas para asegurar la misma.
 - Si pasa un ferrocarril o carretera pública a través de la instalación, describa las medidas que han sido tomadas para asegurar la cerca.
 - ¿Quién tiene a su cargo la conservación de la cerca? ¿Con qué frecuencia es inspeccionada? ¿Cuál es el estado general de las reparaciones?
- (2) Lugares de ingresos y egresos habilitados. Puertas, portones, cerraduras, control de llaves, tipo de acceso, horarios habilitados para cada uno, control de la Gu Prev, etc.
- ¿Cuántas entradas (para personal, vehículos, combinadas personal y vehículos, ferrocarriles, etc.) dan acceso a la instalación o actividad? Expresé el número de cada tipo de entrada.

- ¿Durante qué horas se usan dichas entradas?
- Describa las entradas, incluyendo la forma de construcción y el sistema de seguridad cuando las mismas no se estén utilizando.
- ¿Qué tipo de mecanismo de cierre se usa en las entradas? ¿Con qué frecuencia son inspeccionadas las cerraduras? ¿Con qué frecuencia son intercambiadas? Si se usan precintos o sellos ¿con qué frecuencia son inspeccionados?
- Si se usan llaves para las cerraduras: ¿Dónde se guardan? ¿Cómo se controlan?
- ¿Está justificado el uso de cada entrada por la cantidad de tránsito que pasa por ella?

Explique, indicando el promedio de personas o vehículos que usan cada entrada.

- ¿Qué cantidad de tiempo se necesita para proteger todas las entradas en caso de emergencia?
- ¿Qué cantidad de tiempo se necesita para abrir todas las puertas en caso de emergencia?
- ¿Qué tiempo mínimo de retardo proporcionan las entradas cuando no están en uso?

Explique cómo fue determinado este dato.

(3) Sistemas de control de acceso.

Describa los controles de acceso perimetral, personal responsable de su mantenimiento, forma de identificar al medio que lo utiliza, control de acceso remoto, habilitación – negación del acceso, etc.

(4) Sistemas de alarma.

Describa clase y cantidad de sistemas de alarma, conexión con otros sistemas de seguridad, dispositivos, equipos de control y de señalización, sistemas de transmisión, sistema principal y de alternativa de fuentes de energía, etc.

(5) Sistemas de vigilancia a través de sensores.

Describa clase (activos y pasivos) y cantidad de sistemas de vigilancia y control, conexión con otros sistemas de seguridad, dispositivos, equipos de control y de vigilancia, sistemas de transmisión, sistema principal y de alternativa de fuentes de energía, etc.

e) Barreras humanas.

(1) Sistema de guardia. Describa someramente el sistema de guardia en el sector perimetral, el detalle se deberá desarrollar en el punto 5. SISTEMA DE SEGURIDAD.

(2) Otros sistemas. Describa someramente todo aquel sistema de seguridad que no corresponda con la guardia de prevención, el detalle se deberá desarrollar en el punto 5. SISTEMA DE SEGURIDAD.

f) Barreras animales. Describir en detalle cómo se desarrolla este tipo de barrera. Se deberán considerar los siguientes aspectos: tipo y cantidad de animales, instrucción de los animales, instrucción del personal al mantenimiento, adiestramiento y manejo de los animales, periodicidad en los relevos, etc.

(1) Perros de guerra.

- ¿Se utilizan perros de guerra? En caso afirmativo:
 - ¿Qué tipo se utiliza? ¿Cuántos de cada tipo?
 - ¿Dónde son adquiridos? ¿Quién está a cargo de su adiestramiento?
 - ¿Dónde se consiguen los guías? ¿Dónde son adiestrados?
 - ¿Cómo se emplean los perros, solos o con guías?
 - ¿Se emplean perros en los puestos de guardia?
 - ¿Dónde se emplean los perros en la instalación o actividad?

Describa el área y fundamente la necesidad de contar con los perros.

- ¿Durante qué horas son utilizados los perros?
- ¿Qué facilidades existen para conseguir perros y guías de reemplazo o adicionales para un eventual refuerzo?
- ¿Qué medidas de seguridad son tomadas en cuenta cuando se hace uso de los perros?
- ¿Dónde se adquiere la comida para los perros? ¿Qué medidas de precaución se toman?

g) Sistema de iluminación. Describa en detalle el sistema de alumbrado perimetral. Se deberán considerar los siguientes aspectos: tipo de iluminación, ubicación, tipo de alumbrado (proyección deslumbrante, alumbrado directo, alumbrado indirecto, etc.), clase de lámparas, iluminación medida en lux, desarrollo de los conos de luz, personal afectado al mantenimiento, periodicidad con que se efectúan los controles, fuente de energía alternativa, conectividad a otros sistemas de seguridad (alarmas sonoras, alerta a centros de monitoreo, etc.).

- ¿Se emplea alumbrado para la protección del perímetro en la instalación? En caso afirmativo:
 - ¿Dónde están colocadas las luces y cómo están instaladas? ¿Qué espacio hay entre las luces? ¿Qué tipo de alumbrado se emplea? (proyección deslumbrante, alumbrado directo, alumbrado indirecto).
 - ¿Cuál es la cantidad de luz prevista para cada caso?
 - ¿Qué tipo de lámpara se utiliza? (lámparas incandescentes, reflectores, lámparas de descarga (vapor de mercurio, sodio, etc.), reflectores sellados, etc.).
 - ¿Qué potencia en vatios e intensidad de iluminación tienen las lámparas que se usan?
 - ¿Cuál es la iluminación en lux a lo largo del perímetro de la cerca, en las entradas, en las zonas de almacenamiento, etc.? Explique cómo fue determinado.
 - ¿Cuánto se superponen los conos de luz del alumbrado del perímetro? ¿Quedan zonas oscuras si una luz se apaga?

- ¿Quién está a cargo del mantenimiento del alumbrado del perímetro? ¿Con qué frecuencia es inspeccionado? ¿Cómo se notifica al personal responsable cuando una luminaria deja de funcionar? ¿Cuál es el estado de limpieza y reparación de los reflectores y del cristal de las lámparas? ¿Qué medidas se toman para reducir la rotura de vidrios o lámparas por accidente u otra causa?
- ¿Dónde están ubicadas las líneas conductoras de energía eléctrica? ¿Qué tipo de alumbrado se utiliza?
- ¿Cómo se controlan las luces del perímetro? ¿Quién es el responsable? ¿Cómo son controlados y protegidos los puntos de control?
- ¿Cuál es la principal fuente de energía para las luces del perímetro? ¿Cuál es la fuente auxiliar de energía? ¿Cómo están protegidas?
- En una evaluación conjunta ¿es suficiente el alumbrado para permitir una vigilancia nocturna tan efectiva como la realizada con la luz del día?

h) Todo otro aspecto necesario contenido o no en el presente reglamento.

SECCIÓN IV

CARACTERÍSTICAS DEL ÁREA INTERIOR

3. CARACTERÍSTICAS DEL ÁREA INTERIOR.

a. Aspectos generales.

1) Características topográficas.

Se enumerarán aquellas características del ambiente geográfico en el interior de las instalaciones que representan una amenaza o riesgo para la seguridad de la información, personal o material.

Como ejemplo de ello se puede mencionar la existencia de bosques con riesgo de incendio, cursos de agua próximos a los predios del elemento u organismo con riesgo de inundaciones, zonas de derrumbe, deshielo, etc.

- a) ¿Existen alturas dentro del predio que impliquen una ventaja o desventaja al sistema de seguridad? Brinde detalles.
- b) ¿Existen cursos de agua o espejos de agua dentro del predio que puedan significar una amenaza? ¿Qué tipo de acción o efecto pueda tener con relación a las medidas de seguridad?
- c) ¿Existen formaciones vegetativas que representen una amenaza a la integridad de las instalaciones o personas de la instalación para proteger?
- d) ¿Existen obras de arte que representen una amenaza a la instalación? ¿Cuáles son sus características?
- e) ¿Existen zonas o sectores dentro del predio en los cuales se pueda dar un derrumbe, deshielo o inundación? ¿Qué medidas se han adoptado? ¿Existen planes que contemplen la protección y resguardo del personal, material o información clasificada?

2) Características naturales y antrópicas del área interior que representen riesgos o amenazas para la seguridad.

Se enumerarán aquellas características y condiciones antrópicas dentro de las instalaciones que representan una amenaza o riesgo para la seguridad de la información, personal o material.

b. Medidas de seguridad referidas a la seguridad física de las instalaciones.

1) Seguridad física de las instalaciones.

a) Barreras.

Describe en detalle, según sea posible, lo siguiente:

(1) Edificios / oficinas / depósitos. Las superficies del mismo, cuántas y de qué material están construidas las puertas, cantidad y tipo de cerraduras, control de llaves, cantidad de ventanas, sistemas de cierre y alumbrado interno, etc.

(2) Estructura del edificio.

- Describir el edificio o los edificios que componen el elemento inspeccionado, incluyendo:
 - Tipo de edificio y sistema de construcción.
 - Disposición del edificio o edificios con inclusión de la distribución y dimensiones de las habitaciones.
 - Puertas de entrada al edificio o edificios, incluyendo ubicación, tamaño, sistema de construcción y sistemas de cierre o seguridad.
 - Ventanas, inclusive tamaño, tipo, sistema de construcción, tipos de vidrios, sistema de cierre, altura desde el nivel del suelo y posibilidades de ver el interior del edificio desde el exterior.
- ¿Está el edificio rodeado por una zona despejada? En caso afirmativo:
 - ¿De qué ancho?
 - ¿Está libre de obstáculos que puedan impedir la observación?
 - ¿Cuál es el estado y tipo de las reparaciones que se puedan estar efectuando?
- ¿Cómo está alumbrado el exterior del edificio o edificios? Describir esto en detalle según se indica en la Sección II. Artículo 7.
 - ¿Cómo es el sistema de iluminación interno de los edificios?
 - ¿Existe un plan de iluminación durante las horas de oscuridad? ¿Es acorde con las necesidades de la instalación?

(3) Todo otro aspecto necesario contenido o no en el presente reglamento.

b) Sistemas de acceso a las instalaciones.

Describe los sistemas de acceso utilizados para la habilitación a los distintos locales del elemento u organismo estudiado.

c) Sistemas de alarma contra personas ajenas al elemento y para vigilancia interna.

Describe los sistemas usados en el área interior de la instalación.

(1) ¿Se emplea algún dispositivo de alarma? En caso afirmativo, descríbala(s) por sus características y/o capacidad específica.

(a) ¿Dónde se utiliza? (perímetro, superficie de edificio, habitaciones, etc.)

- (b) Describa el mecanismo, incluyendo su tipo, fabricantes, modelos y forma de empleo.
 - (c) ¿Qué tipo de sistemas de alarma son usados? (local, de estación central, etc.).
 - (d) Describa los sistemas usados para la transmisión de la alarma, incluyendo tipo de alarma, instalación, modo de uso y medidas de seguridad adoptadas para las cajas de empalme y terminales.
 - (e) ¿Qué disposiciones de seguridad se tomaron contra fallas que puedan producirse o en caso de ser operado por personas extrañas?
 - (f) ¿Qué tipo de regulación de fluido eléctrico se emplea para que las falsas alarmas se reduzcan al mínimo?
 - (g) Si el sistema de alimentación funciona con energía comercial exterior, ¿hay una planta auxiliar de energía? Descríbala en detalle.
 - (h) ¿Quién está a cargo del mantenimiento de los sistemas? ¿Con qué frecuencia se les prestan dichos servicios? ¿En qué consisten?
- (2) ¿Se lleva un registro de fallas del sistema de alarma o de falsas alarmas? ¿Cuándo han ocurrido?
- (3) ¿Qué disposiciones existen para hacer reparaciones de emergencia y para reemplazar el sistema de alarma por otro en caso de fallas?
- (4) ¿Cómo pueden identificarse desde la guardia o centro de control los sectores protegidos por el sistema de alarma?
- (5) ¿Dónde está situado el centro de control? ¿Qué medidas de protección del centro de control existen? ¿Hay siempre personal de servicio en él?
- (6) ¿Cuánto tiempo tarda la guardia o sistema de seguridad en responder a la alarma? ¿Cómo son alertados? ¿Qué cantidad de personal o equipos responden a cada alarma?
- (7) ¿Existen sistemas de seguridad por circuito cerrado por TV (CCTV)? En caso afirmativo:
- (a) Ubicación de las micro-cámaras, número.
 - (b) ¿Se encuentran en forma visible o no?
 - (c) ¿Se cuenta con VTR?
 - (d) ¿Cuál es el número mínimo de lux con los cuales pueden operar, capacidad nocturna?
 - (e) Si son fijos o móviles, de movimiento automático o manual.
 - (f) Si cuentan con gran angular y/o zoom.
 - (g) ¿Dónde se encuentran ubicados los monitores? Cantidad.
 - (h) Personal que opera los mismos, si cuentan con el debido entrenamiento.
 - (i) Tiempo de servicio directo y período de descanso durante su horario de trabajo.
 - (j) Medios de comunicación y con quién que se encuentra en la sala de monitores.
 - (k) Directivas con las que cuentan, en caso de detectar alguna anomalía.

- (l) Frecuencia del mantenimiento preventivo de cámaras y monitores.
 - (m) ¿Qué personal es el encargado de realizarlo?
 - (n) ¿Cómo se cubre la zona batida por la micro-cámara durante el mantenimiento preventivo?
 - (o) Tanto las cámaras como los monitores y demás equipos alimentados por electricidad ¿cuentan con equipo auxiliar de encendido automático?
- (8) Existen sistemas de control para las visitas a través de espejos parabólicos o planos de eje concéntrico. En caso afirmativo.
- (a) Ubicación de los mismos.
 - (b) Tipos de espejos.
 - (c) Tamaño de los mismos.
 - (d) ¿Existe luminosidad suficiente que permita el uso de los mismos?
 - (e) Altura en la que se encuentran con respecto al suelo.
 - (f) Zonas batidas por espejos.
 - (g) Tipo de soporte, apoyo o encastre.
 - (h) Mantenimiento de los mismos.
 - (i) Si se encuentran al aire libre, protección que presentan.

d) Sistemas de alarma contra incendios y de extinción de incendio. Describa lo siguiente:

Esta descripción deberá limitarse estrictamente a un punto de vista de las medidas de seguridad física de la información, material o personal para proteger. Los detalles de estos sistemas estarán contenidos en las órdenes, directivas y procedimientos que se configuren, documentos que deberán estar referenciados en el estudio de seguridad.

(1) Sistema de alarma contra incendios. Dispositivos, locales donde están instalados, redes, etc.

(2) En la guardia: servicio contra incendios; personal: tipo y número, su origen y adiestramiento, empleo y vigilancia; equipo o inspección; medios de comunicación; personal de reserva; etc.

(3) En los edificios: directivas, órdenes, etc., para el servicio contra incendios; suboficial encargado del servicio; equipo; inspecciones que se ejecutan; medios de comunicación; adiestramiento del personal; etc.

- ¿Existen procedimientos y normas que establecen prioridades para la evacuación de información y material clasificado? ¿Están debida y claramente señalizados?
- ¿Se contemplan en los planes de lucha contra el fuego las zonas críticas? ¿Qué medidas se adoptan para resguardar del fuego, humo o calor asociado a estos eventos el material y la información clasificada? ¿Se fijan los procedimientos para evacuación de estos efectos de valor? ¿Está especificado taxativamente cuáles son los lugares para reunión del material o información clasificada una vez evacuada? ¿Quién es el personal afectado a la seguridad de estos efectos?

- ¿Está el personal de los equipos contra incendios o bomberos autorizado para trabajar con material clasificado? ¿En qué grado y con qué material?
- ¿El material para extinción de incendio es adecuado al material para proteger? ¿Existen los extintores específicos para material de informática? ¿Existe material de extintores específicos al material clasificado no informático?

e) Servicios.

Esta descripción deberá limitarse estrictamente a un punto de vista de las medidas de seguridad física de la información, material o personal para proteger. Los detalles de estos sistemas estarán contenidos en las órdenes, directivas y procedimientos que se configuren, documentos que deberán estar referenciados en el estudio de seguridad.

(1) Energía eléctrica.

Describe someramente cuáles son los sistemas eléctricos principales y de alternativas que sean de interés a la seguridad. Detalle la fuente y medios de transmisión de la energía, medidas de emergencia, protección, etc.

(a) ¿Cuál es la fuente que provee de energía eléctrica al elemento o actividad?

(b) Si la provee una compañía particular o estatal:

- ¿Son subterráneas o exteriores las líneas conductoras de energía eléctrica para la instalación? ¿Por dónde entran las líneas en la instalación?
- ¿Qué medidas han sido tomadas para proteger las líneas contra manipulaciones por parte de personas extrañas o sabotaje?
- ¿Cuál es la energía máxima necesaria? La energía que se recibe ¿es suficiente para que haya un excedente amplio que permita un normal funcionamiento del sistema?
- ¿Dónde está/n el/los transformadores o el transformador principal? ¿Cómo están protegidos?
- ¿Dónde están las estaciones secundarias o intermedias de energía? ¿Cómo son protegidas?
- ¿Quién está a cargo del mantenimiento de las instalaciones eléctricas?
- ¿Con qué frecuencia y por quién es inspeccionado el sistema eléctrico?

(c) Si la energía eléctrica es generada en la misma instalación:

- ¿Dónde está la planta de energía?
- ¿Cómo están protegidas contra sabotajes o intrusiones?
- La energía máxima generada, ¿sobrepasa ampliamente la carga necesaria para proporcionar una reserva?
- ¿Dónde están las plantas auxiliares? ¿Cómo están protegidas?
- ¿Quién está encargado del mantenimiento del sistema eléctrico?
- ¿Cuándo y por quién es revisado e inspeccionado el sistema eléctrico?
- Explique otras medidas tomadas para proteger el sistema eléctrico contra sabotaje.

- (d) ¿Cómo se suministra la energía eléctrica de emergencia? ¿Puede ser utilizada inmediatamente de día y de noche?
- ¿Qué lugares son alimentados con la corriente de emergencia? ¿Es esta suficiente para solucionar las necesidades principales de operación?
 - ¿Quién está a cargo de la planta de emergencia y de su mantenimiento, inspección, etc.?
- (e) ¿Hay un interruptor general de corriente eléctrica en la instalación o actividad? ¿Quién lo controla? ¿Cómo está protegido? ¿En qué lugar está?

(2) Suministro de agua.

Describe someramente cuáles son las fuentes y sistemas de circulación del líquido que sean de interés a la seguridad. Detalle la fuente y medios de transmisión, lugares de ingreso y egreso, medidas de emergencia, protección, etc.

- (a) ¿Cuál es la fuente de suministro de agua para la instalación o actividad?
- ¿Es razonablemente segura esta fuente?
 - Si se utiliza agua del suministro público ¿cuál es el diámetro de la tubería principal y por dónde penetra a la instalación o actividad?
 - Si se usa un sistema propio del elemento (depósito, tanque, etc.), ¿cuál es la capacidad, nivel del agua, presión y condiciones? ¿Cómo está protegido?
 - ¿Cuáles son las necesidades de agua en la instalación?
 - ¿Cubre el suministro estas necesidades?
 - ¿Cuál es la presión del agua en las tuberías principales?
 - ¿Están protegidas las estaciones de bombeo? ¿Cómo? ¿Dónde están ubicadas?
 - ¿Son inspeccionadas las bombas con frecuencia? ¿Cuándo? ¿Por quién?
 - ¿Están protegidas las tuberías principales, las llaves de control, las llaves de paso? ¿Cómo?
 - ¿Con qué frecuencia es comprobado el grado de pureza del agua? ¿Por quién? ¿Cómo se hace el examen?
 - ¿Se dispone de un suministro de agua para casos de emergencia? Descríbalo incluyendo su ubicación, capacidad y grado de pureza del agua.
 - ¿Qué tipo de cloacas es usado? ¿Es adecuado para las necesidades de la instalación o actividad?

(3) Calefacción, refrigeración y combustible.

Describe someramente cuáles son los medios y el tipo de fuente del combustible, sistemas de circulación de aire, medidas de emergencia, precauciones, etc.

- a) ¿Cuál es la fuente que provee de calefacción y/o refrigeración al elemento o actividad?
- ¿Se utiliza calefacción o refrigeración central? En caso afirmativo, ¿dónde están las plantas y cómo están protegidas?

- ¿El sistema de calefacción y refrigeración es inspeccionado periódicamente?
¿Cuándo y por quién?
- ¿Quién está a cargo del sistema de calefacción y de refrigeración? Si el personal ha de tener acceso a zonas críticas ¿está autorizado para trabajar con material clasificado?
- Si las habitaciones tienen calefacción ¿qué medidas de precaución se adoptan para prevenir incendios u otro tipo de siniestro?
- ¿Dónde se adquiere el combustible? ¿Es inspeccionado para detectar anomalías? ¿Cuándo? ¿Por quién? ¿Cómo se almacena? ¿Dónde? ¿Existen normas adecuadas para evitar acumulaciones innecesarias de combustible o garantizar adecuadas condiciones de almacenamiento o suministro?

(4) Telefonía.

Describe someramente cuáles son los servicios telefónicos públicos de empleo del elemento u organismo, cuáles son las distintas facilidades, ubicación y seguridad de las cajas o tableros, redes, etc.

(1) Medidas de seguridad en los sistemas telefónicos.

- ¿Tiene el elemento su propio sistema telefónico o utiliza teléfonos del Estado o de empresas telefónicas particulares? Si tiene sistema propio:
 - ¿Dónde están instalados los tableros de distribución o centrales?
 - ¿Están esos tableros o centrales debidamente protegidos?
 - Los lugares donde están los tableros de distribución o centrales ¿han sido declarados zonas restringidas?
 - Las líneas telefónicas ¿son exteriores o son subterráneas?
 - Determine la cantidad y ubicación de las cajas, las cajas de cruce de conexiones, cables, etc. ¿Están protegidos y son inspeccionados con frecuencia para comprobar si hay huellas de conexiones? ¿Cómo se realizan estas inspecciones?
 - ¿Se dispone de material para reparaciones?
 - ¿Qué medidas han sido tomadas para evitar que se difunda por teléfono información clasificada?
- ¿Hay algún circuito especial en la instalación?
 - ¿Qué autoridad lo aprobó?
 - Describa el circuito.
 - ¿Qué líneas están conectadas al circuito?
 - ¿Cuándo y por quién es inspeccionado el circuito para descubrir posibles actos de sabotaje o conexiones no autorizadas?
 - ¿Qué medidas preventivas han sido tomadas para protección del circuito?
- Si la instalación emplea teléfonos del estado o de empresas telefónicas particulares:

- ¿Qué compañía facilita el servicio?
- ¿Qué medidas han sido tomadas para evitar difusión de información clasificada mediante el uso del teléfono?
- ¿Qué medidas se toman para impedir o descubrir conexiones en las líneas?

c. Medidas de seguridad referidas a la seguridad del personal.

1) Seguridad de PMI.

2) Seguridad del personal con función crítica.

a) Personal con función crítica.

- (1) Cte, Dir, o J (grado, nombre y apellido). Ha ocupado este cargo desde: (fecha).
- (2) 2do Cte, Subdir o 2do J (grado, nombre y apellido). Ha ocupado este cargo desde: (fecha).
- (3) Oficial de Personal (grado, nombre y apellido). Ha ocupado este cargo desde: (fecha).
- (4) Oficial de Inteligencia (grado, nombre y apellido). Ha ocupado este cargo desde: (fecha).
- (5) Oficial de Material (grado, nombre y apellido). Ha ocupado este cargo desde: (fecha).
- (6) Oficial de Finanzas (grado, nombre y apellido). Ha ocupado este cargo desde: (fecha).
- (7) Oficial de Claves y auxiliares (grado, nombre y apellido). Ha ocupado este cargo desde: (fecha).
- (8) Oficial de Seguridad de la instalación (grado, nombre y apellido). Ha ocupado este cargo desde: (fecha).
- (9) Enc Dep Ars (grado, nombre y apellido). Ha ocupado este cargo desde: (fecha).
- (10) Enc Cen Com Fij (grado, nombre y apellido). Ha ocupado este cargo desde: (fecha).
- (11) Oficial de Informática (grado, nombre y apellido). Ha ocupado este cargo desde: (fecha).
- (12) Oficial de Comunicaciones (grado, nombre y apellido). Ha ocupado este cargo desde: (fecha).
- (13) Otros (grado, nombre y apellido). Ha ocupado este cargo desde: (fecha).

3) Educación e instrucción del personal en las MSCI.

a) Educación e instrucción en cuanto a contrainteligencia.

- (1) ¿Se desarrolla un programa de educación y adiestramiento de temas referidos al planeamiento y ejecución de las medidas de seguridad de contrainteligencia? De ser así:
 - ¿Se desarrollaron las clases?
 - ¿Quiénes fueron los participantes?
 - ¿Estaban presentes aquellas personas que por sus funciones resultan esenciales para su aplicación?

- ¿Aquellas personas que integran los grupos de PMI y que desarrollan funciones críticas conocen las medidas de seguridad específicas que deben aplicar en el desempeño de sus funciones y actividades?

b) Programa de ejercicios.

- (1) ¿Se incluyen temáticas de las MSCl en los ejercicios que desarrolla el elemento u organismo?
- (2) ¿Se contemplan las medidas de seguridad de contrainteligencia durante el planeamiento en las ejercitaciones?

c) Grado de educación e instrucción.

- (1) ¿Se incluyen temas relacionados con las medidas de seguridad de contrainteligencia en las comprobaciones y evaluaciones?
- (2) ¿Se incluyen los aspectos positivos y negativos respecto a la educación y adiestramiento y los resultados alcanzados en la apreciación de situación de educación del elemento del organismo, por parte del oficial de operaciones?

d. Medidas de seguridad referidas a la documentación y material clasificado.

1) Seguridad de la información contenida en documentos y/o materiales clasificados.

a) Clasificación de seguridad de la información.

En el organismo se guarda la información clasificada en los siguientes lugares:

(1) Documentación:

Local (Nro y designación)	Clasificación de la información / Material	Tipo de soporte	Ubicación específica
Ejemplo:			
Nro 23 – J Un	SECRETO	Digital	PC y CD
	RESERVADO	Papel	Armario Nro 2
Nro 25 – Of Icia	ES y C	Papel	Armario Nro 1
	ES y C	Papel	Caja fuerte
Nro 26 – Of Op	SECRETO	Papel	Armario Nro 2
	RESERVADO	Digital	Armario Nro 2
	RESERVADO	Cinta de video	Armario Nro 1

(2) Material:

Local (Nro y designación)	Clasificación de la información / Material	Tipo de soporte	Ubicación específica
Ejemplo:			
Nro 3 – Dep Ars	SECRETO	Papel y material	Estante Nro 22
	RESERVADO	Papel	Armario Nro 2
Nro 2 – Depósito de Municion	PÚBLICO MILITAR	Material	Estante Nro 32
	PÚBLICO MILITAR	Material	Sector A
Nro 25 – Of Icia	ES y C	Material	Caja fuerte

(3) Varios:

Local (Nro y designación)	Clasificación de la información / Material	Tipo de soporte	Ubicación específica
Ejemplo:			
Sala Histórica	RESERVADO	Material	Vitrina Nro 1
	RESERVADO	Papel	Estantería Nro 3
Nro 23 – J Un	PÚBLICO MILITAR	Material	Panoplia Nro 1

b) Sistema para el tratamiento de información clasificada.

Describe en detalle los métodos empleados en el manejo de cada categoría de la información clasificada que se recibe en la unidad estudiada.

(1) Centro de mensajes o mesa de entradas.

(a) ¿Existe un centro de mensajes o mesa de entradas para la distribución de toda la correspondencia que se recibe y para el despacho de toda la que se envía? En caso afirmativo:

- ¿Cuánto personal desempeña sus tareas en el lugar?
- En relación con la clasificación de la información que se maneja, ¿está el personal debidamente autorizado y educado para trabajar con ella?
- ¿Está ordenado que el centro de mensajes o mesa de entradas se encuentre dentro de un área de seguridad clasificada según la necesidad, por la información contenida? En caso afirmativo, ¿quién está autorizado para el acceso? ¿Qué método de identificación es usado?
- ¿Qué facilidades para el almacenamiento existen en el mismo?
- ¿Cuál es el horario de trabajo?
- ¿Qué cantidad de información de naturaleza clasificada está guardada en el centro de mensajes o mesa de entradas?

(2) Registro de información contenida en documentos o material clasificado.

- ¿Se mantiene un registro de la documentación o material clasificado a cargo del elemento inspeccionado? (Sobre la base de los procedimientos operativos normales o directivas dictadas al efecto, describa el registro utilizado).
- ¿Tiene el registro una clasificación de seguridad basada en el nivel de la información que registra o responde a otro sistema? Compruebe algunos casos.
- ¿Está cada página del registro marcada de acuerdo con la clasificación de seguridad según los títulos contenidos en él? Compruebe varias páginas para mayor seguridad.
- Los asientos efectuados ¿identifican suficientemente los documentos o material? Compare el registro con los documentos.
- ¿A cargo de quién está el registro? ¿Quién tiene acceso a él?
- ¿Indica en el registro el lugar de los documentos o material a los que da entrada? ¿En qué forma? (distribución, despacho, destrucción).

- ¿Está el registro al día? ¿Es exacto? Compruebe, eligiéndolos al azar, del 15 al 20% de los documentos o materiales entrados.
- ¿Se da entrada en el registro a todos los documentos originados en la unidad y se indica su destino?

(3) Recibos.

- ¿Están siempre respaldados por un recibo la documentación o el material clasificados que son retirados de su lugar de guarda? Explique el sistema usado.
- ¿Cuál es el formulario de recibo que se usa? ¿Se archiva una copia de todos los documentos clasificados que son remitidos fuera del elemento u organismo?
- ¿Contienen los recibos información clasificada? Compruebe algunos.
- Los recibos de documentos remitidos fuera del elemento u organismo que no hubieran sido devueltos ¿han sido reclamados o buscados convenientemente? h- forme sobre los resultados.
- ¿Se dispone de formularios de recibo de acuerdo con lo establecido en el presente reglamento?
- ¿Quién está encargado de hacer el recibo del material que llega al elemento u organismo inspeccionado?
- ¿Hace el elemento u organismo un uso adecuado de las normas establecidas para el trato de la documentación clasificada?

c) Guarda de la información clasificada.

Describa en detalle los medios y los procedimientos empleados para guardar la información clasificada dentro del organismo estudiado.

- (1) ¿Cómo se guarda la información de alta de clasificación de seguridad? Describir los depósitos, oficinas, etc. con inclusión de tamaño, peso, tipo de mecanismo de cierre y tiempo aproximado de retardo para apertura del local y/o caja/armario donde la misma esté contenida.
- (2) ¿Está debidamente confeccionada y guardada la planilla que contiene las combinaciones de las cajas de seguridad? Dichas combinaciones ¿han sido colocadas en un lugar determinado bajo custodia? ¿Dónde?
- (3) Si los depósitos u oficinas tienen en las ventanas rejas de hierro y puertas de seguridad ¿están debidamente fijadas a las paredes? ¿Son las rejas de tal espesor que sirvan de disuasión en un intento de forzarlas?
- (4) ¿Tienen los muebles o escritorio elementos de cierre como barras, planchas de hierro, etc.?
- (5) Si se usan cajas de seguridad para la guarda ¿cómo están fijadas a la construcción para impedir que puedan ser movidas o sustraídas por alguien? Describa la caja de seguridad y el mecanismo de cierre.
- (6) Si se usan candados de combinación para proteger la información clasificada ¿se mantienen en secreto los números de serie de fábrica? ¿En qué forma?
- (7) ¿Está colocada la planilla de responsables en la parte exterior de cada caja o depósito que guarda información clasificada?

- (8) ¿Se hace la anotación correspondiente en la planilla cada vez que es abierto o cerrado el depósito, oficina o caja? ¿Coinciden las iniciales puestas en la columna "Abierto por" con los nombres que figuran en la parte del formulario de la caja como personas autorizadas para el conocimiento de la combinación o información contenida?
- (9) ¿La persona que inspecciona la caja, oficina o depósito a la terminación de las tareas del día es otra distinta de la que manipuló la caja o desarrolla tareas en la oficina o depósito?
- (10) ¿Están claramente determinados los depósitos en los cuales NO DEBE ser guardada información clasificada?
- (11) ¿Está enterado el personal de la forma en que debe proceder cuando es encontrado un depósito u oficina abierta y sin el personal responsable en su interior después de las horas de trabajo, o cuando es encontrada documentación, material o personal fuera de su lugar o fuera de su depósito? Interrogue al personal e informe los resultados.
- (12) Si se permite al personal retirar de su lugar, por necesidad de trabajo, información clasificada ¿qué medidas de precaución son tomadas para asegurarse que dispone de los medios de guardia convenientes?

d) Distribución o difusión.

Describa en detalle los procedimientos empleados para la distribución interna de la información clasificada o difusión de inteligencia.

- (1) El personal responsable ¿toma las debidas medidas para evitar la divulgación no autorizada de información clasificada? Explique.
- (2) El personal que tiene a su cargo información clasificada ¿conoce profundamente las normas que rigen la difusión de la información a las personas que lo solicitan? y, a la vez, esas personas, ¿están debidamente autorizadas para trabajar con dicha información?
- (3) ¿Se utilizan carátulas para los documentos clasificados?
- (4) ¿Cómo se cumplen los requisitos para la protección de determinada información que no pueda ser conocida por personal extranjero?
- (5) ¿Se saca de sus lugares de archivo, fuera del horario normal, información clasificada con fines de trabajo? En caso afirmativo, ¿qué disposición existe para su debida protección?
- (6) ¿Se extiende un recibo a las personas que, dentro de la unidad, retiran de los lugares de guarda elementos que contienen información clasificada? En caso afirmativo, ¿se confecciona el recibo correspondiente? ¿Quién controla la documentación y el material dentro de las distintas oficinas o depósitos de la unidad?
- (7) ¿Se guarda un registro de a quiénes se distribuyó el documento y quiénes tomaron debido conocimiento?

e) Preparación.

Describa en detalle cómo son redactados los documentos y cómo se preparan, dentro del organismo, los elementos que contienen información clasificada. Indique si han sido tenidos en cuenta los aspectos contenidos en este reglamento.

- (1) ¿Se origina información de alta clasificación en el elemento inspeccionado? En caso afirmativo, ¿tiene el personal responsable autorización para fijar el tipo de clasificación para colocar?
- (2) La información ¿está clasificada de acuerdo con su contenido?

- (3) Si se utilizan procedimientos que requieran para reproducción de positivos, negativos, etc., ¿qué precaución se toma para su debida protección, así como para la destrucción de los desperdicios?
- (4) ¿Están debidamente protegidos los borradores de la documentación que contiene información clasificada?
- (5) ¿Los archivos digitales que sirvieron de base o borradores son debidamente guardados de acuerdo con su importancia y clasificación?

f) Marcación.

Describa en detalle cómo son colocadas las leyendas para su debida protección de la documentación o material clasificado preparado; este informe deberá incluir las copias en borrador, las notas de taquígrafo, si las hay, etc.

- (1) ¿Se respeta la marcación de los documentos de acuerdo con lo establecido en el RFP-70-05 "DOCUMENTACIÓN"?
- (2) ¿Se respeta taxativamente lo especificado con relación a la colocación de los sellos?
¿Se cumple con aquella marcación que debe ser colocada con los sellos de goma?
(Ver RFP-70-05, Capítulo II, Sección II).
- (3) ¿Se asigna la clave de identificación del documento según un registro sin que el mismo guarde relación con las iniciales de alguno de quienes intervinieron ni el elemento u organismo origen o destino del documento? (Ver RFP-70-05, Capítulo II, Sección III, Artículo 3.031, b.).

g) Reproducción.

Describa en detalle cómo es reproducida y marcada la información clasificada contenida en documentos o material.

- (1) Si hacen reproducciones impresas de material clasificado, ¿cómo se protegen las matrices, positivas, pruebas de galera, copias sobrantes, desperdicios, etc., contra la divulgación no autorizada?
- (2) Si se utilizan procedimientos que requieran para reproducción de positivos, negativos, etc. ¿Qué precaución se toma para su debida protección, así como para la destrucción de los desperdicios?
- (3) ¿Autoridades no pertenecientes al organismo autorizan la reproducción de información clasificada de los archivos originada fuera o dentro del mismo?
- (4) ¿Las copias digitales o escritos parciales trabajados en distintas PC o terminales han sido debidamente guardados con relación a su clasificación?

h) Reclasificación.

Describa en detalle el procedimiento usado para revisar y reclasificar la información clasificada; incluya la responsabilidad.

- (1) ¿Qué procedimiento se utiliza para la revisión de la información que es necesario reclasificar?
- (2) ¿Cómo son informados los organismos en los que se maneja información clasificada sobre instrucciones especiales impartidas en una reclasificación?
- (3) ¿Han sido reclasificados correctamente los documentos o materiales de acuerdo con las instrucciones especiales para una nueva clasificación de seguridad? Compruebe varios casos.

- (4) ¿Tienen los documentos o materiales reclasificados la debida autenticación y leyenda? Compruebe.
- (5) ¿Si el organismo ha reclasificado documentos ¿han sido notificadas las personas a quienes los mismos habían sido distribuidos originariamente? ¿Cómo?
- (6) ¿Cómo se requiere la autorización para reclasificar documentos que se considera han sido clasificados incorrectamente?

i) Destrucción normal.

Describe en detalle el procedimiento empleado para llevar a cabo la destrucción normal de la información clasificada y del material desechado: incluya la responsabilidad, los registros, etc.

- (1) ¿Se encuentra normado el procedimiento para llevar a cabo la destrucción de la documentación y material clasificado? ¿Tiene conocimiento el personal que debe desarrollar esta actividad?
- (2) ¿Se confecciona la documentación correspondiente? ¿Se tramita y guarda dicha información de acuerdo con lo establecido?
- (3) ¿Qué medidas de protección están en vigencia para asegurar que el papel carbónico usado en la preparación de documentación clasificada sea debidamente destruido?
- (4) ¿Son debidamente destruidos los desperdicios, sobrantes, borradores, etc. resultantes de la preparación o reproducción de documentación o material clasificado?
- (5) ¿Los archivos digitales que sirvieron de base o borradores son debidamente borrados?
- (6) ¿Las copias digitales o escritos parciales trabajados en distintas PC o terminales han sido debidamente borrados?
- (7) ¿Cuál es el destino final de la documentación destruida? ¿Cuál es el procedimiento que se sigue con los restos? ¿Se vende el papel que ha servido de soporte a información clasificada?
- (8) ¿Quién es la persona autorizada para destruir documentos o material clasificado?
- (9) ¿A quién se designa como testigo de la destrucción? Explique.
- (10) El oficial o suboficial comisionado y el testigo de la destrucción, ¿reúnen los requisitos exigidos por este reglamento?
- (11) ¿Se llevan los registros correspondientes de destrucción? ¿Quién los guarda? ¿Se cita la autoridad que lleva a cabo la destrucción?
- (12) Compare las actas de destrucción con el inventario de documentos o materiales clasificados para ver si concuerdan ¿Refleja el inventario todas las destrucciones que se han llevado a cabo?
- (13) ¿Se lleva algún registro de destrucción especial? Descríbalo.
- (14) ¿Cómo son destruidos los documentos o el material clasificado?

j) Evacuación y destrucción de emergencia del material clasificado.

Describe en detalle qué medidas se han determinado en las órdenes para esta eventualidad.

(1) Evacuación.

- (a) ¿Existen procedimientos operativos normales o disposiciones para la evacuación, en caso de emergencia, de documentación y material clasificado almacenado en el organismo?
- (b) ¿Se ha asignado a determinado personal tareas específicas para poner en práctica la evacuación de emergencia? Identifique al personal. ¿Conocen sus responsabilidades y las disposiciones del sistema?
- (c) ¿De qué vehículos se dispone para la evacuación?
- (d) ¿Dónde están los lugares de reunión?
- (e) En el elemento inspeccionado ¿hay un sistema para marcar la prioridad en la evacuación de los documentos y el material clasificado?

(2) Destrucción.

- (a) ¿Existen procedimientos operativos normales o disposiciones para la destrucción, en caso de emergencia, de documentación o material clasificado almacenado en la unidad inspeccionada?
- (b) ¿Han sido asignadas a determinado personal tareas específicas para llevar a cabo la destrucción de emergencia? Identifique al personal ¿conoce sus responsabilidades y las disposiciones del sistema?
- (c) ¿De qué medios se dispone para la destrucción? Describalos.
- (d) ¿Dónde están los lugares de reunión de los efectos para destruir?
- (e) ¿Existe en el elemento inspeccionado un sistema para marcar la prioridad en la destrucción de los documentos y material clasificado?

e. Medidas de seguridad referidas a informática.

1) Seguridad de los dispositivos informáticos.

a) Medidas de seguridad adoptadas con las máquinas y dispositivos de escritorio.

(1) Computadores personales.

- ¿Están especificados los operadores expresamente autorizados a utilizarlas?
- ¿Están establecidos los programas utilitarios para emplearse en el elemento?
- ¿Existen contraseñas de acceso a las máquinas y a los discos rígidos?
- ¿Existen restricciones para uso de programas, discos flexibles u otros dispositivos no autorizados?
- ¿Existen normas para la preparación, uso y guarda de copias de resguardo, tanto de datos como de programas?
- ¿Están determinados los lugares para guarda de soportes magnéticos y estos, a su vez, inventariados con cargo a determinado personal?
- ¿Existen normas de procedimientos para situaciones de emergencia?

b) Medidas de seguridad adoptadas con las computadoras portátiles.

(1) Computadores personales.

- ¿Están especificados los operadores expresamente autorizados a utilizarlas?
- ¿Están establecidos los programas utilitarios para emplearse en el elemento?
- ¿Existen contraseñas de acceso a las máquinas y a los discos rígidos?
- ¿Existen normas para la preparación, uso y guarda de copias de resguardo, tanto de datos como de programas?
- ¿Están determinados los lugares para guarda de soportes magnéticos y estos, a su vez, inventariados con cargo a determinado personal?
- ¿Existen normas de procedimientos para situaciones de emergencia?

c) Medidas de seguridad adoptadas con los dispositivos de mano.

- (1) ¿Se encuentran debidamente etiquetados los dispositivos de mano?
- (2) ¿Existe un registro de la cantidad de dispositivos? ¿Dónde se guardan? ¿Qué información puede tramitarse a través de ellos?
- (3) ¿Existen restricciones para uso de programas, discos flexibles u otros dispositivos no autorizados?
- (4) ¿Existe un registro detallado del personal autorizado a emplear estos tipos de dispositivos?
- (5) ¿Existen normativas respecto a los procedimientos para la destrucción de este tipo de dispositivo?
- (6) ¿Existen procedimientos y medidas en caso de que estos dispositivos salgan del elemento u organismo?

d) Medidas de seguridad adoptadas con las terminales.

- (1) Computadores personales.
 - ¿Están especificados los operadores expresamente autorizados a utilizarlas?
 - ¿Están establecidos los programas utilitarios a emplearse en el elemento?
 - ¿Existen contraseñas de acceso a las máquinas y a los discos rígidos?
 - ¿Existen normas para la preparación, uso y guarda de copias de resguardo, tanto de datos como de programas?
 - ¿Están determinados los lugares para guarda de soportes magnéticos y estos, a su vez, inventariados con cargo a determinado personal?
 - ¿Existen normas de procedimientos para situaciones de emergencia?

e) Medidas de seguridad adoptadas con los centros de cómputos.

- (1) ¿Se fijan rótulos externos a todas las cintas y/o discos activos? En caso afirmativo, ¿se ajustan los rótulos a los registros de inventarios?
- (2) ¿Los programas están protegidos del uso no autorizado?
- (3) ¿La función utiliza métodos automáticos (por ejemplo, un sistema gerencial del programa) para restringir el acceso a los programas aplicativos?

- (4) ¿Se llevan diariamente registros cronológicos operativos del equipo? En caso afirmativo ¿hay un responsable de su control diario?
- (5) ¿Las impresiones de la consola se examinan independientemente para detectar los problemas del operador y la intervención no autorizada?
- (6) ¿Cumple con las medidas de seguridad física de las instalaciones de acuerdo con la clasificación de la información y el material que contiene?
- (7) ¿Cumple con las medidas de seguridad de acuerdo con la clasificación de las zonas de seguridad?

2) Sistema de redes LAN. Seguridad.

a) Computadores personales.

- (1) ¿Están especificados los operadores expresamente autorizados a utilizarla?
- (2) ¿Están establecidos los programas utilitarios a emplearse en el sistema?
- (3) ¿Existen contraseñas de acceso a las máquinas y a los discos rígidos con acceso a la red LAN?
- (4) ¿Existen normas para la preparación, uso y guarda de copias de resguardo, tanto de datos como de programas?
- (5) ¿Están determinados los lugares para guarda de soportes magnéticos y éstos, a su vez, inventariados con cargo a determinado personal?
- (6) ¿Existen normas de procedimientos para situaciones de emergencia?

b) Aspectos referidos específicamente a la red.

- (1) ¿Existen procedimientos documentados para usar la red LAN?
- (2) ¿Se exige que los códigos de autorización:
 - ¿Tengan acceso al sistema de computación?
 - ¿Tengan acceso a los programas de las aplicaciones?
 - ¿Realicen transacciones?
- (3) ¿Se exige que los distintos códigos de autorización realicen transacciones diferentes?
- (4) ¿Se controlan periódicamente los códigos de autorización:
 - ¿Para restringir el uso no autorizado?
 - ¿Para modificarlos en forma asistemática?
- (5) ¿Se utiliza algún medio para que no aparezcan en pantalla los códigos de autorización que se teclean?
- (6) Las transacciones con errores detectados, ¿se ingresan en el archivo de suspenso, incluyendo:
 - ¿Un código indicando el tipo de error?
 - ¿La fecha, hora, tipo de transacción y la identificación de la terminal correspondiente?

- ¿Los valores de crédito/débito de la transacción (si hubiere)?

(7) La cinta de diario de la transacción ¿se puede usar para proporcionar parte del rastreo de auditoría, incluyendo la terminal lógica, la identificación del mensaje, el código del tipo de transacción y una copia del registro de transacción?

3) Seguridad de los sistemas operativos.

a) Controles organizativos.

- (1) ¿Existe un trabajo integrado entre el oficial de inteligencia y el oficial de SCD? Detállalo.
- (2) ¿Las siguientes funciones son todas realizadas por personas diferentes? (separación adecuada de tareas).
 - Diseño de sistemas y aplicaciones.
 - Programación
 - Prueba de aceptación.
 - Autorización de cambios de programa.
 - Manejo de documentos fuente.
 - Operaciones de la máquina.
 - Mantenimiento de archivos separados (sistemas/datos).
 - Consultas.
- (3) ¿Existen niveles de conducción y de ejecución debidamente diferenciados y equilibrados?
- (4) ¿Existen mecanismos de control, tanto verticales como horizontales?
- (5) ¿Existen normas de procedimientos ante eventuales situaciones de emergencia?
- (6) ¿Existe un paquete de documentación para cada aplicación?
- (7) ¿Existe un responsable por el manejo y guarda de cada paquete de documentación?
- (8) Los listados del programa, ¿son inaccesibles a los operadores?
- (9) Los cambios de todos los programas y sus fechas de vigencia ¿se registran de manera tal de preservar un registro cronológico preciso del sistema y sus respectivos responsables?
- (10) ¿Se guardan las copias de los archivos y los programas duplicados en un lugar alejado, restringiendo el acceso no autorizado?
- (11) ¿Existen controles automáticos para auditorías?
- (12) ¿Existen restricciones y controles para la duplicación de archivos magnéticos por parte de usuarios, incluyendo copias de resguardo?
- (13) ¿Existen previsiones para el salvado periódico de archivos centralizados?
- (14) ¿Existen distintos depósitos para los soportes de uso diario y para los soportes con copias de resguardo o seguridad?

4) Seguridad de la información.

a) Tratamiento de los datos.

- (1) Los datos, ¿son ingresados por el correspondiente usuario de la aplicación, o por alguna fracción afectada exclusivamente a esta tarea?
- (2) Los documentos originales, ¿tienen identificado a un responsable por los datos que configuran la información para ingresar?
- (3) ¿Cómo se repondrían dichos documentos si se extraviaran antes de grabarlos?
- (4) ¿Cómo se verifica el procesamiento de los datos?
- (5) ¿Cuál es el destino final de los documentos originales?

b) Manejo externo de datos.

- (1) ¿Están totalmente documentados los procedimientos para el manejo de datos, tanto interno como externo?
- (2) ¿Existen previsiones para certificar que los datos no estén expuestos a ser alterados de cualquier forma cuando estén en tránsito?
- (3) ¿Están correctamente delimitadas las responsabilidades individuales de los usuarios en el manejo de datos, así como la debida identificación de los operadores?

5) Sistemas de resguardo de la información y sistemas operativos.

Se describirá cuáles son los dispositivos de almacenamiento removible, identificación, guarda, conservación, periodicidad del back up, responsable, cantidad de copias, etc.

6) Sistemas de acceso.

a) ¿Existen sistemas de contraseña de acceso:

- (1) a cada equipo?
- (2) para cada usuario individual?
- (3) para cada aplicación?
- (4) para funciones de edición/modificación eliminación de datos?

b) ¿Cómo está establecida la ejecución del acceso maestro a los distintos sistemas y su debido control?

7) Medidas de seguridad de aquellos dispositivos con conexión a la Intranet / EA.

a) Computadoras personales.

- (1) ¿Están especificados los operadores expresamente autorizados a utilizarlas?
- (2) ¿Están establecidos los programas utilitarios para emplearse en el sistema?
- (3) ¿Existen contraseñas de acceso a las máquinas y a los discos rígidos?
- (4) ¿Existen normas para la preparación, uso y guarda de copias de resguardo, tanto de datos como de programas?
- (5) ¿Están determinados los lugares para guarda de soportes magnéticos y éstos, a su vez, inventariados con cargo a determinado personal?

(6) ¿Existen normas de procedimientos para situaciones de emergencia?

b) Aspectos referidos específicamente a la red.

(1) ¿Existen procedimientos documentados para usar la Intranet?

(2) ¿Se exige que los códigos de autorización:

- ¿Tengan acceso al sistema de computación?
- ¿Tengan acceso a los programas de las aplicaciones?
- ¿Realicen transacciones?

(3) ¿Se exige que los distintos códigos de autorización realicen transacciones diferentes?

(4) ¿Se controlan periódicamente los códigos de autorización:

- ¿Para restringir el uso no autorizado?
- ¿Para modificarlos en forma asistemática?

(5) ¿Se utiliza algún medio para que no aparezcan en pantalla los códigos de autorización que se teclean?

(6) Las transacciones con errores detectados, ¿se ingresan en el archivo de suspenso, incluyendo:

- ¿Un código indicando el tipo de error?
- ¿La fecha, hora, tipo de transacción y la identificación de la terminal correspondiente?
- ¿Los valores de crédito/débito de la transacción (si hubiere)?

(7) La cinta de diario de la transacción ¿se puede usar para proporcionar parte del rastreo de auditoría, incluyendo la terminal lógica, la identificación del mensaje, el código del tipo de transacción y una copia del registro de transacción?

8) Medidas de seguridad de aquellos dispositivos con conexión a la Internet.

a) Computadores personales.

(1) ¿Están especificados los operadores expresamente autorizados a utilizarlas?

(2) ¿Están establecidos los programas utilitarios para emplearse en el sistema?

(3) ¿Existen contraseñas de acceso a las máquinas y a los discos rígidos?

(4) ¿Existen normas para la preparación, uso y guarda de copias de resguardo, tanto de datos como de programas?

(5) ¿Están determinados los lugares para guarda de soportes magnéticos y estos, a su vez, inventariados con cargo a determinado personal?

(6) ¿Existen normas de procedimientos para situaciones de emergencia?

b) Aspectos referidos específicamente a la red.

(1) ¿Existen procedimientos documentados para usar la Intranet?

- (2) ¿Se exige que los códigos de autorización:
- ¿Tengan acceso al sistema de computación?
 - ¿Tengan acceso a los programas de las aplicaciones?
 - ¿Realicen transacciones?
- (3) ¿Se exige que los distintos códigos de autorización realicen transacciones diferentes?
- (4) ¿Se controlan periódicamente los códigos de autorización:
- ¿Para restringir el uso no autorizado?
 - ¿Para modificarlos en forma asistemática?
- (5) ¿Se utiliza algún medio para que no aparezcan en pantalla los códigos de autorización que se teclean?
- (6) Las transacciones con errores detectados, ¿se ingresan en el archivo de suspenso, incluyendo:
- ¿Un código indicando el tipo de error?
 - ¿La fecha, hora, tipo de transacción y la identificación de la terminal correspondiente?
 - ¿Los valores de crédito/débito de la transacción (si hubiere)?
- (7) La cinta de diario de la transacción ¿se puede usar para proporcionar parte del rastreo de auditoría, incluyendo la terminal lógica, la identificación del mensaje, el código del tipo de transacción y una copia del registro de transacción?

f. Medidas de seguridad referidas a las comunicaciones.

1) Medidas de seguridad de los sistemas de comunicaciones. Medios de comunicación.

a) Medios de comunicaciones principales, de alternativa y de emergencia que están disponibles en el elemento u organismo para la recepción y transmisión de información.

Descripción de los sistemas disponibles, enlaces, seguridad física de los equipos, campo de antenas, etc.

(1) ¿Cuáles son los principales medios de comunicación utilizados en el elemento?

(2) ¿Se usan sistemas adicionales?

(a) ¿Dispone el elemento o actividad de sistemas de comunicaciones radioeléctricas?
En caso afirmativo:

- ¿Qué tipo de información se envía por el sistema? Si para determinada clasificación se dispone de claves: ¿Son las provistas por el EMGE?
- ¿Están los radioperadores familiarizados con las medidas de seguridad de contrainteligencia para transmitir por la radio en forma segura?

(b) ¿Se usan en la instalación teletipos, sistemas informatizados de transmisión de datos u otro sistema? En caso afirmativo:

- ¿Dónde están instalados?

- ¿Qué medidas de protección se toman para garantizar que no será enviada información clasificada sin las correspondientes medidas?
- ¿Qué medidas han sido tomadas para asegurarse de que el personal que transmite ha sido debidamente autorizado para trabajar con información clasificada?
- ¿Cuándo se realizan inspecciones por parte de los elementos responsables del EMGE o del comando de quien depende?
- Describa cualquier otro medio de comunicación usado en la instalación. Incluir las medidas de seguridad de contrainteligencia utilizadas para impedir la divulgación no autorizada de información clasificada.
- ¿Tiene la instalación o actividad un centro de mensajes o de comunicaciones?
En caso afirmativo:
 - ¿Dónde está instalado el centro de mensajes o de comunicaciones?
 - Haga una descripción detallada del centro de mensajes o de comunicaciones, incluyendo las medidas tomadas para protegerlo contra entradas no autorizadas.
 - El centro ¿ha sido declarado área restringida o excluida?
 - El personal del centro ¿es militar o civil? Si es civil, ¿de dónde se toma y cómo?
 - ¿Está autorizado el personal del centro para trabajar con material clasificado? ¿En qué grado? ¿Es suficiente este grado para la categoría de clasificación de la información que se maneja?
 - ¿Hay siempre una persona de servicio?
 - ¿Qué categoría de información clasificada se maneja en el mismo?
 - ¿De qué facilidades se dispone para la guarda de la información?
 - ¿Cómo se hace la distribución de la información por parte del centro de mensajes? ¿Es recogida individualmente, es enviada por correo, estafeta, por correo de Ejército o por otro medio?

(c) ¿Utiliza el elemento o actividad servicio de estafeta?

- El personal de estafetas ¿es militar o empleado civil?
- Los estafetas ¿están autorizados para trabajar con material clasificado? ¿En qué grado?
- ¿Qué categoría tiene el material clasificado que se envía por los estafetas?
- Los estafetas ¿Están armados? ¿Con qué armas?
- ¿Qué medios de transporte emplean los estafetas?

(d) ¿Qué medidas han sido tomadas para mantener las comunicaciones en caso de emergencia? Descríbalas en detalle.

b) Medios de comunicaciones principales, de alternativa y de emergencia que están disponibles en el sistema de guardia en apoyo al sistema de seguridad.

Descripción de los sistemas de comunicaciones en apoyo al sistema de seguridad, enlaces, comprobaciones, seguridad física de los equipos, campo de antenas, nivel de capacitación del personal que habitualmente debe emplearlos, etc.

c) Personal empleado para operar y mantener los medios de comunicación, inclusive el tipo y número, previsión y autorización para su uso, vigilancia establecida, etc.

Enumerar al personal responsable de la operación y mantenimiento de los equipos de comunicaciones fijos y móviles, grado de capacitación, educación de contrainteligencia, etc.

- (1) Los telefonistas ¿son militares o empleados civiles?
- (2) Si son empleados civiles ¿cómo son seleccionados?
- (3) ¿Están los telefonistas autorizados para trabajar con material clasificado? ¿En qué grado?
- (4) El personal de mantenimiento ¿está compuesto por personal militar o por empleados civiles?
- (5) Si son empleados civiles ¿cómo son seleccionados?
- (6) El personal de mantenimiento ¿está autorizado para trabajar con material clasificado? ¿En qué grado?

d) Medios de comunicación para el tráfico informático, incluyendo procedimientos de operación y normativa vigente.

Describir los sistemas de comunicaciones y enlaces informáticos para la transmisión de comunicaciones. Describir los sistemas operativos, criptografía específica, procedimientos de operación, normativa vigente, etc.

e) Sistemas de provisión de energía alternativa para asegurar el desarrollo sostenido de la operación.

Describir los sistemas de alternativa para la provisión de energía eléctrica para asegurar la continuidad de operación de los sistemas de comunicaciones y otros equipos asociados.

- (1) ¿Se dispone de un subsistema de alimentación de respaldo para el caso de que falte la corriente normal? Explique.
- (2) ¿Sabe operarlo el personal designado para tal fin?

f) Medidas de seguridad referidas a la criptografía.

Describir someramente el cumplimiento de las medidas de seguridad criptográfica, la documentación que corresponda, los procedimientos adoptados, el personal que interviene. La descripción en detalle será tratada en el punto 4 CARACTERÍSTICAS PARTICULARES DEL ÁREA INTERIOR.

SECCIÓN V

ZONAS CRÍTICAS

4. ZONAS CRÍTICAS.

a. Áreas o zonas críticas.

Las áreas críticas constituyen aquellos lugares que por la información y material que allí se almacena o tramita o personal que allí permanece o desenvuelve sus actividades deberán ser consideradas especialmente. Cada área deberá tratarse desde cada una de los distintos conceptos que las medidas de seguridad de contrainteligencia consideran. En este sentido, cuando se estudie para su evaluación, deberá considerarse lo siguiente:

Área crítica Nro 1: Oficina del Cte / Dir / J elemento u organismo.

- 1) Medidas de seguridad física de la instalación.
- 2) Medidas de seguridad referidas a la seguridad del personal.
- 3) Medidas de seguridad referidas a la documentación y material clasificado.
- 4) Medidas de seguridad referidas a la informática.
- 5) Medidas de seguridad referidas a las comunicaciones.

Área crítica Nro 2: Oficina del 2do Cte / Subdir / 2do J elemento u organismo.

- 1) Medidas de seguridad física de la instalación.
- 2) Medidas de seguridad referidas a personal.
- 3) Medidas de seguridad referidas a la documentación y material clasificado.
- 4) Medidas de seguridad referidas a la informática.
- 5) Medidas de seguridad referidas a las comunicaciones.

Área crítica Nro 3: Oficina del área de inteligencia.

- 1) Medidas de seguridad física de la instalación.
- 2) Medidas de seguridad referidas a personal.
- 3) Medidas de seguridad referidas a la documentación y material clasificado.
- 4) Medidas de seguridad referidas a la informática.
- 5) Medidas de seguridad referidas a las comunicaciones.

Área crítica Nro 4: Depósito central de arsenales.

Área crítica Nro 5: Polvorines.

Área crítica Nro 6: Centro de comunicaciones fijo.

Área crítica Nro 7: Cifrario.

Área crítica Nro 8: Helipuerto

Área crítica Nro XX:

SECCIÓN VI

SISTEMA DE SEGURIDAD

5. SISTEMA DE SEGURIDAD.

Describa en detalle cómo se estructura el sistema de seguridad, el sistema de guardia y todos aquellos procedimientos de los que se valen los sistemas de seguridad para llevar a cabo su cometido.

a. Sistema de seguridad.

Describa cómo se estructura el sistema de seguridad y planes previstos, incluyendo a aquel personal y medios que sin formar parte de la Gu Prev complementan o suplementan a la misma. Es necesario considerar, entre otros aspectos, los siguientes puntos:

- 1) Servicios de seguridad guarnicionales (otros sistemas de guardia, jefes de día, corresponsables del sistema de comunicaciones guarnicionales, etc.).
- 2) ¿Existe una integración y complementación de los sistemas de seguridad y guardia entre los elementos u organismos de la guarnición?
- 3) ¿Se designa un jefe a cargo del sistema de seguridad guarnicional?
- 4) ¿Existe una señal de reconocimiento a nivel guarnicional?
- 5) ¿Se ha instrumentado y funciona el sistema de comunicaciones guarnicional que integre los sistemas de guardia? De ser así:
 - a) ¿Existe una tabla de autenticación?
 - b) ¿Se han elaborado las IFC correspondientes?
 - c) ¿Se prevén medios de alternativas?
- 6) Planes de recuperación por parte de los propios medios y aquellos en los que participan otros elementos u organismos de la Fuerza.
 - a) ¿Se han desarrollado los planes de recuperación de instalaciones a nivel guarnicional?
 - b) ¿Se han practicado los planes?
 - c) ¿El personal conoce los planes previstos para la recuperación de instalaciones militares?
 - d) ¿Los planes contemplan las cadenas de llamada, lugares de reunión, medios de comunicación, etc.?
- 7) Convenios y acuerdos con fuerzas de seguridad, fuerzas policiales sistemas de salud para responder a determinadas situaciones.
 - a) ¿Existen previsiones de planes para coordinar las acciones de las FFSS y FFPP en caso de recuperación de instalaciones militares?
 - b) ¿Existen previsiones de planes para coordinar las acciones de los sistemas de salud ante la eventualidad de tener que atender y evacuar heridos?
 - c) ¿Los planes determinan aquel personal que se desempeñará como oficiales de enlaces y personal de guías con las FFSS, FFPP, Sis salud, etc. durante las acciones?

b. Sistema de guardia.

1) **Guardia.** Sistema, tipo y número de centinelas u otro personal de seguridad, su origen y adiestramiento, su empleo y vigencia, equipo, medios de comunicación, sistemas de patrullas, reservas, etc.

a) Personal de la guardia.

- (1) ¿Qué clase de personal de guardia se emplea en la instalación o actividad? (soldados de guardia, policía militar, personal civil, etc.).
- (2) Por tipo ¿cuáles son los efectivos de la guardia?
- (3) ¿Qué normas se siguen para seleccionar o nombrar al personal de guardia?
- (4) ¿De qué procedencia es el personal?
- (5) En caso de ser contratado, ¿se verifican los antecedentes personales de acuerdo con el marco legal vigente antes de darle el empleo?
- (6) ¿Ha sido concedida autorización a determinado personal de guardia para trabajar con información clasificada? ¿En qué grado?
- (7) ¿A qué tipo de adiestramiento es sometido el personal de guardia? (Se incluirán materias enseñadas y alcance, método de adiestramiento, grado de capacitación del personal instructor, quién es el responsable del adiestramiento, clases y programas de instrucción, vigilancia y comprobación).
- (8) ¿Qué adiestramiento se da a la guardia de prevención, una vez que se hace cargo de sus funciones? (Incluir materias, frecuencia del adiestramiento, personal instructor, comprobación, ejercicios prácticos, etc.).
- (9) ¿Cuál es el promedio de ausentismo que se produce en el personal que debe cubrir guardia?
- (10) ¿Cuál es el promedio de cambios que se efectúan en el personal de guardia por orden de personas responsables o por solicitud de los causantes?
- (11) ¿Cuál es el aspecto general del personal de guardia?
- (12) ¿Han sido impuestas sanciones disciplinarias durante el desempeño del personal de guardia?
- (13) ¿Cuál es la moral general del personal de guardia?

b) Inspección y control de la guardia.

- (1) ¿Qué sistema se usa para controlar la guardia?
- (2) ¿Cómo está organizada la guardia?
- (3) ¿Por cuántos hombres está constituida la guardia? ¿Cuántos relevos pueden ser formados? ¿Cuenta con retenes?
- (4) ¿Dónde está ubicado el edificio de la guardia? ¿Qué personal de guardia está de cuarto vigilante por cada relevo?
- (5) Control de reglamentos, directivas, PON y órdenes que han sido impartidas para el funcionamiento de la guardia.
- (6) ¿Qué reglamentos se aplican en cuanto a medidas disciplinarias para el personal de guardia?

- (7) ¿De qué facilidades dispone el personal de guardia o el que está de reserva para cumplir mejor con su cometido y para el descanso?
- (8) ¿Cómo comprueba el personal de los cuadros de la guardia que los integrantes de la misma estén desempeñando correctamente su obligación?
- (9) Si se usa un sistema de vigilancia, descríballo en detalle.
- (10) ¿Existen retenes contra incendio?

c) Material provisto a la guardia.

- (1) ¿De qué material dispone la guardia?
- (2) ¿Cuántos vehículos hay destinados para la guardia?
- (3) ¿Dónde se guardan los vehículos? ¿Están protegidos? ¿Quién está a cargo de su mantenimiento?
- (4) ¿Cómo está armada la guardia? ¿Cuál es la dotación de equipos y efectos clase V?
- (5) Describa el uniforme de la guardia. ¿Qué credenciales llevan?
- (6) ¿Qué equipo individual se entrega a cada hombre?
- (7) ¿De qué equipo adicional se dispone en la guardia de prevención?
- (8) ¿De qué medios se dispone para la guarda del material? ¿Qué medidas de seguridad se adoptan en la guardia de prevención?

d) Patrullas

- (1) ¿Cuántas patrullas son utilizadas en el elemento o actividad? ¿Recorren a pie o utilizan vehículos u otros medios?
- (2) ¿Cuál es la longitud o extensión del camino o zona para patrullar?
- (3) ¿Se usan itinerarios determinados e irregulares? Explique.
- (4) ¿Cuánto tiempo se invierte en un recorrido completo del camino o zona?
- (5) ¿Qué tiempo transcurre entre las inspecciones de lugares determinados a lo largo del camino o zona?
- (6) ¿De cuántos hombres se componen las patrullas?
- (7) ¿Qué órdenes especiales se aplican a cada patrulla?
- (8) ¿De qué medios de comunicación se dispone para la comunicación de una patrulla con otra y de cada patrulla con la guardia?
- (9) ¿Durante qué horas recorren las patrullas?
- (10) ¿Con qué rapidez puede ser enviado personal de reemplazo o adicional a una patrulla?
- (11) ¿Qué clase de personal compone las patrullas?
- (12) ¿Cuál es la duración del empleo y del recorrido de las patrullas?
- (13) ¿Qué sistema se emplea para que la guardia pueda localizar o ponerse en contacto inmediato con una patrulla?

- 2) **Puestos fijos.** Sistema, tipo y número de centinelas u otro personal de seguridad, su origen y adiestramiento, su empleo y vigencia, equipo, medios de comunicación, etc.
- a) ¿Cuál es la misión particular de la guardia?
 - b) ¿Cuántos puestos fijos existen en el elemento/actividad?
 - c) ¿Dónde están ubicados los puestos de guardia? ¿Son fijos o móviles? ¿Se apoyan mutuamente?
 - d) El puesto ¿ofrece protección contra el viento, la lluvia, etc.?
 - e) ¿Cuánto cantidad de personal entra apostado en cada puesto?
 - f) ¿De qué medios de comunicación se dispone entre los distintos puestos fijos? ¿Y entre cada puesto y la guardia?
 - g) ¿Qué órdenes especiales se aplican en cada puesto?
 - h) ¿Cuáles son las horas en las que están instalados los puestos?
 - i) ¿Cuál es la duración de los turnos de guardia en los puestos?
 - j) ¿Cuánto tiempo se tarda en enviar personal de refuerzo o adicional a cualquier puesto?
 - k) ¿Existe algún factor que pueda impedir la observación de todo el espacio asignado para su custodia a cada puesto fijo?
 - l) Compare el lapso durante el cual puede quedar interrumpida la observación con el tiempo de retardo que facilitan las barreras que protegen el área custodiada.
- 3) **Centros de control y vigilancia.** Ubicación, disponibilidad de facilidades de comunicaciones, servicios, recursos alternativos, personal, etc.
- a) ¿El elemento cuenta con un centro de control y vigilancia? Explique:
 - (1) ¿Se ubica en un lugar adecuado?
 - (2) ¿La guardia ejerce control sobre el centro de control y vigilancia?
 - (3) ¿Qué sistemas de comunicación tiene con la guardia?
 - (4) ¿Dispone de subsistemas de alimentación de resguardo?
 - (5) ¿Cuál es el horario de funcionamiento?
 - (6) ¿Tiene capacidad de grabar la captura de los sensores?
 - (7) ¿Qué sectores están cubiertos?
 - b) Personal.
 - (1) ¿Cuál es el personal asignado al centro de control y vigilancia?
 - (2) ¿Qué capacitación posee el personal asignado?
- 4) Todo otro aspecto necesario contenido o no en el reglamento.

Se deberán describir aquellos aspectos que sin estar comprendidos en la doctrina se han instrumentado o el sistema no contempla al sistema de guardia.

5) Procedimientos de control e identificación de personas.

Describe en detalle lo siguiente:

6) Control por parte del personal de guardia del organismo, oficina, depósito, etc. de las personas ajenas a la instalación.

Describe los métodos para el registro, identificación y control del personal ajeno a la instalación por parte del personal que integra el sistema de seguridad y de aquel personal que, si bien no integra el sistema aludido, debe colaborar.

7) Control de entrada, circulación y salida de personal del organismo.

Describe los métodos para el control de entrada, circulación y salida del personal, tanto del organismo como ajeno a la instalación por parte del personal que integra el sistema de seguridad y de aquel personal que, si bien no integra el sistema aludido, debe colaborar.

a) Con referencia al personal del elemento:

- (1) ¿Qué cantidad de personal compone el elemento? ¿Es militar o civil?
- (2) ¿Cuál es el promedio de cambios en el personal referido a renovación por baja, cesantía, cambios de destino, de puestos internos, etc.?
- (3) Durante el adiestramiento y antes de que empiecen a prestar servicio ¿se instruye suficientemente al personal de guardia a fin de tener la seguridad de que pueda reconocer al personal autorizado para entrar por sus puestos?
- (4) ¿Se comprueba si está capacitado para hacerlo? En caso afirmativo:
 - ¿Con qué frecuencia y quién hace esta comprobación?
 - ¿Puede el personal de guardia identificar a personal autorizado también por medio de su nombre?
 - ¿Son notificadas las guardias del personal que en lo sucesivo no podrán entrar por el puesto? En caso afirmativo: ¿En qué forma? ¿Cuándo? ¿Por quién son notificados?

b) ¿Se utiliza algún sistema de identificación en el elemento o actividad? En caso afirmativo:

- (1) Describe el sistema empleado (pase, credencial, cambio del pase por una insignia u otros).
- (2) Describe la identificación utilizada (credencial del organismo): color, tamaño, material y datos que aparecen en ella.
- (3) Los datos pueden incluir, por lo menos, nombre, rango o grado, señas particulares de identificación, huellas dactilares claras del dedo pulgar, la firma y la fotografía.
- (4) Si la identificación tiene fotografía del portador: ¿De qué tamaño es la fotografía? ¿Con qué frecuencia se la cambia? ¿De qué clase es la fotografía?
- (5) ¿Se entrega la identificación por un lapso determinado para cambiarla luego o se la hace por tiempo indefinido? Si es por un período determinado: ¿De qué duración? ¿Cómo se procede con la credencial caduca?
- (6) ¿Se hace conocer al interesado la forma de utilizar la identificación y el procedimiento en caso de pérdida o deterioro?

- (7) ¿Se hace constar en algún registro la expedición de las identificaciones? En caso afirmativo:
- ¿Quién controla este registro?
 - ¿Qué datos de identificación se hacen constar en el registro?
 - ¿Cuál es el nombre, cargo (grado y número del instituto en el Ejército, si es militar) y número del documento de identidad de la persona que firma la identificación?
- (8) ¿Se lleva un registro y, a su vez, se ha establecido un porcentaje de pérdidas o deterioros de identificaciones que haría aconsejable la adopción de un tipo nuevo de identificación o documento?
- (9) ¿Qué precauciones han sido tomadas para impedir la alteración o reproducción de la identificación? (Puede comprender una o varias de las siguientes medidas: un fondo especial en lo posible inalterable; en alguna parte tintas o tintes que puedan ser afectados por la aplicación de calor; numeración en sede; legalización por un funcionario que la autentique; características secretas conocidas solo por ciertos funcionarios; papel con marcas al agua; cordones o cintas superpuestos a la fotografía; papel que pierda su resistencia fibrosa al ser expuesto al calor; tinta que se corra o pierda el color al ser aplicado algún disolvente para eliminar el material plástico en identificaciones laminadas; tintas fluorescentes visibles únicamente a través de rayos ultravioletas; identificaciones de composiciones plásticas con la foto y los datos de identificación entre láminas de plástico, sello o firma puestos parcialmente sobre la foto y sobre la identificación, otros).
- (10) ¿Consta en la identificación la dirección y, si es posible, la garantía del franqueo para la devolución de la identificación en caso de pérdida?
- (11) ¿Existe un sistema de clave en la identificación (forma, tamaño, color, número, etc.) para señalar áreas, puertas de acceso, horas de trabajo, etc.? Describa el sistema en detalle.
- c) ¿Es utilizado algún sistema electrónico o automático de identificación? En caso afirmativo, explíquelo en detalle.
- d) ¿Se utiliza un sistema de pase sencillo (credencial del organismo, plaqueta de identificación) en el elemento o actividad? Si es así:
- (1) El personal de guardia, ¿controla individualmente?, ¿recibe y examina la credencial cuando entra una persona?
 - (2) ¿Cómo es exhibida la credencial o plaqueta de identificación al personal de guardia?
 - (3) Explique el sistema usado, inclusive quién es responsable de la custodia de las credenciales en caso de quedar retenida.
 - (4) ¿Qué medidas han sido tomadas para la admisión de personas autorizadas para entrar que hayan perdido sus credenciales, las hayan dejado olvidadas en la casa o por alguna otra razón no las tengan en su poder cuando se presentan al trabajo?
 - (5) ¿Es examinada la credencial por la guardia cuando el portador entra y sale de la instalación o actividad?
- e) ¿Se utiliza un sistema sencillo de identificación en el elemento o actividad? Si es así:
- (1) ¿Conserva siempre el interesado la credencial del elemento en su poder? En caso afirmativo: ¿Qué precauciones se toman para protegerla?

- (2) ¿Se retiene la credencial del organismo o la plaqueta de credencial en la instalación o actividad cuando sale el dueño? En caso afirmativo: ¿Cómo recibe el personal la identificación cuando se presenta al trabajo? ¿Cómo es cuidado cuando no está en poder del dueño?
- f) ¿Se usa el sistema de cambio de credencial del organismo por otro tipo de credencial interna? En caso afirmativo:
- (1) ¿Tienen ambos una fotografía del portador? ¿Son reproducidas del mismo negativo las dos fotografías?
- (2) ¿Compara el guardia la credencial del organismo y otra credencial interna cuando el portador entra y sale de la instalación o actividad?
- (3) Describa los modelos usados, indicando la similitud.
- (4) Explique el sistema detalladamente.

6) Control de entrada, circulación y salida de personal ajeno al organismo.

- a) ¿Qué sistema se emplea para el control de visitantes en el elemento o actividad?
- (1) ¿Cómo son identificados los visitantes del elemento o actividad?
- (2) ¿Por qué entradas se permite el acceso a los visitantes? ¿Cómo se consigue o se pone en vigor el sistema?
- (3) ¿Se lleva un registro de visitantes? En caso afirmativo, ¿qué información se registra?
- (4) ¿Dónde se conserva el registro de visitantes? ¿A cargo de quién está?
- (5) ¿Se exige que los visitantes entren y salgan por la misma puerta? ¿Cómo se hace cumplir esto?
- b) ¿Se utiliza un sistema de custodia para control de los visitantes? En caso afirmativo:
- (1) ¿Se emplea personal de custodia?
- (2) ¿Cuánto personal está asignado al elemento de custodia?
- (3) ¿Cómo se asigna la custodia a los visitantes?
- (4) El personal de custodia ¿es permanente?, ¿cómo se selecciona?
- (5) Este personal ¿está enterado de cuáles son las áreas excluidas para los visitantes?
- (6) El personal de custodia ¿está suficientemente familiarizado con la instalación o actividad para poder desempeñar su misión debidamente? Explíquelo.
- (7) ¿Cómo se identifica al personal de custodia?
- (8) ¿El personal está armado? Dé detalles.
- (9) ¿Permanece el hombre de custodia con el visitante durante todo el período de la visita? De no ser así, explique qué medidas de control son empleadas.
- (10) ¿Se mantiene un registro en el que figure el nombre tanto del visitante como del personal de custodia? ¿Durante cuánto tiempo es conservado este registro? ¿A cargo de quién está?
- c) ¿Qué medidas están previstas para el caso de que la custodia y el visitante se separen?

- (1) ¿Por quién es entregado el personal para custodia? ¿Es facilitado por la guardia?
¿Se le asigna otro por las personas que han de ser visitadas? Si es así:
- ¿Cómo se comprueba la visita al personal visitado?
 - ¿Cómo comprueba la guardia que la persona que desea entrar es un visitante autorizado?
 - ¿Se mantiene un registro en el que conste tanto el visitante como la persona que designó al hombre de custodia? ¿Quién lleva este registro? ¿Durante cuánto tiempo se conserva?
 - El hombre de custodia ¿acompaña al visitante cuando este regresa a la puerta de salida después de terminada la visita? Si no es así, explique qué medidas de precaución se toman.
 - ¿Qué medidas se toman si el visitante es separado de su custodia?
- d) ¿Existe un sistema de recorrido de patrullas para controlar que los visitantes se encuentren en el lugar establecido? En caso afirmativo:
- (1) ¿Mantiene la guardia un registro en el que se consigne la hora de entrada y de salida de todos los visitantes?
- (2) ¿Se le exige al visitante salir por la misma puerta por la que entró? En caso contrario, explique cómo es coordinado el sistema de control con la otra puerta antes de la salida del visitante.
- (3) La persona visitada ¿notifica a la guardia la hora de llegada y de salida del visitante del lugar visitado?
- (4) ¿Cómo puede la guardia determinar el tiempo máximo y mínimo necesario del recorrido del visitante desde la entrada al lugar de destino?
- e) ¿Se emplea un sistema de registro de visitantes? ¿Se hace entrega al visitante de un documento que deba ser visado por la persona que es visitada?
- (1) Describa la ficha de control que se da a los visitantes con inclusión de la información contenida en el formulario.
- (2) ¿Se entrega a cada visitante un formulario separado?
- (3) ¿Se llena el formulario por duplicado, uno para el visitante y otro para el que quede en la guardia?
- (4) La persona que autentica el formulario de paso en un lugar ¿consigna en el formulario el lugar siguiente para ser visitado? Explique.
- (5) ¿Durante cuánto tiempo son conservados estos formularios? ¿Quién los guarda?
- f) ¿Se hacen controles a los visitantes durante su permanencia en la instalación o actividad? ¿Por quién? ¿En qué condiciones? ¿En qué consiste la comprobación?
- g) ¿Cómo deberá proceder la guardia si en el elemento o actividad fuera encontrada una persona no autorizada a entrar o permanecer en ella?
- h) ¿Qué medidas se adoptarán en caso de pérdida de credenciales y/o actualizaciones y cómo se da de baja la extraviada para que no pueda ser nuevamente utilizada?

c. Sistema utilizado por la guardia o control de seguridad para el registro, identificación y control de los vehículos del personal del organismo o ajeno al mismo.

Describa los métodos de registro, identificación y control de los vehículos.

1) Registro de vehículos.

- a) ¿Se exige que sean registrados los vehículos pertenecientes al personal permanente?
En caso afirmativo:

(1) ¿Quién registra los vehículos? ¿Está instruido para hacerlo?

(2) ¿Qué aspectos se incluyen en el registro? ¿Qué requisitos previos son exigidos?
¿Dónde se ejecuta la inspección, con qué medios?

(3) ¿Se entrega una identificación para los vehículos del personal del organismo? En caso afirmativo, descríbala en detalle.

(4) ¿En qué forma se controla el registro de control? Explíquelo en detalle, incluyendo las transferencias de propiedad de vehículos, cambio de destinos, cese como empleados, etc.

(5) ¿Se registran los vehículos por un período determinado o por tiempo indefinido? Explíquelo en detalle.

2) Control de vehículos.

- a) ¿Se ha ordenado al personal que utilice la entrada de vehículos más cercana a su zona de trabajo o a alguna otra? Explíquelo.

b) ¿Han sido establecidos itinerarios específicos por los que deban o puedan desplazarse los vehículos particulares? Explique cómo se ejecuta.

c) ¿Han sido señaladas zonas para estacionamiento y se asignaron lugares de estacionamiento para el personal del organismo? Explíquelo en detalle.

3) Vehículos de visitantes.

- a) ¿Cómo se controlan los vehículos conducidos por los visitantes que concurren al elemento o actividad?

(1) ¿Se entrega una identificación al visitante para que sea colocada en su vehículo en lugar bien visible?

(2) Si se usan identificaciones para los vehículos: ¿cómo se controlan?

(3) ¿Se mantiene un registro de los vehículos que entran a la instalación? ¿Qué datos se consignan en el registro? ¿Quién lo lleva? ¿Durante cuánto tiempo se conserva el registro?

(4) ¿Hay entrada o zonas de estacionamiento especialmente reservadas para los visitantes? ¿Dónde están? ¿Cuántas hay?

- b) ¿Qué control se ejerce sobre los vehículos comerciales que tienen que entrar en la instalación o actividad?

(1) ¿Se provee de identificación de visitante a estos vehículos? Explíquelo en detalle.

(2) Si tienen que entrar vehículos comerciales en áreas de seguridad ¿Cómo son controlados?

- (3) ¿Se lleva un registro de vehículos comerciales? ¿Qué información se anota en él? ¿Quién efectúa las anotaciones? ¿Durante cuánto tiempo son conservados esos registros?

c) Inspecciones de vehículos.

- (1) Los vehículos de particulares o de visitantes ¿son inspeccionados alguna vez mientras permanecen en la instalación o actividad? ¿Cuándo? ¿En qué condiciones? ¿Quién lo hace? ¿Dónde se hace?

- (2) ¿Hay colocado algún aviso en forma bien visible en las entradas de la instalación o actividad que advierta al personal que está sujeto a registro mientras se halla en la instalación o actividad?

4) Otras particularidades.

Otras consideraciones que se hayan implementado o resulten necesarias a los fines de ejercer un control de los vehículos en las instalaciones.

SECCIÓN VII

CONCLUSIONES SOBRE ASPECTOS QUE AFECTAN LA SEGURIDAD

6. CONCLUSIONES SOBRE ASPECTOS QUE AFECTAN LA SEGURIDAD.

a. Conclusiones sobre los antecedentes relacionados con la seguridad.

Se considerarán los aspectos analizados para concluir acerca de los efectos sobre la seguridad del elemento u organismo. Resultará determinar la experiencia y conocimiento del personal que ejecuta el estudio, los antecedentes de otros estudios, inspecciones e incidentes de seguridad, etc.

b. Conclusiones sobre las características del área exterior.

- 1) Acerca de las características topográficas periféricas a la instalación.
- 2) Acerca de las características naturales que representan riesgos o amenazas para la seguridad.
- 3) Acerca de las condiciones antrópicas que representan riesgos o amenazas para la seguridad.

c. Conclusiones sobre las características del perímetro.

- 1) Acerca de la zona perimetral.

d. Conclusiones sobre las características del área interior.

- 1) Acerca de las características topográficas del área interior.
- 2) Acerca de las características naturales que representan riesgos o amenazas para la seguridad.
- 3) Acerca de las condiciones antrópicas que representan riesgos o amenazas para la seguridad.
- 4) Medidas de seguridad referidas a la seguridad física de las instalaciones.
- 5) Medidas de seguridad referidas a la seguridad del personal.
- 6) Medidas de seguridad referidas a la documentación y material clasificado.

7) Medidas de seguridad referidas a las comunicaciones.

8) Medidas de seguridad referidas a la criptografía.

e. Conclusiones sobre las áreas críticas.

1) Acerca de las áreas críticas.

f. Acerca del sistema de seguridad.

1) Sistema de guardia.

2) Control e identificación de personas.

3) Control e identificación de vehículos.

4) Otras particularidades del sistema.

g. Conclusiones en función de las amenazas detectadas y/o por actividad deducida.

Los aspectos precedentemente enumerados serán desarrollados mediante la formulación de conclusiones basadas en la información básica y actual descripta en los apartados 1. ANTECEDENTES RELACIONADOS CON EL ESTUDIO DE SEGURIDAD, 2. CARACTERÍSTICAS DEL ÁREA EXTERIOR, 3. CARACTERÍSTICAS DEL ÁREA INTERIOR, 4. CARACTERÍSTICAS PARTICULARES DEL ÁREA INTERIOR Y 5. SISTEMA DE SEGURIDAD, en el orden allí señalado.

En ningún caso se extraerán conclusiones que no estuvieren avaladas por la correspondiente información escrita.

SECCIÓN VIII

RECOMENDACIONES

7. RECOMENDACIONES.

En este apartado se señalan las medidas que se proponen, en materia de seguridad, basadas en las conclusiones consignadas en el apartado 6.

Estarán relacionadas con medidas para adoptar con respecto a:

a. Propuestas sobre el área exterior.

1) Acerca de las características topográficas periféricas a la instalación.

2) Acerca de las características naturales que representan riesgos o amenazas para la seguridad.

3) Acerca de las condiciones antrópicas que representan riesgos o amenazas para la seguridad.

b. Propuestas sobre el área interior.

1) Acerca de las características topográficas del área interior.

2) Acerca de las características naturales que representan riesgos o amenazas para la seguridad.

3) Acerca de las condiciones antrópicas que representan riesgos o amenazas para la seguridad.

- 4) Acerca de las medidas de seguridad referidas a la seguridad física de las instalaciones.
 - 5) Acerca de las medidas de seguridad referidas a la seguridad del personal.
 - 6) Acerca de las medidas de seguridad referidas a la documentación y material clasificado.
 - 7) Acerca de las medidas de seguridad referidas a las comunicaciones.
 - 8) Acerca de las medidas de seguridad referidas a la criptografía.
- c. Propuestas sobre las particularidades del área interior.
- 1) Acerca de la zona perimetral.
 - 2) Acerca de las áreas críticas.
- d. Acerca del sistema de seguridad.
- 1) Sistema de guardia.
 - 2) Control e identificación de personas.
 - 3) Control e identificación de vehículos.
 - 4) Otras particularidades del sistema.
- e. Conclusiones en función de las amenazas detectadas y/o por actividad deducida.

SECCIÓN IX

PRESUPUESTACIÓN INICIAL A LAS PROPUESTAS

8. PRESUPUESTACIÓN INICIAL A LAS PROPUESTAS.

Analizadas cada una de las propuestas se deberá confeccionar una presupuestación inicial posibilitando al Cte, Dir o J posteriores resoluciones.

Firma y aclaración

DOCUMENTOS AGREGADOS:

DISTRIBUIDOR:

MODELO DE INFORME DE UN ESTUDIO DE SEGURIDAD

SECRETO

Copia Nro:
Unidad u organismo
Lugar
Oportunidad
Clave de identificación

INFORME SOBRE ESTUDIO DE SEGURIDAD Nro 00/0000

UNIDAD U ORGANISMO: (Nombre y designación completa del elemento inspeccionado).

1. ANTECEDENTES RELACIONADOS CON EL ESTUDIO DE SEGURIDAD.

- a. Autoridad que ordena.
- b. Período abarcado por el estudio propiamente dicho.
- c. Personal que ejecuta la tarea, especificando grado, apellido, nombre y lugar de revista.
- d. Misión del elemento.
- e. Grado de seguridad impuesto y deseado.
- f. Estudios de seguridad (enunciarlos).
- g. Inspecciones de seguridad (enunciarlos).
- h. Otros antecedentes básicos existentes.

Se citarán los hechos ocurridos en el elemento que hubieren afectado la seguridad, consignándolos por separado, según estuvieren relacionados con la seguridad física, de la información, documentos y material clasificados, de los sistemas de comunicaciones y de las personas y del sistema informático.

2. CARACTERÍSTICAS DEL ÁREA EXTERIOR.

- a. Características topográficas periféricas.
- b. Características naturales y antrópicas de las áreas inmediatas que representen riesgos o amenazas para la seguridad actual o en el futuro inmediato.
- c. Riesgos o amenazas informáticas.

3. CARACTERÍSTICAS DEL PERÍMETRO Y ZONA PERIMETRAL.

a. Zona perimetral.

- 1) Barreras perimétricas. Describa en detalle, según sea posible, cómo se desarrolla el sistema de barrera por sectores. El perímetro comprende tres componentes claramente diferenciadas: la zona despejada interior, la barrera misma y la zona despejada exterior.

Se deberá dejar establecido claramente y en detalle los siguientes aspectos:

(a) Zona despejada interior.

Describa con detalle la extensión (ancho) de esta zona, ubicación de obstáculos, responsabilidad del mantenimiento, periodicidad con que se efectúan los trabajos necesarios, sectores iluminados, sectores sin iluminación, clase y altura o despeje de la vegetación existente, transitabilidad, determinar si corresponde a un sector público, privado o propio, tipo y cantidad de personas que habitualmente transitan, etc.

(b) Zona despejada exterior.

Describa con detalle la extensión (ancho) de esta zona, ubicación de obstáculos, responsabilidad del mantenimiento, periodicidad con que se efectúan los trabajos necesarios, sectores iluminados, sectores sin iluminación, clase y altura o despeje de la vegetación existente, etc.

(c) Barreras naturales.

(1) Obstáculos en el perímetro exterior. Describa en detalle cuáles son los accidentes topográficos que se desarrollan próximos al perímetro exterior del elemento u organismo y que sirven como barrera. Se deben considerar cursos o espejos de agua, vegetación, zanjas, mamelones, etc.

(2) Obstáculos en el perímetro interior. Describa en detalle cuáles son los accidentes topográficos que se desarrollan próximos al perímetro exterior del elemento u organismo y que sirven como barrera. Se deben considerar cursos o espejos de agua, vegetación, zanjas, mamelones, etc.

(d) Barreras artificiales.

Describa en detalle cada una de las estructuras y sistemas componentes de las barreras artificiales que se desarrollan en las instalaciones en estudio.

(1) Cercas. Tipo de material, características de su construcción, altura, etc.

(2) Lugares de ingresos y egresos habilitados. Puertas, portones, cerraduras, control de llaves, tipo de acceso, horarios habilitados para cada uno, control de la Gu Prev, etc.

(3) Sistemas de control de acceso.

Describa los controles de acceso perimetral, personal responsable de su mantenimiento, forma de identificar al medio que lo utiliza, control de acceso remoto, habilitación – negación del acceso, etc.

(4) Sistemas de alarma.

Describa clase y cantidad de sistemas de alarma, conexión con otros sistemas de seguridad, dispositivos, equipos de control y de señalización, sistemas de transmisión, sistema principal y de alternativa de fuentes de energía, etc.

(5) Sistemas de vigilancia a través de sensores.

Describa clase (activos y pasivos) y cantidad de sistemas de vigilancia y control, conexión con otros sistemas de seguridad, dispositivos, equipos de control y de vigilancia, sistemas de transmisión, sistema principal y de alternativa de fuentes de energía, etc.

(e) Barreras humanas.

(1) Sistema de guardia. Describa someramente el sistema de guardia en el sector perimetral, el detalle se debe desarrollar en el punto 5. SISTEMA DE SEGURIDAD.

(2) Otros sistemas. Describa someramente todo aquel sistema de seguridad que no corresponda con la guardia de prevención, el detalle se debe desarrollar en el punto 5. SISTEMA DE SEGURIDAD.

- (f) Barreras animales. Describir en detalle cómo se desarrolla este tipo de barrera. Se deben considerar los siguientes aspectos: tipo y cantidad de animales, instrucción de los animales, instrucción del personal al mantenimiento, adiestramiento y manejo de los animales, periodicidad en los relevos, etc.
- (g) Sistema de iluminación. Describa en detalle el sistema de alumbrado perimetral. Se deben considerar los siguientes aspectos: tipo de iluminación, ubicación, tipo de alumbrado (proyección deslumbrante, alumbrado directo, alumbrado indirecto, etc.), clase de lámparas, iluminación medida en lux, desarrollo de los conos de luz, personal afectado al mantenimiento, periodicidad con que se efectúan los controles, fuente de energía alternativa, conectividad a otros sistemas de seguridad (alarmas sonoras, alerta a centros de monitoreo, etc.
- (h) Todo otro aspecto necesario contenido o no en el presente reglamento.

4. CARACTERÍSTICAS DEL ÁREA INTERIOR.

a. Aspectos generales.

1) Características topográficas

Se considerarán aquellos aspectos topográficos que representan ventajas o desventajas para brindar la seguridad deseada.

2) Características naturales y antrópicas del área interior que representen riesgos o amenazas para la seguridad.

Se enumerarán aquellas características del ambiente geográfico o características antrópicas dentro de las instalaciones que representan una amenaza o riesgo para la seguridad de la información, personal o material.

Como ejemplo de ello se puede mencionar la existencia de bosques con riesgo de incendio, cursos de agua dentro de los predios del elemento u organismo con riesgo de inundaciones, depósitos de efectos peligrosos, depósitos de gas, de oxígeno, etc.

b. Medidas de seguridad referidas a la seguridad física de las instalaciones.

1) Seguridad física de las instalaciones.

a) Barreras.

Describa en detalle, según sea posible, lo siguiente:

(1) Edificios / oficinas / depósitos. Las superficies del mismo, cuántas y de qué material están construidas las puertas, cantidad y tipo de cerraduras, control de llaves, cantidad de ventanas, sistemas de cierre y alumbrado interno, etc.

(2) Todo otro aspecto necesario contenido o no en el presente reglamento.

b) Sistemas de acceso a las instalaciones.

Describa los sistemas de acceso utilizados para la habilitación a los distintos locales del elemento u organismo estudiado.

c) Sistemas de alarma contra personas ajenas al elemento y para vigilancia interna.

Describa los sistemas usados en los edificios y en las oficinas del organismo estudiado.

d) Sistemas de alarma contra incendios y de extinción de incendio. Describa lo siguiente:

- (1) Sistema de alarma contra incendios. Dispositivos, locales donde están instalados, redes, etc.**
- (2) En la guardia: servicio contra incendios; personal: tipo y número, su origen y adiestramiento, empleo y vigilancia; equipo o inspección; medios de comunicación; personal de reserva; etc.**
- (3) En el edificio: directivas, órdenes, etc., para el servicio contra incendios; suboficial encargado del servicio; equipo; inspecciones que se ejecutan; medios de comunicación; adiestramiento del personal; etc.**

Esta descripción debe limitarse estrictamente a un punto de vista de las medidas de seguridad física de la información, material o personal para proteger. Los detalles de estos sistemas estarán contenidos en las órdenes, directivas y procedimientos que se configuren, documentos que deberán estar referenciados en el estudio de seguridad.

e) Servicios.

(1) Energía eléctrica.

Describa someramente cuáles son los sistemas eléctricos principales y de alternativas que sean de interés a la seguridad en detalle la fuente y transmisión de la energía, medidas de emergencia, protección, etc.

(2) Suministro de agua.

Describa someramente cuáles son las fuentes y los sistemas de circulación del líquido, medidas de emergencia, protección, etc.

(3) Calefacción y combustible.

Describa someramente cuáles son los medios y el tipo de fuente del combustible, sistemas de circulación, medidas de emergencia, precauciones, etc.

(4) Telefonía.

Describa someramente cuáles son los servicios telefónicos públicos de empleo del elemento u organismo, cuáles son las distintas facilidades, ubicación y seguridad de las cajas o tableros, redes, etc.

Esta descripción debe limitarse estrictamente a un punto de vista de las medidas de seguridad física de la información, material o personal para proteger. Los detalles de estos sistemas estarán contenidos en las órdenes, directivas y procedimientos que se configuren, documentos que deberán estar referenciados en el estudio de seguridad.

c. Medidas de seguridad referidas a la seguridad del personal.

1) Seguridad de PMI.

2) Seguridad del personal con función crítica.

a) Personal con función crítica.

- (1) Cte, Dir, o J (grado, nombre y apellido). Ha ocupado este cargo desde: (fecha).
- (2) 2do Cte, Subdir o 2do J (grado, nombre y apellido). Ha ocupado este cargo desde: (fecha).
- (3) Oficial de personal (grado, nombre y apellido). Ha ocupado este cargo desde: (fecha).
- (4) Oficial de inteligencia (grado, nombre y apellido). Ha ocupado este cargo desde: (fecha).

- (5) Oficial de material (grado, nombre y apellido). Ha ocupado este cargo desde: (fecha).
- (6) Oficial de finanzas (grado, nombre y apellido). Ha ocupado este cargo desde: (fecha).
- (7) Oficial de claves y auxiliares (grado, nombre y apellido). Ha ocupado este cargo desde: (fecha).
- (8) Oficial de seguridad de la instalación (grado, nombre y apellido). Ha ocupado este cargo desde: (fecha).
- (9) Enc Dep Ars (grado, nombre y apellido). Ha ocupado este cargo desde: (fecha).
- (10) Enc Cen Com Fij (grado, nombre y apellido). Ha ocupado este cargo desde: (fecha).
- (11) Oficial de informática (grado, nombre y apellido). Ha ocupado este cargo desde: (fecha).
- (12) Oficial de comunicaciones (grado, nombre y apellido). Ha ocupado este cargo desde: (fecha).
- (13) Otros (grado, nombre y apellido). Ha ocupado este cargo desde: (fecha).

3) Educación e instrucción del personal en las MSCI.

a. Educación e instrucción en cuanto a contrainteligencia.

(Describa en detalle el programa de educación en cuanto a contrainteligencia que se ha establecido y llevado a cabo)

Nro	GFH	Med Seg referidas a:	Temario	Participantes	Resultados alcanzados	Obs

b. Programa de ejercicios.

Describa en detalle la incorporación de temas de medidas de seguridad de contrainteligencia en los ejercicios del elemento u organismo.

c. Grado de educación e instrucción.

Desarrollar una apreciación acerca del grado de educación alcanzado en el elemento u organismo.

d. Medidas de seguridad referidas a la documentación y material clasificado.

1) Seguridad de la información contenida en documentos y/o materiales clasificados.

a) Clasificación de seguridad de la información.

En el organismo se guarda la información clasificada en los siguientes lugares:

(1) Documentación:

Local (Nro y designación)	Clasificación de la información / Material	Tipo de soporte	Ubicación específica
Ejemplo:			
Nro 23 – J Un	SECRETO	Digital	PC y CD
	RESERVADO	Papel	Armario Nro 2
Nro 25 – Of Icia	ES y C	Papel	Armario Nro 1
	ES y C	Papel	Caja fuerte
Nro 26 – Of Op	SECRETO	Papel	Armario Nro 2
	RESERVADO	Digital	Armario Nro 2
	RESERVADO	Cinta de video	Armario Nro 1

(2) Material:

Local (Nro y designación)	Clasificación de la información / Material	Tipo de soporte	Ubicación específica
Ejemplo:			
Nro 3 – Dep Ars	SECRETO	Papel y material	Estante Nro 22
	RESERVADO	Papel	Armario Nro 2
Nro 2 – Depósito de Munición	PÚBLICO MILITAR	Material	Estante Nro 32
	PÚBLICO MILITAR	Material	Sector A
Nro 25 – Of Icia	ES y C	Material	Caja fuerte

(3) Varios:

Local (Nro y designación)	Clasificación de la información / Material	Tipo de soporte	Ubicación específica
Ejemplo:			
Sala Histórica	RESERVADO	Material	Vitrina Nro 1
	RESERVADO	Papel	Estantería Nro 3
Nro 23 – J Un	PÚBLICO MILITAR	Material	Panoplia Nro 1

Dentro de cada uno se especificarán: muebles, estanterías, cajas de seguridad, volumen ocupado en m³, depósitos, etc.

b) Sistema para el tratamiento de información clasificada.

Describa en detalle los métodos empleados en el manejo de cada categoría de la información clasificada que se recibe en la unidad estudiada.

c) Guarda de la información clasificada.

(Describa en detalle los medios y los procedimientos empleados para guardar la información clasificada dentro del organismo estudiado).

d) Distribución o difusión.

(Describa en detalle los procedimientos empleados para la distribución interna de la información clasificada o difusión de inteligencia).

e) Preparación.

(Describa en detalle cómo son redactados los documentos y cómo se preparan, dentro del organismo, los elementos que contienen información clasificada. Indique si han sido tenidos en cuenta los aspectos contenidos en este reglamento).

f) Marcación.

(Describa en detalle cómo son colocadas las leyendas para su debida protección de la documentación o material clasificado preparado; este informe deberá incluir las copias en borrador, las notas de taquígrafo, si las hay, etc.).

g) Reproducción.

(Describa en detalle cómo es reproducida y marcada la información clasificada contenida en documentos o material).

h) Reclasificación.

(Describa en detalle el procedimiento usado para revisar y reclasificar la información clasificada; incluya la responsabilidad).

i) Destrucción normal.

(Describa en detalle el procedimiento empleado para llevar a cabo la destrucción normal de la información clasificada y del material desechado: incluya la responsabilidad, los registros, etc.).

j) Evacuación y destrucción de emergencia del material clasificado.

(Describa en detalle qué medidas se han determinado en las órdenes para esta eventualidad).

e. Medidas de seguridad referidas a informática.

1) Seguridad de los dispositivos informáticos.

- a. Medidas de seguridad adoptadas con las máquinas y dispositivos de escritorio.**
- b. Medidas de seguridad adoptadas con las computadoras portátiles.**
- c. Medidas de seguridad adoptadas con los dispositivos de mano.**
- d. Medidas de seguridad adoptadas con las terminales.**
- e. Medidas de seguridad adoptadas con los centros de cómputos.**

2) Sistema de redes LAN. Seguridad.

3) Seguridad de los sistemas operativos.

4) Seguridad de la información.

5) Sistemas de resguardo de la información y sistemas operativos.

Se describirán cuáles son los dispositivos de almacenamiento removible, identificación, guarda, conservación, periodicidad del back up, responsable, cantidad de copias, etc.

6) Sistemas de acceso.

7) Medidas de seguridad de aquellos dispositivos con conexión a la Intranet / EA.

8) Medidas de seguridad de aquellos dispositivos con conexión a la Internet.

f. Medidas de seguridad referidas a las comunicaciones.

1) Medidas de seguridad de los sistemas de comunicaciones. Medios de comunicación.

a) Medios de comunicaciones principales, de alternativa y de emergencia que están disponibles en el elemento u organismo para la recepción y transmisión de información.

Descripción de los sistemas disponibles, enlaces, seguridad física de los equipos, campo de antenas, etc.

b) Medios de comunicaciones principales, de alternativa y de emergencia que están disponibles en el sistema de guardia en apoyo al sistema de seguridad.

Descripción de los sistemas de comunicaciones en apoyo al sistema de seguridad, enlaces, comprobaciones, seguridad física de los equipos, campo de antenas, nivel de capacitación del personal que habitualmente debe emplearlos, etc.

c) Personal empleado para operar y mantener los medios de comunicación, inclusive el tipo y número, previsión y autorización para su uso, vigilancia establecida, etc.

Enumerar al personal responsable de la operación y mantenimiento de los equipos de comunicaciones fijos y móviles, grado de capacitación, educación de contrainteligencia, etc.

d) Medios de comunicación para el tráfico informático, incluyendo procedimientos de operación y normativa vigente.

Describir los sistemas de comunicaciones y enlaces informáticos para la transmisión de comunicaciones. Describir los sistemas operativos, criptografía específica, procedimientos de operación, normativa vigente, etc.

e) Sistemas de provisión de energía alternativa para asegurar el desarrollo sostenido de la operación.

Describir los sistemas de alternativa para la provisión de energía eléctrica para asegurar la continuidad de operación de los sistemas de comunicaciones y otros equipos asociados.

g. Medidas de seguridad referidas a la criptografía.

Describir someramente el cumplimiento de las medidas de seguridad criptográfica, la documentación que corresponda, los procedimientos adoptados, el personal que interviene. La descripción en detalle será tratada en el punto 4. CARACTERÍSTICAS PARTICULARES DEL ÁREA INTERIOR.

5. ZONAS CRÍTICAS.

a. Áreas o zonas críticas.

Las áreas críticas constituyen aquellos lugares que por la información y material que allí se almacena o tramita o personal que allí permanece o desenvuelve sus actividades debe ser considerada especialmente. Cada área debe tratarse desde cada uno de los distintos conceptos que las medidas de seguridad de contrainteligencia consideran. En este sentido, cuando se estudie para su evaluación, debe considerarse lo siguiente:

Área crítica Nro 1: Oficina del Cte / Dir / J elemento u organismo.

- 1) Medidas de seguridad física de la instalación.
- 2) Medidas de seguridad referidas a la seguridad del personal.
- 3) Medidas de seguridad referidas a la documentación y material clasificado.
- 4) Medidas de seguridad referidas a la informática.
- 5) Medidas de seguridad referidas a las comunicaciones.

Área crítica Nro 2: Oficina del 2do Cte / Subdir / 2do J elemento u organismo.

- 1) Medidas de seguridad física de la instalación.
- 2) Medidas de seguridad referidas a personal.
- 3) Medidas de seguridad referidas a la documentación y material clasificado.
- 4) Medidas de seguridad referidas a la informática.
- 5) Medidas de seguridad referidas a las comunicaciones.

Área crítica Nro 3: Oficina del área de inteligencia.

- 1) Medidas de seguridad física de la instalación.
- 2) Medidas de seguridad referidas a personal.
- 3) Medidas de seguridad referidas a la documentación y material clasificado.
- 4) Medidas de seguridad referidas a la informática.
- 5) Medidas de seguridad referidas a las comunicaciones.

Área crítica Nro 4: Depósito central de arsenales.

Área crítica Nro 5: Polvorines.

Área crítica Nro 6: Centro de comunicaciones fijo.

Área crítica Nro 7: Cifrario.

Área crítica Nro XX:

Área crítica Nro XX:

6. SISTEMA DE SEGURIDAD.

Describa en detalle cómo se estructura el sistema de seguridad, el sistema de guardia y todos aquellos procedimientos de los que se valen los sistemas de seguridad para llevar a cabo su cometido.

a. Sistema de seguridad.

Describa cómo se estructura el sistema de seguridad y planes previstos, incluyendo a aquel personal y medios que sin formar parte de la Gu Prev complementan o suplementan a la misma. Es necesario considerar, entre otros aspectos, los siguientes puntos:

- 1) Servicios de seguridad guarnicionales (otros sistemas de guardia, jefes de día, corresponsables del sistema de comunicaciones guarnicionales, etc.).
- 2) Planes de recuperación por parte de los propios medios y aquellos en los que participan otros elementos u organismos de la Fuerza.
- 3) Convenios y acuerdos con fuerzas de seguridad, fuerzas policiales sistemas de salud para responder a determinadas situaciones.

b. Sistema de guardia.

- 1) **Guardia.** Sistema, tipo y número de centinelas u otro personal de seguridad, su origen y adiestramiento, su empleo y vigencia, equipo, medios de comunicación, etc.
- 2) **Puestos fijos.** Sistema, tipo y número de centinelas u otro personal de seguridad, su origen y adiestramiento, su empleo y vigencia, equipo, medios de comunicación, etc.
- 3) **Centros de control y vigilancia.** Ubicación, disponibilidad de facilidades de comunicaciones, servicios, recursos alternativos, personal, etc.
- 4) **Todo otro aspecto necesario contenido o no en el reglamento.**

c. Procedimientos de control e identificación de personas.

Describa en detalle lo siguiente:

- 1) **Control por parte del personal de guardia del organismo, oficina, depósito, etc. de las personas ajenas a la instalación.**

Describa los métodos para el registro, identificación y control del personal ajeno a la instalación por parte del personal que integra el sistema de seguridad y de aquel personal que, si bien no integra el sistema aludido, debe colaborar.

- 2) **Control de entrada, circulación y salida de personal, tanto del organismo como ajeno.**

Describa los métodos para el control de entrada, circulación y salida del personal, tanto del organismo como ajeno a la instalación por parte del personal que integra el sistema de seguridad y de aquel personal que, si bien no integra el sistema aludido, debe colaborar.

d. Procedimientos de control e identificación de vehículos.

Describa en detalle lo siguiente:

- 1) **Sistema utilizado por la guardia o control de seguridad para el registro, identificación y control de los vehículos del personal del organismo o ajeno al mismo.**

Describa los métodos de registro, identificación y control de los vehículos.

- 2) **Lugares habilitados y prohibidos para el acceso y tránsito de vehículos particulares.**

Describa cuáles son los lugares habilitados y prohibidos para el estacionamiento y tránsito de los vehículos.

- 3) **Otras particularidades.**

Otras consideraciones que se hayan implementado o resulten necesarias a los fines de ejercer un control de los vehículos en las instalaciones.

7. CONCLUSIONES SOBRE ASPECTOS QUE AFECTAN LA SEGURIDAD.

a. Conclusiones sobre los antecedentes relacionados a la seguridad.

Se considerarán los aspectos analizados para concluir acerca de los efectos sobre la seguridad del elemento u organismo. Resultará determinar la experiencia y conocimiento del personal que ejecuta el estudio, los antecedentes de otros estudios, inspecciones e incidentes de seguridad, etc.

b. Conclusiones sobre las características del área exterior.

- 1) Acerca de las características topográficas periféricas a la instalación.**
- 2) Acerca de las características naturales que representan riesgos o amenazas para la seguridad.**
- 3) Acerca de las condiciones antrópicas que representan riesgos o amenazas para la seguridad.**

c. Conclusiones sobre las características del perímetro.

- 1) Acerca de la zona perimetral.**

d. Conclusiones sobre las características del área interior.

- 1) Acerca de las características topográficas del área interior.**
- 2) Acerca de las características naturales que representan riesgos o amenazas para la seguridad.**
- 3) Acerca de las condiciones antrópicas que representan riesgos o amenazas para la seguridad.**
- 4) Medidas de seguridad referidas a la seguridad física de las instalaciones.**
- 5) Medidas de seguridad referidas al personal.**
- 6) Medidas de seguridad referidas a la documentación y material clasificado.**
- 7) Medidas de seguridad referidas a las comunicaciones.**
- 8) Medidas de seguridad referidas a la criptografía.**

e. Conclusiones sobre las áreas críticas.

- 1) Acerca de las áreas críticas.**

f. Acerca del sistema de seguridad.

- 1) Sistema de guardia.**
- 2) Control e identificación de personas.**
- 3) Control e identificación de vehículos.**
- 4) Otras particularidades del sistema.**

g. Conclusiones en función de las amenazas detectadas y/o por actividad deducida.

Los aspectos precedentemente enumerados serán desarrollados mediante la formulación de conclusiones basadas en la información básica y actual descripta.

En ningún caso se extraerán conclusiones que no estuvieren avaladas por la correspondiente información escrita.

8. RECOMENDACIONES.

En este apartado se consignarán las medidas que se proponen, en materia de seguridad, basadas en las conclusiones consignadas en el apartado 6.

Estarán relacionadas con medidas para adoptar con respecto a:

a. Propuestas sobre el área exterior.

- 1) Acerca de las características topográficas periféricas a la instalación.**
- 2) Acerca de las características naturales que representan riesgos o amenazas para la seguridad.**
- 3) Acerca de las condiciones antrópicas que representan riesgos o amenazas para la seguridad.**

b. Propuestas sobre el área interior.

- 1) Acerca de las características topográficas del área interior.**
- 2) Acerca de las características naturales que representan riesgos o amenazas para la seguridad.**
- 3) Acerca de las condiciones antrópicas que representan riesgos o amenazas para la seguridad.**
- 4) Acerca de las medidas de seguridad referidas a la seguridad física de las instalaciones.**
- 5) Acerca de las medidas de seguridad referidas al personal.**
- 6) Acerca de las medidas de seguridad referidas a la documentación y material clasificado.**
- 7) Acerca de las medidas de seguridad referidas a las comunicaciones.**
- 8) Acerca de las medidas de seguridad referidas a la criptografía.**

c. Propuestas sobre las particularidades del área interior.

- 1) Acerca de la zona perimetral.**
- 2) Acerca de las áreas críticas.**

d. Acerca del sistema de seguridad.

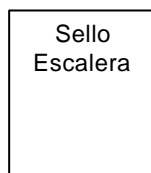
- 1) Sistema de guardia.**
- 2) Control e identificación de personas.**
- 3) Control e identificación de vehículos.**
- 4) Otras particularidades del sistema.**

e. Conclusiones en función de las amenazas detectadas y/o por actividad deducida.

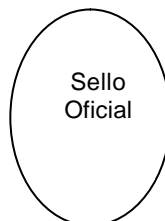
9. PRESUPUESTACIÓN INICIAL A LAS PROPUESTAS.

Analizadas cada una de las propuestas, se deberá confeccionar una presupuestación inicial posibilitando al Cte, Dir o J posteriores resoluciones.

AGREGADOS:



Lugar y fecha.



Firma y aclaración

DISTRIBUIDOR:

MODELO DE PRESUPUESTACIÓN INICIAL

Copia Nro:
Unidad
Lugar
Oportunidad
Clave

APÉNDICE 01 AL ANEXO 00/0000 (Presupuestación inicial del sistema de seguridad)
AL INFORME DEL ESTUDIO DE SEGURIDAD DEL CUARTEL.....Nro 00/0000

N r o	PRODUCTO	CANTIDAD	UBICACIÓN	VALORIZACIÓN SUGERIDA	FUENTE	OBSERVACIONES
SEGURIDAD FÍSICA DE LAS INSTALACIONES (BARRERAS ARTIFICIALES)						
ETAPA XX - PERÍMETRO E INSTALACIONES DEL CUARTEL.....						
01						
02						
03						

N r o	PRODUCTO	CANTIDAD	UBICACIÓN	VALORIZACIÓN SUGERIDA	FUENTE	OBSERVACIONES
SEGURIDAD FÍSICA DE LAS INSTALACIONES (BARRERAS NATURALES)						
ETAPA XX - PERÍMETRO E INSTALACIONES DEL CUARTEL.....						
01						
02						
03						

N r o	PRODUCTO	CANTIDAD	UBICACIÓN	VALORIZACIÓN SUGERIDA	FUENTE	OBSERVACIONES
SEGURIDAD FÍSICA DE LAS INSTALACIONES (BARRERAS HUMANAS)						
ETAPA XXI - PERÌMETRO E INSTALACIONES DEL CUARTEL.....						
01						
02						
03						

N r o	PRODUCTO	CANTIDAD	UBICACIÓN	VALORIZACIÓN SUGERIDA	FUENTE	OBSERVACIONES
SEGURIDAD FÍSICA DE LAS INSTALACIONES (BARRERAS ANIMALES)						
ETAPA XX - PERÌMETRO E INSTALACIONES DEL CUARTEL.....						
01						
02						
03						

VALORIZACIÓN SUGERIDA TOTAL DE MATERIAL PROPUESTO PARA LA SEGURIDAD PERIMETRAL	\$0,0
--	-------

VALORIZACIÓN SUGERIDA TOTAL DE MATERIAL PROPUESTO PARA SEGURIDAD INTERNA	\$ 0,0
	U\$S 0,0

N r o	PRODUCTO	CANTIDAD	UBICACIÓN	VALORIZACIÓN SUGERIDA	FUENTE	OBSERVACIONES
SEGURIDAD DE LAS PERSONAS						
ETAPA XX - SEGURIDAD DE LAS PERSONAS MUY IMPORTANTES						
01						
02						
03						

N r o	PRODUCTO	CANTIDAD	UBICACIÓN	VALORIZACIÓN SUGERIDA	FUENTE	OBSERVACIONES
SEGURIDAD DE LAS PERSONAS						
ETAPA XX - SEGURIDAD DE LAS PERSONAS CON FUNCIONES CRÍTICAS						
01						
02						
03						

N r o	PRODUCTO	CANTIDAD	UBICACIÓN	VALORIZACIÓN SUGERIDA	FUENTE	OBSERVACIONES
SEGURIDAD DE LAS PERSONAS						
ETAPA XX - SEGURIDAD DE LAS PERSONAS DEL INSTRUMENTO MILITAR						
01						
02						
03						

N r o	PRODUCTO	CANTIDAD	UBICACIÓN	VALORIZACIÓN SUGERIDA	FUENTE	OBSERVACIONES
SEGURIDAD DE COMUNICACIONES						
ETAPA XX - SEGURIDAD DE LAS COMUNICACIONES						
01						
02						
03						

N r o	PRODUCTO	CANTIDAD	UBICACIÓN	VALORIZACIÓN SUGERIDA	FUENTE	OBSERVACIONES
SEGURIDAD INFORMÁTICA						
ETAPA XX - SEGURIDAD DE LAS PERSONAS DEL INSTRUMENTO MILITAR						
01						
02						
03						

VALORIZACIÓN SUGERIDA TOTAL DE MATERIAL PROPUESTO PARA INSTALACIONES DEL CUARTEL	\$ 0,0
--	--------

VALORIZACIÓN SUGERIDA TOTAL *	\$ 0,0	U\$S 0,0
VALORIZACION TOTAL CON LA APLICACIÓN DE COEFICIENTE	\$ 0,0	U\$S 0,0

NOTA: Se incluirán los aspectos necesarios que permitan disponer de los elementos de juicio para adoptar una resolución.

Jefe Equipo Est Seg

Oficial de Inteligencia / RI Mte 35

DISTRIBUIDOR:

FORMATO DEL PLAN DE MEDIDAS DE SEGURIDAD DE CONTRAINTELIGENCIA

SECRETO

Copia Nro
Unidad u organismo
Lugar
Oportunidad
Clave de identificación

PLAN DE MEDIDAS DE SEGURIDAD DE CONTRAINTELIGENCIA Nro 00/0000

UNIDAD U ORGANISMO: (Nombre y designación completa del elemento).

FASE O PERIODO DE LA OPERACIÓN	MEDIDAS DE SEGURIDAD INCLUIDAS EN EL PON QUE DEBEN ENFATIZARSE	MEDIDAS ADICIONALES QUE DEBEN ADOPTARSE	UNIDADES U ORGANISMOS RESPONSABLES DE LA EJECUCIÓN										INSTRUCCIONES, NOTAS PARA ACCIONES FUTURAS Y MEDIDAS DE COORDINACIÓN DE EM A ESTABLECER

EJEMPLO ESQUEMÁTICO DE UN PLAN DE MEDIDAS DE SEGURIDAD DE CONTRAINTELIGENCIA

Copia Nro
Comando
Lugar
Fecha – Hora
Clave de Identificación

PLAN DE MEDIDAS DE SEGURIDAD DE CONTRAINTELIGENCIA

FASE O PERIODO DE LA OPERACIÓN	MEDIDAS DE SEGURIDAD INCLUIDAS EN EL PON QUE DEBEN ENFATIZARSE	MEDIDAS ADICIONALES QUE DEBEN ADOPTARSE	UNIDADES U ORGANISMOS RESPONSABLES DE LA EJECUCION											INSTRUCCIONES, NOTAS PARA ACCIONES FUTURAS Y MEDIDAS DE COORDINACIÓN DE EM A ESTABLECER
			RI 32	RI 38	RI 40	GA 10	Ca Ing 10	Ca Com 10	Etc.	Etc.	Etc.	Etc.	Etc.	
1. TRANSPORTE POR TREN	1. SEGURIDAD MILITAR. a. Disciplina del secreto.	a. Distribuir nuevos códigos de identificación de unidades.	X	X	X	X	X	X	X	X	X	X	X	Los órganos de EM y unidades dependientes retirarán del Dpto II lcia las planillas con las claves de identificación
		b. La identificación del tren y vagones que corresponda a cada elemento se establecerá por una clave.	X	X	X	X	X	X	X	X	X	X	X	

FASE O PERIODO DE LA OPERACIÓN	MEDIDAS DE SEGURIDAD INCLUIDAS EN EL PON QUE DEBEN ENFATIZARSE	MEDIDAS ADICIONALES QUE DEBEN ADOPTARSE	UNIDADES U ORGANISMOS RESPONSABLES DE LA EJECUCION											INSTRUCCIONES, NOTAS PARA ACCIONES FUTURAS Y MEDIDAS DE COORDINACIÓN DE EM A ESTABLECER
			RI 32	RI 38	RI 40	GA 10	Ca Ing 10	Ca Com 10	Etc.	Etc.	Etc.	Etc.	Etc.	
	b. Seguridad de personas	a. Se modifica el PON de contrainteligencia. 1) No se permitirá al personal descender del tren en ninguna oportunidad hasta su arribo a destino. 2) No se aceptarán alimentos de personal civil que se acerque al tren.	X	X	X	X	X	X	X	X	X	X	X	
			X	X	X	X	X	X	X	X	X	X	X	

FASE O PERIODO DE LA OPERACIÓN	MEDIDAS DE SEGURIDAD INCLUIDAS EN EL PON QUE DEBEN ENFATIZARSE	MEDIDAS ADICIONALES QUE DEBEN ADOPTARSE	UNIDADES U ORGANISMOS RESPONSABLES DE LA EJECUCION											INSTRUCCIONES, NOTAS PARA ACCIONES FUTURAS Y MEDIDAS DE COORDINACIÓN DE EM A ESTABLECER
	c. Seguridad de documentos	3) Durante las horas de oscuridad se bajarán las ventanillas y persianas.	X	X	X	X	X	X	X	X	X	X	X	
		b. ----- a. Los cofres con documentación clasificada, cerrados y precintados se entregarán en el vagón Nro 4. b. -----	X	X	X	X	X	X	X	X	X	X	X	

FASE O PERIODO DE LA OPERACIÓN	MEDIDAS DE SEGURIDAD INCLUIDAS EN EL PON QUE DEBEN ENFATIZARSE	MEDIDAS ADICIONALES QUE DEBEN ADOPTARSE	UNIDADES U ORGANISMOS RESPONSABLES DE LA EJECUCION											INSTRUCCIONES, NOTAS PARA ACCIONES FUTURAS Y MEDIDAS DE COORDINACIÓN DE EM A ESTABLECER
		a. Se establecerá un vagón con carga falsa que aparente munición y que tendrá su guardia visible.	X	X	X	X	X	X	X	X	X	X	X	
		b. La munición será embarcada en vagones independientes y enganchados como último vagón.	X	X	X	X	X	X	X	X	X	X	X	

RECTIFICACIONES

Rect Nro	Fecha			B. M.	Pág.	Nro	Forma en que se incluirá en el reglamento
	Día	Mes	Año				

[illegible]