

ANEXO "A"
NORMAS Y ESTÁNDARES DE SEGURIDAD INFORMÁTICA

DIRECTIVA PERMANENTE N° 200-12
POLÍTICA DE SEGURIDAD INFORMÁTICA PARA LAS FUERZAS
MILITARES

MINISTERIO DE DEFENSA NACIONAL
FUERZAS MILITARES DE COLOMBIA
COMANDO GENERAL
BOGOTÁ D.C., DICIEMBRE-2006

TABLA DE CONTENIDO

	Pág.
1. POLÍTICAS DE USO ACEPTABLE -PUA-	6
2. SEGURIDAD ORGANIZACIONAL	8
2.1 INFRAESTRUCTURA DE SEGURIDAD DE LA INFORMACIÓN	8
2.1.1 Foro de seguridad de la información	8
2.1.2 Coordinación de la seguridad de la información	9
2.1.3 Responsabilidades en seguridad de la información	9
2.1.4 Proceso de autorización para los servicios de procesamiento de información	10
2.1.5 Asesoramiento especializado en materia de seguridad de la información	10
2.1.6 Cooperación entre organizaciones	10
2.1.7 Revisión independiente de la seguridad de la información	11
2.2 SEGURIDAD FRENTE AL ACCESO POR PARTE DE TERCEROS	11
2.2.1 Identificación de riesgos del acceso de terceras partes	11
2.2.2 Requerimientos de seguridad en contratos con terceros	13
3. CLASIFICACIÓN Y CONTROL DE ACTIVOS	16
3.1 RESPONSABILIDAD POR RENDICIONES DE CUENTAS DE LOS ACTIVOS	16
3.1.1 Inventario de activos	16
3.2 CLASIFICACIÓN DE LA INFORMACIÓN	17
3.2.1 Pautas para clasificación y manejo de la información	17
3.2.2 Rotulado y manejo de información	18
3.2.3 Control de hardware	18
3.2.4 Control de software	18
3.2.5 Control de medios de almacenamiento	18
3.3 MATRIZ DE RIESGOS	19
4. SEGURIDAD DE LOS RECURSOS HUMANOS	19
4.1 ANTES DE LA RELACIÓN LABORAL	19
4.2 DURANTE LA RELACIÓN LABORAL	20
4.2.1 Responsabilidades del jefe de la unidad respectiva	20
4.3 AL TÉRMINO DE LA RELACIÓN LABORAL	20
4.3.1 Devolución de activos	20
5. SEGURIDAD FÍSICA Y DE ENTORNO	21
5.1 ÁREAS SEGURAS O RESTRINGIDAS	21
5.1.1 Perímetro de seguridad física	21
5.1.2 Controles de acceso físico	22
5.1.3 Seguridad de oficinas, recintos y servicios	23
5.1.4 Protección contra amenazas externas y ambientales	23
5.1.5 Trabajo en áreas seguras o restringidas	23
5.1.6 Áreas de carga, despacho y acceso público	24
5.2 SEGURIDAD DE LOS EQUIPOS	24
5.2.1 Ubicación y protección de los equipos	25
5.2.2 Servicios de soporte	25
5.2.3 Seguridad del cableado	26
5.2.4 Mantenimiento de los equipos	26

5.2.5	Seguridad de los equipos fuera de las instalaciones	27
5.2.6	Seguridad en la reutilización o eliminación de los equipos	27
5.2.7	Retiro de Propiedad	28
6.	COMUNICACIÓN Y ADMINISTRACIÓN DE OPERACIONES DE SISTEMAS INFORMÁTICOS	28
6.1	PROCEDIMIENTOS Y RESPONSABILIDADES OPERATIVAS	28
6.1.1	Documentación de los procedimientos operativos	28
6.1.2	Control de cambios en las operaciones	29
6.1.3	Procedimiento de manejo de incidentes informáticos	29
6.1.4	Separación de funciones	29
6.1.5	Separación entre las instalaciones de desarrollo e instalaciones operativas	30
6.2	PLANIFICACIÓN Y APROBACIÓN DEL SISTEMA	30
6.2.1	Planificación de la capacidad	30
6.2.2	Aprobación del sistema	31
6.3	PROTECCIÓN CONTRA SOFTWARE MALICIOSO	31
6.3.1	Controles contra software malicioso	31
6.3.2	Control contra códigos móviles	32
6.4	MANTENIMIENTO	32
6.4.1	Respaldo de la información	33
6.4.2	Registro de actividades del personal operativo	33
6.4.3	Registro de fallas	33
6.5	ADMINISTRACIÓN DE LA RED	34
6.5.1	Controles de redes	34
6.6	ADMINISTRACIÓN Y SEGURIDAD DE LOS MEDIOS DE ALMACENAMIENTO	37
6.6.1	Administración de Medios Informáticos Removibles	37
6.6.2	Eliminación de medios informáticos	38
6.6.3	Procedimientos del manejo de la información	38
6.6.4	Seguridad de la documentación del sistema	38
6.7	INTERCAMBIOS DE INFORMACIÓN Y SOFTWARE	39
6.7.1	Acuerdos de intercambios de información y software	40
6.7.2	Seguridad de los medios en tránsito	40
6.7.3	Seguridad del correo electrónico	40
6.7.4	Sistemas de acceso público	41
7.	CONTROL DE ACCESO	41
7.1	REQUERIMIENTOS PARA EL CONTROL DE ACCESO	41
7.1.1	Políticas del control de acceso	41
7.2	ADMINISTRACIÓN DE ACCESO DE USUARIOS	42
7.2.1	Registro de usuarios	42
7.2.2	Administración de privilegios	43
7.2.3	Administración de contraseñas de usuario	44
7.2.4	Revisión de derechos de acceso a usuario	44
7.3	RESPONSABILIDADES DEL USUARIO	44
7.4	RESPONSABILIDAD DE LOS ADMINISTRADORES DEL SISTEMA	45
7.5	USO DE CONTRASEÑAS	46
7.5.1	Uso de cuentas sin password ó passwords por defecto	46
7.5.2	Uso de passwords reusables	47
7.5.3	Uso de one-time passwords	47

7.5.4	Uso de cuentas de guest (ó invitados)	47
7.6	EQUIPOS DESATENDIDOS EN ÁREAS DE TRABAJO	47
7.7	ESTACIONES DE TRABAJO Ó COMPUTADORES DESKTOP	48
7.8	SITIOS DE TRABAJO	49
7.9	CONTROL DE ACCESO A LA RED	50
7.9.1	Utilización de los servicios de red	50
7.9.2	Autenticación de usuarios para conexiones externas	50
7.9.3	Autenticación de nodos	51
7.9.4	Protección de los puertos de diagnóstico remoto	51
7.9.5	Subdivisión de redes	51
7.9.6	Control de conexión a la red	51
7.9.7	Control de ruteo de red	52
7.9.8	Seguridad de los servicios de red	52
7.9.9	Control de acceso al sistema operativo	52
7.9.10	Identificación automática de terminales	53
7.9.11	Identificación y autenticación de usuarios	53
7.9.12	Sistema de administración de contraseñas	53
7.9.13	Uso de utilitarios del sistema	54
7.9.14	Alarmas silenciosas para la protección de los usuarios	54
7.9.15	Desconexión de terminales por tiempo muerto	54
7.9.16	Limitación del horario de conexión	54
7.10	CONTROL DE ACCESO A LAS APLICACIONES	54
7.10.1	Restricción del acceso a la información	55
7.10.2	Aislamientos de sistemas sensibles	55
7.10.3	Monitoreo del acceso y uso de los sistemas	55
7.10.4	Sincronización de relojes	56
7.10.5	Registro de eventos	56
7.11	COMPUTACIÓN MÓVIL Y TRABAJO REMOTO	56
8.	DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN....	58
8.1	REQUERIMIENTOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN.....	58
8.1.1	Análisis y especificación de los requisitos de seguridad	58
8.2	SEGURIDAD EN LOS SISTEMAS DE APLICACIÓN	59
8.2.1	Validación de los datos de entrada	59
8.2.3	Autenticación de los mensajes	60
8.2.4	Validación de los datos de salida	60
8.3	SEGURIDAD DE LOS ARCHIVOS DEL SISTEMA	61
8.3.1	Control del software operativo	61
8.3.2	Protección de los datos de prueba del sistema	61
8.3.3	Control de acceso a las bibliotecas de programas fuente	62
8.4	SEGURIDAD EN LOS PROCESOS DE DESARROLLO Y SOPORTE	62
8.4.1	Procedimientos de control de cambios	62
8.4.2	Revisión técnica de las aplicaciones después de los cambios en el sistema operativo	63
8.4.4	Canales ocultos y código troyano	64
8.4.5	Desarrollo de software contratado externamente	64
9.	GESTIÓN DE LA CONTINUIDAD DE LOS SERVICIOS INFORMÁTICOS....	64
9.1	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN.....	64

9.1.1	Inclusión de la seguridad de la información en el proceso de gestión de la continuidad de los servicios informáticos	64
9.1.2	Continuidad de los servicios informáticos y evaluación de riesgos	65
9.1.3	Desarrollo e implementación de planes de continuidad que incluyan la seguridad de la información	66
9.1.4	Estructura para la planificación de la continuidad de los servicios Informáticos	66
9.1.5	Pruebas, mantenimiento y reevaluación de los planes de continuidad de los servicios informáticos	67
10.	REQUERIMIENTOS LEGALES.....	67
10.1	PRESUNCIÓN	67
10.2	EN CUANTO A LOS PERJUICIOS	67
10.3	RESPECTO A LA ENTREGA	67
10.4	RESPONSABILIDADES	68
10.5	EFFECTOS LEGALES DE LA INFORMACIÓN	68
10.6	AUTORIZACIONES	68

1. POLÍTICAS DE USO ACEPTABLE -PUA-

El uso aceptable de los activos informáticos de las Fuerzas Militares, implica la aceptación implícita por parte de los usuarios de estos, de las normas, políticas y estandares establecidos para garantizar la seguridad informática y el buen uso de los mismos, así como de los compromisos y responsabilidades adquiridas.

Los siguientes se consideran actos no autorizados o de obligatorio cumplimiento para el uso de los activos informáticos de las Fuerzas Militares y están expresamente prohibidos así:

1. El intento o violación de los controles de seguridad establecidos para la protección de los activos informáticos de las FF.MM.
2. Realizar cualquier actividad que pudiera comprometer la seguridad de cualquier activo informático de las FF.MM.
3. El uso sin autorización de los activos informáticos de las Fuerzas Militares.
4. El uso no autorizado o impropio de la conexión al sistema.
5. Intentar evadir ó violar la seguridad o autenticación de usuario de cualquier host, red o cuenta.
6. El uso indebido de las contraseñas, firmas digitales ó dispositivos de autenticación.
7. Esta prohibido a cualquier usuario acceder a servicios informáticos utilizando cuentas o medios de autenticación de otros usuarios. Aún con la autorización expresa del usuario propietario de la misma.
8. El almacenamiento, instalación, configuración, ó uso de software ilegal o no autorizado o de datos no autorizados en los activos informáticos de las FF.MM.
9. Está prohibido el uso, distribución y ejecución de software o código malicioso que cause daño, hostigamiento, molestias a personas, daño o alteración de información o traumatismos en la continuidad de los servicios informáticos ó vulnere la seguridad de los sistemas.
10. El hurto, robo, sustracción ó uso no autorizado de: datos, información, materiales, equipos y otros elementos pertenecientes a los activos informáticos de las Fuerzas Militares.
11. Está prohibido retirar de las instalaciones de las Fuerzas Militares ó áreas bajo su administración ó control, cualquier activo informático sin autorización previa.
12. El acceso, modificación o alteración no autorizada de componentes, datos o información de los activos informáticos de las FF.MM.

13. El uso de medios electrónicos, medios de almacenamiento, software, hardware, datos o información en medios digitales provenientes de fuentes no certificadas o de terceros, sin la previa revisión y autorización del Administrador del Sistema y/o Oficial de Seguridad Informática.
14. El Servicio de Internet puede ser utilizado solamente con fines autorizados y legales. Se prohíbe toda transmisión, difusión, distribución o almacenamiento de cualquier material –digital o impreso- en violación de cualquier ley o regulación aplicable. Esto incluye, sin limitación alguna, todo material protegido por los derechos de autor, marcas, secretos comerciales u otros derechos de propiedad intelectual usados sin la debida autorización, y todo material obsceno o pornográfico, difamatorio, o que constituya una amenaza ilegal.
15. En el uso del correo electrónico, está prohibido el SPAM, el TROLL, MAILBOMBING, reenvío o retransmisión de mensajes de carácter no oficial, o la suscripción a otro usuario a una lista de correo sin su permiso. –ver definiciones en el Anexo "B".
16. Realizar por internet, o a través de los activos informáticos, cualquier actividad cualquier que pudiera potencialmente traer des prestigio a las Fuerzas Militares de Colombia.
17. Los mensajes contenidos en los correos electrónicos no pueden ser contrarios a las disposiciones del Orden Público, la moral, las buenas costumbres nacionales e internacionales y los usos y costumbres aplicables en Internet, y el respeto de los derechos de tercera personas.
18. Está prohibido el almacenamiento y reproducción de aplicaciones, programas o archivos de audio ó video que no están relacionados con las actividades propias de las funciones que cumple la dependencia o el usuario.
19. El usuario está de acuerdo en aceptar responsabilidad por todas las actividades realizadas con los activos informáticos bajo su responsabilidad y custodia o desde las cuentas asignadas para su acceso a los servicios informáticos de las Fuerzas Militares.
20. Está prohibido el intento o el hecho de agregar, remover o modificar información identificadora o de contenido en la red, que engañe o confunda al sistema o al usuario destinatario ó suplante a otro usuario utilizando su información identificadora.
21. Las cuentas de red de las Fuerzas Militares operan con recursos compartidos. Está prohibido el uso abusivo de estos recursos por parte de un usuario en una forma tal que afecte negativamente el rendimiento de la misma.
22. Cualquier violación o sospecha de violación de las medidas o controles de seguridad de los sistemas de información, o de las políticas de seguridad Informática para las Fuerzas Militares, debe ser reportada inmediatamente por quien conozca de ellas, al Oficial de Seguridad Informática de su respectiva unidad, para los fines pertinentes. Las Fuerzas Militares cooperarán con investigaciones de violaciones a la seguridad de redes y sistemas, incluyendo la cooperación con las autoridades legales en la investigación de cualquier incidente informático., que de origen a procesos administrativos, disciplinarios, penales o civiles.

2. SEGURIDAD ORGANIZACIONAL

2.1 INFRAESTRUCTURA DE SEGURIDAD DE LA INFORMACIÓN

El Modelo de seguridad informática de las Fuerzas Militares está conformado por políticas, normas, estándares, procedimientos y mecanismos de seguridad y controles basados en siete (7) fundamentos que son la plataforma para la conformación del modelo. Estos fundamentos son: confidencialidad, integridad, disponibilidad, autenticación, autorización, no repudio y auditabilidad de la información.

Todos los mecanismos de seguridad informática que se implementen en los sistemas de información de las Fuerzas Militares deben relacionarse con el fundamento sobre el cual se aplican o soportan mediante una matriz con el fin de tener clara su aplicación para el diseño e implementación de controles de seguridad.

Ver figura 2.1 Ejemplo Matriz Mecanismos y relaciones de seguridad de la información, donde se muestran algunos mecanismos y sus relaciones

2.1.1 Foro de seguridad de la información

1. Los funcionarios pertenecientes al Comité de Seguridad Informática, al Grupo de Respuesta a Incidentes de Seguridad en Cómputo (CSIRT); así como los Oficiales del Sistema de Gestión de Seguridad de la Información (OSGSI) y los Oficiales de Seguridad Informática se deben contactar entre sí y pertenecer a foros o grupos de interés especial en seguridad informática y manejo de evidencia digital para:
 2. Mejorar el conocimiento sobre las mejores prácticas y estar actualizado con la información pertinente a la seguridad.
 3. Garantizar que la comprensión del entorno de seguridad de la información es actual y completa.
 4. Recibir advertencias oportunas de alertas, avisos y parches relacionados con ataques y vulnerabilidades.
 5. Obtener acceso a asesoría especializada sobre seguridad de la información.
 6. Compartir e intercambiar información acerca de nuevas tecnologías, productos, amenazas o vulnerabilidades.
 7. Suministrar puntos adecuados de enlace cuando se trata de incidentes de seguridad de la información.
 8. Se pueden establecer acuerdos para compartir información con el objeto de mejorar la cooperación y la coordinación de los temas de seguridad con organismos afines

externos. Dichos acuerdos deben identificar los requisitos para la protección de la información sensible o clasificada.

Tecnologías Fundamento -->	Autentificación	Integridad	Confidencialidad	No Repudiancia	Control de Acceso	Disponibilidad	Auditoría
Alta disponibilidad por hardware						X	
Alta disponibilidad por software						X	
Antivirus	X				X	X	X
Atención de Incidentes	X	X	X		X	X	X
Biométricos	X						
Encripción Asimétrica	X	X	X	X			
Encripción Simétrica	X	X					
Firewall	X				X		X
IDS		X			X	X	X
Password	X						
Perfiles de Acceso					X		X
PKI	X	X	X	X			X
Planes de Continuidad							X
Políticas de Seguridad	X	X	X	X	X	X	X
Pruebas de Vulnerabilidad							X
Redundancias de CPU							
Redundancia de Discos							X
SSL	X	X	X				
VPN	X	X	X				
Servidores					X	X	X

Figura 2.1 Ejemplo Matriz Mecanismos y relaciones de seguridad de la información

2.1.2 Coordinación de la seguridad de la información

La coordinación de la Seguridad Informática en las Fuerzas Militares, será ejecutada entre los siguientes grupos de trabajo: el Comité de Seguridad Informática, el Grupo de Respuesta a Incidentes de Seguridad en Cómputo (CSIRT), los Oficiales del Sistema de Gestión de Seguridad de la Información (OSGSI), los Oficiales de Seguridad Informática y usuarios de los sistemas de información y todas las unidades informáticas y dependencias que se relacionen de manera particular con esta área, tanto de orden interno como externo.

2.1.3 Responsabilidades en seguridad de la información

Los usuarios con responsabilidades de seguridad de la información deben determinar la ejecución correcta de las labores delegadas y tener en cuenta los siguientes aspectos:

1. Identificar y definir claramente los activos y los procesos de seguridad asociados con cada sistema en particular.
2. Asignar la unidad y/o funcionario responsable de cada activo o proceso de seguridad, así como documentar esta responsabilidad.

3. Definir y documentar claramente los niveles de autorización, a la Información

2.1.4 Proceso de autorización para los servicios de procesamiento de información

Se deben tener en cuenta los siguientes aspectos para el proceso de autorización:

1. Los servicios nuevos deben tener autorización por el Jefe de la Unidad para el acceso a la información. La autorización también se debe obtener del oficial de seguridad responsable de mantener el entorno de seguridad del sistema de información local, para asegurar el cumplimiento de todas las políticas y los requisitos de seguridad correspondientes.
2. El software y hardware, se debe verificar para asegurar que son compatibles con otros componentes del sistema.
3. La utilización de servicios de procesamiento de información en dispositivos electrónicos ó equipos personales o privados, como computadores portátiles, computadores domésticos o dispositivos manuales para procesar, almacenar, transmitir o recibir información de la Institución, no son autorizados debido a que pueden introducir vulnerabilidades a las redes de las Fuerzas Militares y facilitar la fuga de información.

2.1.5 Asesoramiento especializado en materia de seguridad de la información

De ser necesario, se debe contratar asesoría externa especializada en el área de Seguridad Informática para controlar y proteger los activos informáticos de la Institución. Así como para capacitar y entrenar y certificar al personal involucrado en el área de gestión de seguridad informática.

2.1.6 Cooperación entre organizaciones

1. Las Fuerzas Militares deben tener procedimientos establecidos que especifiquen cuándo y a través de qué autoridades se deben contactar y la forma en que se deben reportar oportunamente los incidentes identificados de la seguridad de la información, si se sospecha de incumplimiento de la ley.
2. El mantenimiento de dichos contactos debe ser un requisito para dar soporte a la gestión de incidentes de seguridad de la información o la continuidad de la Institución y el proceso de planes de contingencia.
3. Los contactos con otras autoridades incluyen servicios públicos, servicios de emergencia, salud y seguridad, como el departamento de bomberos (en conexión con la continuidad de la Institución), proveedores de telecomunicaciones con enrutamiento en línea, disponibilidad) y proveedores de agua con medios de refrigeración para los equipos.

2.1.7 Revisión independiente de la seguridad de la información

1. El Comité de Seguridad Informática debe poner en marcha la revisión independiente y la realización de pruebas de vulnerabilidad a la red de las Fuerzas Militares, con personal idóneo y capacitado en el área de seguridad Informática.
2. Esta revisión independiente es necesaria para asegurar la eficacia, idoneidad y propiedad del enfoque de la Institución para la gestión de la seguridad de la información. La revisión debe incluir la evaluación de las oportunidades de mejora y la necesidad de cambios en el enfoque de la seguridad, incluyendo la política y los objetivos de control.
3. Dicha revisión debe ser realizada por personas independientes del área sometida a revisión, por ejemplo la auditoría interna, el Oficial de Seguridad Informática de otra unidad i o una organización externa especializada en tales revisiones.
4. Los resultados de la revisión independiente se deben registrar y reportar a la Unidad que ha iniciado la revisión. Estos registros se deben conservar.
5. Si la revisión identifica que el enfoque y la implementación de la seguridad de la información son inadecuados o no cumplen la orientación para la seguridad de la información establecida en el documento de políticas de la seguridad de la información, se deben considerar las acciones correctivas.

2.2 SEGURIDAD FRENTES AL ACCESO POR PARTE DE TERCEROS

1. Se debe controlar todo acceso a los servicios de procesamiento de información, así como el procesamiento y comunicación de información por partes externas.
2. Cuando exista la necesidad de trabajar con partes externas y se requiera acceso a la información de la Institución, a sus servicios de procesamiento de información, o de obtener o suministrar productos y servicios de o para una parte externa, se debe realizar una evaluación de riesgos para determinar las implicaciones para la seguridad de la información de las Fuerzas Militares y los requisitos de control.

2.2.1 Identificación de riesgos del acceso de terceras partes

En la identificación de los riesgos relacionados con el acceso de partes externas se deben considerar los siguientes aspectos, los cuales deben quedar documentados así:

1. Los servicios de procesamiento de información a los cuales requiere acceso la parte externa.
2. El tipo de acceso que tendrá la parte externa a la información y a los servicios de procesamiento de información:
 - a. Acceso físico, a oficinas, recintos de computadores y gabinetes de archivos.

- b. Acceso lógico, a las bases de datos o a los sistemas de la Institución.
 - c. Conexión de red entre las redes de la Institución y de la parte externa por ejemplo conexión permanente a servicios públicos.
 - d. Si el acceso tendrá lugar en las instalaciones o fuera de ellas.
3. Valor y la sensibilidad de la información involucrada y su importancia para las operaciones de la Institución.
 4. Los controles necesarios para proteger la información que no está destinada a ser accesible por las partes externas;
 5. Control del personal de la parte externa involucrado en manejar la información de la Institución.
 6. La forma en que se puede identificar a la organización externa o al personal autorizado a tener acceso, la manera de verificar la autorización, así como la forma en que es necesario confirmarlo.
 7. Los diferentes medios y controles utilizados por la parte externa al almacenar, procesar, comunicar, compartir e intercambiar la información.
 8. El impacto del acceso negado a la parte externa cuando lo requiere y de la recepción o el acceso de la parte externa a información inexacta o engañoso.
 9. Las prácticas y los procedimientos para tratar los incidentes de seguridad de la información y los daños potenciales, al igual que los términos y las condiciones para la continuación del acceso de la parte externa en el caso de un incidente de seguridad de la información.
 10. Los requisitos legales y reglamentarios, las garantías y otras obligaciones contractuales pertinentes a la parte externa que se deben tener en cuenta.
 11. La forma en que se podrían ver afectados los intereses de cualquier otro ente externo, debido a los acuerdos.
 12. El documento de aceptación de conocimiento y cumplimiento de las políticas de seguridad informática para las Fuerzas Militares y los estudios de seguridad pertinentes tanto a la empresa como a los funcionarios o empleados de las terceras partes involucradas.
 13. El acceso de las partes externas a la información de la Institución, no se debe brindar hasta haber implementado los controles apropiados y cuando es viable, haber firmado un contrato que defina los términos y las condiciones para la conexión o el acceso y el acuerdo de trabajo.
 14. Se debe garantizar que la parte externa es consciente de sus obligaciones y acepta las responsabilidades y deberes involucrados en el acceso, procesamiento, comunicación

o gestión de la información y los servicios de procesamiento de información de la Institución.

15. Se deben utilizar las promesas de reserva y los acuerdos de no-divulgación a los siguientes agentes externos:

- a. Proveedores y empleados de servicios, de seguridad, Internet, de red, de servicios telefónicos, mantenimiento, de limpieza, alimentación y otros servicios de soporte contratados externamente.
- b. Contratistas externos de servicios y/u operaciones, de sistemas de tecnología de la información, servicios de recolección de datos, operaciones de centros de llamadas, asesores de negocios, gestión y auditores.
- c. Desarrolladores y proveedores de productos de software y sistemas de tecnología de la información y personal temporal, estudiantes y otras asignaciones casuales a corto plazo.

2.2.2 Requerimientos de seguridad en contratos con terceros

1. Los proveedores externos, contratistas, asesores, deben tener los Estudios de Seguridad y la promesa de reserva en la Dirección de Contra Inteligencia de la Unidad y de ser necesario por el tipo de información que se maneje, se podrá solicitar la Prueba de Poligrafía pertinente.
2. El acceso de terceros y/o empresas contratistas, no debe ser autorizado por ningún funcionario de las Fuerzas Militares hasta que no se haya realizado el estudio de seguridad correspondiente por las unidades de Contra Inteligencia.
3. Se debe mantener una bitácora con la descripción del servicio al que se va a acceder, lista de usuarios autorizados y de permisos de acceso a recursos o activos específicos, horas y fechas de disponibilidad del servicio.
4. Se deben realizar procedimientos de protección de los activos; medidas de protección física y contra la introducción y propagación de virus, código malicioso en los sistemas informáticos instalados.
5. Se deben establecer responsabilidades de cada parte: derecho de auditoria para complementar las responsabilidades contractuales, derecho de las Fuerzas Militares para controlar (y suspender en su caso) la actividad de uno o varios usuarios; acuerdo para la investigación e informes de incidentes de seguridad informática.
6. Se deben tener en cuenta responsabilidades derivadas de las leyes nacionales o locales y deben haber restricciones contra la copia y la revelación no autorizada de información Institucional.
7. Se debe tener en cuenta las responsabilidades en el mantenimiento del hardware y del software.

8. Se debe tener en cuenta medidas para asegurar la devolución de documentación y activos de información al finalizar el contrato.
9. Se deben tener en cuenta los siguientes términos para la inclusión en el acuerdo con el objeto de cumplir los requisitos de seguridad identificados así:
 - a. La política de seguridad de la información.
 - b. Procedimientos para proteger los activos de la institución, incluyendo información, software y hardware.
 - c. Todos los controles y mecanismos de protección física requeridos.
 - d. Controles para asegurar la protección contra software malicioso.
 - e. Procedimientos para determinar si alguna vez se han puesto en peligro los activos, por ejemplo pérdida o modificación de información; software y hardware.
 - f. Controles para asegurar la devolución o la destrucción de la información y los activos al finalizar el acuerdo o en un punto acordado en el tiempo durante la duración del acuerdo.
 - g. Confidencialidad, integridad, disponibilidad y cualquier otra propiedad pertinente.
 - h. Restricciones a la copia y a la divulgación de información, y uso de acuerdos de confidencialidad.
 - i. La transferencia de tecnología en la formación del usuario y del administrador en métodos, procedimientos y seguridad.
 - j. Asegurar la concientización del usuario sobre responsabilidades y aspectos de la seguridad de la información.
 - k. Las disposiciones para la transferencia de personal, cuando es apropiado.
 - l. Las responsabilidades relacionadas con la instalación y el mantenimiento del software y el hardware.
 - m. La estructura clara y los formatos acordados para la presentación de los informes.
 - n. El proceso claro y específico para la gestión de cambios.
 - o. La política de control del acceso, incluyendo:
 - 1) Requisitos y beneficios de la necesidad del acceso por terceras partes.
 - 2) Métodos de acceso permitido y control y uso de identificadores únicos, tales como las identificaciones de usuario (ID) y las contraseñas.

- 3) Proceso de autorización para los privilegios y el acceso del usuario, con fechas de expiración claras acordes con las fases de participación del usuario en el proyecto.
 - 4) Requisito para mantener una lista de las personas autorizadas a usar los servicios que se ponen a disposición, de sus derechos y privilegios con relación al uso.
 - 5) Declaración de que el acceso que no se autorice explícitamente está prohibido.
 - 6) Proceso para revocar los derechos de acceso o interrumpir la conexión entre los sistemas, en cualquier momento del contrato o convenio y al terminar las funciones o participación de cada uno de los usuarios.
- p. Las disposiciones para el reporte, la notificación y la investigación de los incidentes de seguridad de la información y las violaciones de la seguridad, así como los incumplimientos de los requisitos establecidos en el acuerdo.
- q. La descripción de cada servicio que va a estar disponible y una descripción de la información que ya a estar disponible junto con su clasificación de seguridad.
- r. La meta del nivel de servicio y los niveles inaceptables de servicio.
- s. La definición de criterios verificables de desempeño, su monitoreo y reporte.
- t. El derecho a monitorear y revocar cualquier actividad relacionada con los activos de la Institución. Así como el de auditar las responsabilidades definidas en el acuerdo y a que dichas auditorías sean realizadas por una tercera parte.
- u. El establecimiento de un proceso escalable para la solución de problemas.
- v. Las responsabilidades civiles correspondientes de las partes del acuerdo.
- w. Las responsabilidades relacionadas con asuntos legales y la forma en que se garantiza el cumplimiento de los requisitos legales, por ejemplo la legislación sobre protección de datos, teniendo en cuenta particularmente los diversos sistemas legales nacionales, si el acuerdo implica cooperación con organizaciones en otros países.
- x. Los derechos de propiedad intelectual (DPI) y asignación de derechos de copia y la protección de cualquier trabajo en colaboración.
- y. La participación de las terceras partes con los subcontratistas y los controles de seguridad que estos subcontratistas necesitan implementar.
- z. Las condiciones para la renegociación / terminación del acuerdo:
 - 1) Se debe establecer un plan de contingencia en caso de que cualquiera de las partes desee terminar la relación antes del término de los acuerdos.

- 2) Renegociación de acuerdos si cambian los requisitos de seguridad de la Institución.
- 3) Documentación vigente de las listas de activos, licencias, acuerdos o derechos relacionados con ellos.

3. CLASIFICACIÓN Y CONTROL DE ACTIVOS

Cada usuario debe firmar un acta de responsabilidad y custodia sobre los activos informáticos que le sean asignados y el compromiso de cumplimiento de las políticas de seguridad informática sobre los mismos.

3.1 RESPONSABILIDAD POR RENDICIONES DE CUENTAS DE LOS ACTIVOS

Se deben identificar todos los usuarios de todos los activos y se debe asignar la responsabilidad por el mantenimiento de los controles adecuados.

3.1.1 Inventario de activos

1. Todo el hardware y software, será recepcionado por el almacenista de cada Unidad. El Oficial de Seguridad Informática en coordinación con el Administrador del Sistema de cada unidad se asegurarán de que el hardware, software y los sistemas de información sean clasificados y registrados en un sistema centralizado de activos informáticos.
2. Los inventarios de hardware, software e información deben ser revisados por lo menos una vez al año y las novedades deberán ser reportadas aparte de los organismos propios de la administración al sistema centralizado de activos informáticos.
3. Todo el hardware, software, sistemas de información debe tener un expediente separado del mantenimiento. Se hará y archivará un registro de mantenimiento cada vez que se haga éste en un componente de hardware, software, sistema de información de la red de las Fuerzas Militares para reflejar el mantenimiento realizado, la identidad de la persona que efectuó el mantenimiento y la persona que lo acompañó. Todos los expedientes del mantenimiento serán revisados por el representante técnico y el oficial de seguridad de cada unidad y serán conservados por lo menos doce meses estando disponibles para la revisión y la inspección del Administrador del Sistema.
4. La información mínima que se debe consignar en el sistema centralizado para control de activos informáticos de cada uno de los componentes de hardware, software, sistemas de información es la siguiente:

Hardware:	
Chasis	Nombre del Fabricante, Número Serie, Tipo de chasis
Discos Duros:	Fabricante, No. Serie de los discos duros, Modelo, Capacidad de almacenamiento
Memoria RAM:	Nombre del Fabricante, Numero de Serie, Capacidad en MB de la

	memoria
Procesador:	Fabricante procesador, Número de serie, Velocidad de procesamiento, Modelo del procesador
Tarjeta de red	Fabricante, Modelo tarjeta, MAC ((Media Access Control address))
Elementos periféricos	Nombre del elemento, Fabricante, Número de serie del elemento, Modelo del elemento
Software	Nombre software, Versión, Número de licencia, Proveedor, fecha de compra y tiempo de soporte y actualización.
Sistemas de Información	Nombre del sistema, Grado de clasificación del sistema de Información, Nombre del proveedor, Fecha de puesta en funcionamiento, Para qué fue diseñado, Unidad de destino, Registro manual técnico, Registro manual del usuario, Usuarios del sistema, Nombre del software de desarrollo del sistema, Ambiente de trabajo (Sistema Operativo), Arquitectura, Tiempo de Garantía
Información del funcionario responsable custodio.	Grado, Nombre del usuario responsable, número de cédula, fecha de recibo, número de teléfono oficina, número de teléfono personal, dirección de residencia, cargo, dependencia, número de cédula

3.2 CLASIFICACIÓN DE LA INFORMACIÓN

1. La información se debe clasificar en los grados de ULTRASECRETO, SECRETO, RESERVADO, CONFIDENCIAL, RESTRINGIDO, acuerdo con lo establecido en el Manual de Contrainteligencia FF.MM. 2-6 Segunda Edición, Segunda Parte “Seguridad Militar”, Capítulo 1, Sección C “Seguridad de la Información”.
2. EXCLUSIVO DE COMANDO, no corresponde a ningún grado de clasificación de seguridad. Se emplea cuando se requiere que la información contenida en el documento así marcado sea conocida directamente por el Comandante. Dicha información puede ser clasificada o no y su divulgación queda a su discreción.

3.2.1 Pautas para clasificación y manejo de la información

Cualquier información o documento que sea elaborado por las Fuerzas Militares y no se encuentre en los grados de clasificación ultrasecreto, secreto, reservado, confidencial, restringido y exclusivo de comando, se considera de conocimiento público y su tratamiento será bajo las normas establecidas para el manejo de documentos y las leyes vigentes. -Leyes de Derecho de Autor Colombia, Ley 23 de 1982. LEY 594 DE 2000 Responsabilidad: Los servidores públicos son responsables de la organización, conservación, uso y manejo de los documentos. Código Penal Colombiano: Artículo 418. “El servidor público que indebidamente dé a conocer documento o noticia que deba mantener en secreto o reserva, incurrirá en multa y pérdida del cargo. Si de la conducta resultare perjudicada la institución, la pena será de diez (10) a quince (15) años de prisión, multa de quince (15) a ciento cincuenta (150) salarios mínimos legales mensuales vigentes e inhabilitación para el ejercicio de derechos y funciones públicas por cinco (5) años.”. Decreto No. 1797 de 2000, Capítulo III De las Faltas, artículo 56 Faltas Gravísimas. Ley 522 de 1999, Código Penal Militar : Capítulo III, De la Revelación de Secretos. Ley 734 de 202 Deberes de los funcionarios públicos.

3.2.2 Rotulado y manejo de información

1. Todos los equipos de la red de las Fuerzas Militares, deben ser objeto de un control sobre su configuración para administrar su contabilidad e inventario. A cada parte de equipo le será asignado un número de inventario que se ate al número de serie, MAC (Media Access Control address) y modelo del equipo o parte. Las etiquetas se colocarán estratégicamente en sitio visible de cada parte conteniendo el número de inventario y su identificación, así como el propietario del recurso.
2. Para el plan de evacuación se deben marcar de manera especial los activos informáticos que contengan información de inteligencia, operaciones, proyectos y planes especiales de las Fuerzas Militares, ó información sensible o clasificada.
3. El Oficial de Seguridad Informática de las Unidades es el responsable de establecer y determinar qué equipos de comunicaciones, servidores y equipos de cómputo deben ser evacuados en orden de prioridades en caso de evacuación. Así mismo, los equipos que por su arquitectura, información, tecnología, capacidades o importancia, pudieran comprometer la Seguridad y Defensa Nacional, si cayeran en posesión del enemigo o terceros con el fin de priorizar y determinar el proceso de destrucción de los mismos en caso de abandono de la unidad. Esto debe ser realizado mediante una etiqueta especial fijada en una parte visible.

3.2.3 Control de hardware

Para mantener la integridad del sistema y del hardware , se deben aplicar controles físicos para el acceso al sitio de trabajo y al área de la red de las Fuerzas Militares; así mismo se deben usar contenedores de seguridad para almacenar los medios de almacenamiento y discos duros removibles de las estaciones de trabajo, cuando el sitio o el área de la red están desatendidos. (Excepto los servidores, que necesitan estar en línea para la replicación de datos). Todo el hardware de la red debe estar etiquetado.

3.2.4 Control de software

Las redes informáticas de las unidades de las Fuerzas Militares, deben ser supervisadas de manera permanente – en línea y a través de los logs de auditoría- por el respectivo administrador, para detectar incidentes informáticos, ó eventos ó actividad que pueda indicar cambios en el funcionamiento normal del sistema. De estas revistas se debe realizar el registro cronológico.

Todos los incidentes informáticos deben ser investigados y reportados. Sobre la investigación, se elaborará un informe escrito detallado que identifique el incidente, los resultados y acciones tomadas o recomendadas, el cual debe ser enviado al OSGSI.

3.2.5 Control de medios de almacenamiento

Cualquier medio para almacenamiento de datos, de tipo fijo ó extraíble que contenga información sensible y/o clasificada, debe ser controlado y protegido de manera especial, según el nivel de sensibilidad y clasificación de la información que contiene, observando las

normas para el manejo de información. Estos procedimientos deberán ser documentados de manera especial por el administrador y el Oficial de Seguridad Informática.

3.3 MATRIZ DE RIESGOS

1. El Oficial de Seguridad Informática de la unidad, verificará de manera permanente que todos los procedimientos estén relacionados en el mapa de riesgos, el cual debe tener entre otros, los siguientes aspectos para cada procedimiento que realicen los usuarios, en el desarrollo de sus funciones: Nombre de la Jefatura o Dirección, Procedimiento, Objetivo, Causas, Efectos, Riesgo, Impacto, Probabilidad de que ocurra el riesgo, Evaluación del riesgo, Control existente, Valoración del riesgo, Opciones de manejo, Acciones, Responsabilidades, Cronograma, Indicadores.
2. Mediante los análisis de riesgos se deben identificar y analizar los riesgos latentes en los sistemas y procedimientos y los respectivos impactos sobre éstos; es importante realizar este tipo de análisis para ser proactivo en la aplicación de controles, y no esperar que ocurra un incidente para controlarlos. Sobre las amenazas y el mapa de riesgos el Oficial de Seguridad Informática, hará un análisis y determinará los procedimientos necesarios para la recuperación en caso de materializarse el riesgo, con el objeto de orientar la contención y recuperación en caso de desastre.

4. SEGURIDAD DE LOS RECURSOS HUMANOS

4.1 ANTES DE LA RELACIÓN LABORAL

1. Las dependencias encargadas de la incorporación de personal o de contratar bienes ó servicios o de establecer acuerdos o convenios con terceras partes, ó por asignación de nuevos cargos con responsabilidades sobre información y activos informáticos, deberán poner especial atención en la etapa pre-laboral, para que los aspirantes cumplan con los requisitos de idoneidad y requisitos de seguridad mínimos establecidos en las políticas de seguridad informática con el fin de reducir el riesgo de robo, fraude o uso inadecuado de los activos informáticos y las instalaciones.
2. Se deben definir claramente las funciones o términos en los cuales se va a laborar de acuerdo con las políticas de seguridad de la información de la Fuerzas Militares de Colombia.
3. Se deben proteger en las áreas –físicas y lógicas- todos los activos contra acceso, divulgación, modificación, destrucción o interferencia no autorizados. Tanto los asignados para su cumplimiento, como los que se encuentren en el área de su alcance.
4. Se deben ejecutar procesos o actividades particulares de seguridad, para verificar la documentación de referencia presentada por el aspirante, como consultar fuentes externas para corroborar la exactitud y certeza de la misma. Los casos para cargos, funciones o actividades de manejo de información sensible o clasificada, deberán tener estudios especiales de seguridad personal y pruebas poligráficas.

5. Todos los empleados, contratistas y usuarios de terceras partes que tengan acceso a información sensible deberán firmar un acuerdo de confidencialidad o no-divulgación antes de tener acceso a los servicios de procesamiento de información, así mismo, dentro de los términos de su contrato, convenio ó condiciones laborales deberá quedar el compromiso de aceptación y cumplimiento de las políticas de seguridad informática para las Fuerzas Militares.
6. Se deberá informar al funcionario, el contratista o usuario de tercera parte sobre las acciones de carácter legal, administrativo, penal, disciplinario ó civil, a que puede estar sujeto si viola u omite el cumplimiento de las normas de seguridad establecidas en la institución.

4.2 DURANTE LA RELACIÓN LABORAL

4.2.1 Responsabilidades del jefe de la unidad respectiva

1. Informar al funcionario, contratista o usuario de tercera parte, sobre las funciones y las responsabilidades respecto a la seguridad de la información antes de que se les otorgue acceso a la información o a los sistemas de información sensibles ó clasificados
2. Cumplir las políticas de seguridad Informática para las Fuerzas Militares.
3. Desarrollar los procesos de concientizar y sensibilizar al personal, sobre la seguridad informática, sus funciones y responsabilidades dentro de la Institución.
4. Verificar permanentemente el cumplimiento de las políticas de seguridad por parte de todo el personal y ordenar los estudios de seguridad que considere pertinentes; así como la actualización de la matriz de riesgos.

4.3 AL TÉRMINO DE LA RELACIÓN LABORAL

4.3.1 Devolución de activos

1. Se deberá formalizar el proceso de terminación de la relación laboral, para incluir la devolución del software previamente desarrollado dentro de la Institución, los documentos corporativos y los activos informáticos asignados.
2. Las Direcciones de Personal, o la dependencia encargada del control del personal que termina su relación laboral, contrato o convenio, ó que es reasignada a una nueva función ó cargo, deberá informar de manera inmediata la novedad presentada al Administrador del Sistema de información y al Oficial de Seguridad Informática con el fin de que tomen las acciones inmediatas para cancelar ó revocar los permisos ó autorizaciones de acceso y la devolución y restitución de activos informáticos.
3. Los derechos de acceso que se deben adaptar o retirar incluyen acceso físico y lógico, claves, tarjetas de identificación, servicios de procesamiento de información,

suscripciones y retiro de cualquier documentación que lo identifique como miembro actual de la organización.

4. Cuando un funcionario, contratista o usuario de terceras partes con autorización especial con términos de uso definidos, usa uno o más equipos de la organización o utiliza su propio equipo, se debe aplicar un procedimiento especial de seguridad, durante el tiempo de su uso y al término, garantizar que toda la información pertinente se transfiera a las Fuerzas Militares y se elimina con seguridad de tales activos informáticos.
5. Cuando un funcionario, contratista o usuario de terceras partes tiene un conocimiento especial que es importante para la continuación de las operaciones informáticas, esa información ó conocimiento, debe estar documentada y transferirse a la organización.

5. SEGURIDAD FÍSICA Y DE ENTORNO

5.1 ÁREAS SEGURAS O RESTRINGIDAS

1. La implementación de medidas de seguridad física y de entorno, tiene como fin evitar el acceso físico no autorizado, el daño o la interferencia a las instalaciones y a la información de la organización.
2. Los servicios de procesamiento de información sensible o crítica deberán estar ubicados en áreas seguras o restringidas, protegidas por perímetros de seguridad definidos, con barreras de seguridad y controles de entrada adecuados. Dichas áreas deberán estar protegidas físicamente contra acceso no autorizado, daño e interferencia. La protección suministrada deberá estar acorde con los riesgos identificados.

5.1.1 Perímetro de seguridad física

1. Se deberán utilizar perímetros de seguridad (barreras tales como paredes, puertas de acceso controladas con tarjetas ó dispositivos electrónicos o mostradores de recepción atendidos) para proteger las áreas que contienen información y servicios de procesamiento de información.
2. Se deberán considerar e implementar los siguientes aspectos para los perímetros de seguridad física:
 - a. Se deben definir claramente los perímetros de seguridad y la ubicación y la fortaleza de cada perímetro deberá depender de los requisitos de seguridad, de los activos que protegen.
 - b. Los perímetros de una edificación o un lugar que contenga servicios de procesamiento de información deben ser sólidos (es decir, no deberían existir brechas en el perímetro o las áreas en donde se podría producir fácilmente una

- violación de la seguridad); las paredes externas del sitio deberían tener una construcción sólida y todas las puertas externas deberán tener protección adecuada contra el acceso no autorizado con mecanismos de control tales como barras, alarmas, relojes, etc., las puertas y ventanas deberían estar cerradas con llave cuando no están atendidas y se debe tener presente la protección externa para las ventanas, particularmente a nivel del suelo.
- c. Se debe establecer un área de recepción atendida u otros medios para controlar el acceso físico al lugar o edificación, el acceso a los sitios y edificaciones deberá estar restringido únicamente al personal autorizado y cuando sea viable, se deben construir barreras físicas para evitar el acceso físico no autorizado.
 - d. Si existen puertas contra incendio en el perímetro de seguridad, estas deben tener alarma, monitorearse y someterse a prueba junto con las paredes para establecer el grado requerido de resistencia, según las normas regionales, nacionales e internacionales; éstas deben funcionar de manera segura de acuerdo con el código local de incendios.
 - e. Se deben instalar sistemas adecuados de detección de intrusos según normas nacionales, regionales o internacionales y someterlos a pruebas regularmente para cubrir todas las puertas externas y ventanas accesibles; las áreas desocupadas siempre deberán tener alarmas; también se debe tener cubrimiento de otras áreas, tales como los centros de cómputo y de comunicaciones.
 - f. Las áreas de procesamiento de información clasificada o crítica de la organización deben estar físicamente separadas de aquellas dirigidas por terceras partes o personal externo.

5.1.2 Controles de acceso físico

- 1. Las áreas críticas donde se administra información clasificada o crítica, deben estar protegidas con controles de acceso apropiados para asegurar que sólo se permite el acceso a personal autorizado.
- 2. Se debe establecer un control especial para el personal visitante y se debe llevar un registro manual o digital que contenga: la fecha, la hora de entrada y salida de visitantes, sitio a visitar, motivo de la visita, persona que lo atiende y escolta, así como el nombre del funcionario que autoriza la visita. Todos los visitantes deberán estar supervisados y sólo se deben autorizar los accesos para propósitos específicos los cuales deben ser emitidos con instrucciones sobre los requisitos de seguridad del área y sobre los procedimientos de emergencia. De ser viable, se deberán incorporar dispositivos de cámaras, video ó dispositivos biométricos.
- 3. Se debe exigir a todos los funcionarios, contratistas y usuarios de terceras partes la utilización de alguna forma de identificación visible y se debe notificar inmediatamente al personal de seguridad si se encuentran visitantes sin acompañante y cualquiera que no use identificación visible.
- 4. El acceso del personal de servicio de soporte ó mantenimiento de terceras partes debe ser autorizado únicamente cuando sea necesario. Este acceso debe ser limitado para

las áreas seguras ó restringidas o a los servicios de procesamiento de información sensible y escoltado por un funcionario de la dependencia durante el tiempo de su permanencia. Se debe monitorear y registrar la actividad desarrollada.

5. Las autorizaciones de acceso a áreas seguras o restringidas se deben revisar y actualizar con regularidad y revocar cuando sea necesario.

51.3 Seguridad de oficinas, recintos y servicios

Se deben tener en cuenta los siguientes aspectos para la seguridad de oficinas, recintos y servicios:

1. Aplicar los reglamentos y las normas pertinentes a la seguridad industrial y física de las instalaciones.
2. Los servicios claves ó sensibles se deben ubicar estratégicamente, de modo que se evite el acceso al público.
3. Las edificaciones deben ser discretas y no tener indicaciones sobre su propósito. No deben tener señales obvias, fuera o dentro de ellas, que identifiquen a personas ajenas o visitantes, la presencia de actividades de procesamiento de información.
4. Los directorios y los listados telefónicos internos que indican las ubicaciones y los servicios de procesamiento de información sensible no deben estar disponibles al público.

5.1.4 Protección contra amenazas externas y ambientales

1. Se deben tomar en consideración todas las amenazas de orden natural, humano, y tecnológico, de carácter fortuito o intencional, que afecten las instalaciones propias o circundantes, para diseñar y establecer los controles necesarios que garanticen la seguridad de las instalaciones propias.
2. Los materiales combustibles o peligrosos así como los suministros a granel tales como los materiales de oficina, deberán recibir un tratamiento especial para su almacenamiento, el cual debe ser en un área acondicionada que no afecte el área segura por explosión o conato de incendio.
3. Las instalaciones con activos informáticos, deben estar dotadas de equipos o sistemas apropiados contra incendios y tener diseños especiales para este fin.

5.1.5 Trabajo en áreas seguras o restringidas

Se deben tener en cuenta los siguientes aspectos de seguridad para trabajar en áreas seguras o restringidas.

1. El personal sólo debe conocer las actividades que se desarrollan dentro de un área segura o restringida solo función de su cargo o función asignada.

2. El trabajo en áreas seguras o restringidas debe ser supervisado permanentemente para evitar las oportunidades de actividades maliciosas.
3. Las áreas seguras o restringidas vacías deberán tener bloqueo físico y se deben revisar periódicamente.
4. En las áreas seguras o restringidas no se debe permitir el acceso con equipos de cómputo ó equipos electrónicos tales como videograbadoras, cámaras fotográficas, celulares, dispositivos de almacenamiento, equipos de transmisión o recepción de señales ú otros dispositivos que puedan vulnerar la seguridad del área y activos informáticos.

5.1.6 Áreas de carga, despacho y acceso público

1. Los puntos de acceso tales como las áreas de carga y despacho y otros puntos por donde pueda ingresar personal no autorizado a las instalaciones se deben controlar y aislar de los servicios de procesamiento de información para evitar el acceso no autorizado.
2. El área de despacho y carga se debe ubicar de tal forma que los suministros se puedan descargar sin que el personal de despacho tenga acceso a otras partes de la edificación.
3. Las puertas externas del área de despacho y entrega deben estar aseguradas mientras las puertas internas estén abiertas.
4. El material que llega se debe inspeccionar para determinar posibles amenazas antes de moverlo desde el área de despacho y carga hasta el punto de uso.
5. El material que llega se debe registrar de acuerdo con los procedimientos de gestión de activos a su entrada al lugar.
6. Los envíos entrantes y salientes se deben separar físicamente, cuando sea posible.

5.2 SEGURIDAD DE LOS EQUIPOS

1. Se debe prevenir la pérdida, daño, robo o puesta en riesgo de los activos y la interrupción de los servicios informáticos de las Fuerzas Militares, para garantizar la confidencialidad, integridad y disponibilidad de la información.
2. Los activos informáticos deben estar protegidos contra todo tipo de amenazas físicas y lógicas.
3. Se deben tener pólizas o seguros que garanticen la reposición de los activos informáticos para respaldar los planes de contingencia y la continuidad de los servicios informáticos.

4. Es posible que se requieran controles especiales o equipos redundantes para la protección contra amenazas físicas y para salvaguardar los servicios de soporte tales como energía eléctrica e infraestructura de cableado.

5.2.1 Ubicación y protección de los equipos

Los equipos deben estar ubicados y protegidos para reducir el riesgo de amenazas o peligros del entorno, y las oportunidades de acceso no autorizado.

1. Los equipos que manejan datos sensibles, se deben ubicar en ángulo de tal forma que se reduzca el riesgo de visualización de la información por personas no autorizadas durante su uso.
2. Los elementos que requieran protección especial deben estar aislados para reducir el nivel general de protección requerida.
3. Se deben adoptar controles para minimizar el riesgo de amenazas físicas potenciales, como robo, incendio, explosión, humo, agua (o falta en el suministro de agua), polvo, vibración, efectos químicos, interferencia con el suministro eléctrico, interferencia en las comunicaciones, radiación electromagnética y vandalismo.
4. Se deben mantener las condiciones adecuadas como temperatura, humedad, iluminación que garanticen el normal funcionamiento de los servicios de procesamiento de información.
5. Se debe considerar el cumplimiento de normas técnicas y estándares para la instalación de equipos que presten servicio en ambientes industriales.

5.2.2 Servicios de soporte

Todos los servicios de soporte, tales como electricidad, suministro de agua, alcantarillado, calefacción / ventilación y aire acondicionado deben ser adecuados para los sistemas a los que dan apoyo.

1. Los servicios de soporte se deben inspeccionar regularmente y someter a las pruebas apropiadas para garantizar su efectividad y reducir los riesgos de mal funcionamiento y falla.
2. Se debe proporcionar un suministro eléctrico acorde con las especificaciones del fabricante del equipo.
3. Se debe tener un suministro de energía sin interrupción (UPS) para dar soporte al cierre ordenado o al funcionamiento continuo de equipos que soportan operaciones críticas para las Fuerzas Militares.
4. Los planes de contingencia deben incluir la acción que se ha de tomar en caso de falla de la UPS. Se recomienda pensar en un generador de soporte, si se requiere la continuidad del procesamiento en caso de fallas energéticas prolongadas.

5. Se debe tener disponible el suministro adecuado de combustible para garantizar que el generador pueda funcionar por un periodo prolongado. El equipo de UPS y los generadores se deben revisar con regularidad para asegurarse de que tienen la capacidad adecuada y someterse a prueba según las recomendaciones del fabricante.

5.2.3 Seguridad del cableado

Se deben tener en cuenta los siguientes aspectos para la seguridad del cableado:

1. Las líneas de energía y de telecomunicaciones en los servicios de procesamiento de información deben estar enterradas, cuando sea posible, o tener protección alterna adecuada.
2. El cableado de la red debe estar protegido contra interceptación no autorizada o daño, utilizando conductos rutas a través de áreas públicas.
3. Los cables de energía deben estar separados de los cables de comunicaciones para evitar interferencia.
4. se debe utilizar rótulos de equipo y de cables claramente identificables para minimizar los errores en el manejo, tales como conexiones provisionales de cables erróneos en la red.
5. Se debe emplear una lista de las conexiones temporales documentadas para reducir la posibilidad de errores.
6. Para sistemas críticos o sensibles se deben tener controles adicionales incluyendo:
 - a. Instalación de conductos blindados y recintos o cajas bloqueadas en los puntos de inspección y terminación.
 - b. Uso de medios alternos de enrutamiento y/o transmisión que suministren seguridad adecuada.
 - c. Uso de cableado de fibra óptica.
 - d. Uso de pantallas electromagnéticas para proteger los cables.
 - e. Inicio de reconocimientos técnicos e inspecciones para detectar dispositivos no autorizados ajustados a los cables.
 - f. Acceso controlado a los paneles o racks y a recintos de cables.

5.2.4 Mantenimiento de los equipos

Se debe seguir las siguientes directrices para el mantenimiento de los equipos:

1. El mantenimiento de los equipos debe estar acorde con las especificaciones y los intervalos de servicio recomendados por el proveedor.

2. Sólo personal de mantenimiento autorizado debe realizar las reparaciones y el servicio de los equipos.
3. Se debe conservar registros de todas las fallas reales o sospechadas y de todo el mantenimiento preventivo y correctivo.
4. Se deben implementar controles apropiados cuando se programa el mantenimiento para el equipo, teniendo en cuenta si el mantenimiento lo realiza el personal dentro o fuera de la organización; cuando sea necesario, la información sensible se debe borrar de forma segura.
5. Se deben cumplir todos los requisitos impuestos por las pólizas de seguros.
6. Los discos duros dañados o para reparación no pueden salir de las instalaciones.

5.2.5 Seguridad de los equipos fuera de las instalaciones

Se deben tener en cuenta los siguientes aspectos para la protección del equipo por fuera de las instalaciones:

1. El equipo y los medios llevados fuera de las instalaciones no se deben dejar solos en sitios públicos, los computadores portátiles se deben llevar como equipaje de mano y camuflado, cuando sea posible, durante los viajes.
2. Se deben observar en todo momento las instrucciones del fabricante para la protección del equipo, por ejemplo, protección contra la exposición a campos electromagnéticos fuertes.
3. Se debe determinar controles para las áreas de trabajo mediante una evaluación de riesgos y controles adecuados que se aplican de forma idónea (gabinetes de archivos que se puedan bloquear, política de escritorio despejado, controles de acceso para computadores y comunicaciones seguras)
4. Se debe establecer el cubrimiento adecuado, para proteger el equipo fuera de las instalaciones. Los riesgos de seguridad, como daño, robo o escuchas no autorizadas pueden variar considerablemente entre los lugares y se debe tener en cuenta para determinar los controles más apropiados.

5.2.6 Seguridad en la reutilización o eliminación de los equipos

1. Se deben verificar todos los elementos del equipo que contengan medios de almacenamiento para asegurar que no se haya eliminado algún software con licencia ni datos sensibles o asegurar que se hayan sobrescrito con seguridad antes de la eliminación.
2. Los dispositivos que contienen información sensible se deben destruir físicamente o su información se debe destruir, borrar o sobrescribir usando técnicas que permitan que la información original no se pueda recuperar, en lugar de utilizar las funciones de borrado o formateado estándar.

3. Los dispositivos deteriorados que contengan datos sensibles se les debe hacer una evaluación de riesgos para determinar si los elementos se deben destruir físicamente en lugar de enviarlos a reparación o desecharlos.

5.2.7 Retiro de Propiedad

1. Ningún activo informático se debe retirar de las instalaciones de las Fuerzas Militares ó áreas bajo su administración ó control, sin autorización previa.
2. Los empleados, contratistas y usuarios de terceras partes que tengan autoridad para permitir retirar activos deben estar claramente identificados.
3. Se deben establecer límites de tiempo para el retiro de equipos y verificar el cumplimiento y registro en el momento de devolución.
4. Los controles al azar, se deben realizar para determinar el retiro no autorizado de propiedad, también se pueden usar para detectar dispositivos de grabación no autorizados, armas, etc., y evitar su ingreso. Tales controles al azar se deben llevar a cabo según los planes de Contrainteligencia de cada unidad.

6. COMUNICACIÓN Y ADMINISTRACIÓN DE OPERACIONES DE SISTEMAS INFORMÁTICOS

6.1 PROCEDIMIENTOS Y RESPONSABILIDADES OPERATIVAS

Se deben separar las áreas de desarrollo, y de prueba para evitar que se use el sistema de manera inadecuada, deliberada o negligente.

6.1.1 Documentación de los procedimientos operativos

Los procedimientos operativos deben especificar las instrucciones para la ejecución detallada de cada trabajo, teniendo en cuenta:

1. Procesamiento y manejo de información.
2. Copias de respaldo.
3. Requisitos de programación, incluyendo las interdependencias con otros sistemas, hora de comienzo del trabajo inicial y de terminación del trabajo final.
4. Instrucciones para el manejo de errores y otras condiciones excepcionales que se pueden presentar durante la ejecución del trabajo, restricciones al uso de las utilidades del sistema.
5. Contactos de soporte en caso de dificultades técnicas u operativas inesperadas.

6. Instrucciones de manejo de los medios y los resultados especiales, como el uso de papelería especial o el manejo de los resultados confidenciales incluyendo los procedimientos para la eliminación segura de los resultados de trabajos fallidos.
7. Procedimientos para el reinicio y la recuperación del sistema que se deben de usar en caso de falla del sistema.
8. Gestión de la prueba de auditoria y de la información de registro del sistema.
9. Los procedimientos operativos y documentados para las actividades con los activos informáticos de las Fuerzas Militares deben tratarse como documentos formales y sus cambios deben ser autorizados por los responsables de cada área de trabajo.

6.1.2 Control de cambios en las operaciones

Los sistemas operativos y el software de aplicación deben estar sujetos a un control sólido de la gestión del cambio, se deben considerar los siguientes elementos:

1. Identificación y registro de los cambios significativos.
2. Planificación y pruebas de los cambios.
3. Evaluación de los impactos potenciales de tales cambios, incluyendo los impactos en la seguridad.
4. Procedimiento de aprobación formal para los cambios propuestos.
5. Comunicación de los detalles del cambio a todos los usuarios involucrados.
6. Procedimientos de emergencia, incluyendo los procedimientos y las responsabilidades de cancelar o recuperarse de cambios fallidos y eventos imprevistos.
7. Los cambios en los sistemas operativos sólo se deben realizar cuando existe una razón válida para la Institución.

6.1.3 Procedimiento de manejo de incidentes informáticos

El incidente informático debe ser reportado al Oficial de Seguridad Informática de la unidad, quien lo evaluará e informará al grupo de respuesta a incidentes de seguridad de computo (CSIRT) de ser necesario.

6.1.4 Separación de funciones

1. Se deben separar las funciones y las áreas de responsabilidad para reducir las oportunidades de modificación no autorizada o no intencional, o el uso inadecuado de activos informáticos de las Fuerzas Militares.

2. Se deben establecer controles que permitan realizar auditorías, supervisión de las actividades por los técnicos responsables de la infraestructura de red de las Fuerzas Militares y sistemas de información.

6.1.5 Separación entre las instalaciones de desarrollo e instalaciones operativas

Se deben separar los ambientes operativos, de prueba y de desarrollo, para prevenir problemas operativos e implementar los controles adecuados, teniendo en cuenta los siguientes aspectos:

1. Definir y documentar las reglas para la transferencia de software del estado de desarrollo al operativo.
2. El software de desarrollo y el operativo se debe ejecutar en diferentes sistemas o procesadores de computación y en diferentes dominios o directorios.
3. Los compiladores, editores y otras herramientas de desarrollo o utilidades del sistema no deben ser accesibles por usuarios no autorizados.
4. El ambiente del sistema de prueba debe emular el ambiente del sistema operativo lo más estrechamente posible.
5. Los usuarios deben emplear perfiles de usuario diferentes para los sistemas operativos y de prueba y los menús deben desplegar mensajes de identificación adecuados para reducir el riesgo de error.
6. Los datos sensibles no deben ser copiados en el entorno del sistema de prueba.

Cuando el personal de desarrollo y de pruebas tiene acceso al sistema operativo y a la información, pueden introducir códigos no autorizados sin probar o alterar los datos operativos. En algunos sistemas, esta capacidad podría ser mal utilizada para cometer fraude o introducir códigos maliciosos o sin probar, lo cual puede crear problemas operativos graves.

6.2 PLANIFICACIÓN Y APROBACIÓN DEL SISTEMA

Los requisitos operativos de los sistemas nuevos de las Fuerzas Militares se deben identificar, documentar y probar antes de su aceptación y uso.

6.2.1 Planificación de la capacidad

1. Se debe hacer seguimiento y adaptación del uso de los recursos informáticos, así como proyecciones de los requisitos de capacidad futura para asegurar el desempeño requerido de los sistemas de las Fuerzas Militares.
2. Se debe poner atención a los recursos cuya adquisición toma mucho tiempo o requiere costos elevados; por lo tanto, los oficiales de seguridad informática de las unidades deben monitorear la utilización de los recursos claves de los sistemas.

3. Se deben identificar las tendencias del uso, particularmente en relación con las aplicaciones de la Institución o las herramientas del sistema de información para la gestión Institucional.

6.2.2 Aprobación del sistema

Los sistemas de información nuevos, las actualizaciones y las nuevas versiones únicamente se deben pasar a producción después de obtener la aceptación formal. Se deben considerar los siguientes elementos antes de la aceptación:

1. Requisitos de desempeño y capacidad de los computadores.
2. Procedimientos de recuperación por errores, reinicio y planes de contingencia.
3. Preparación y prueba de procedimientos operativos de rutina para las normas definidas.
4. Establecimiento de controles de seguridad.
5. Procedimientos y manuales eficaces.
6. Disposiciones para la continuidad operativa de la Institución.
7. Evidencia de que la instalación del sistema nuevo no afectará adversamente a los sistemas existentes, particularmente en los momentos pico de procesamiento, como el final de mes.
8. Evidencia de que se ha tenido en cuenta el efecto del sistema nuevo en toda la seguridad de la Institución.
9. Transferencia tecnológica en el funcionamiento o utilización de los sistemas nuevos.
10. Facilidad de uso, en la medida en que afecte el desempeño del usuario y evite el error humano.

6.3 PROTECCIÓN CONTRA SOFTWARE MALICIOSO

La protección contra códigos maliciosos, se debe basar en software de detección y reparación de daños por códigos maliciosos.

6.3.1 Controles contra software malicioso

1. Se deben realizar revisiones regulares del software y del contenido de datos de los sistemas que dan soporte a los procesos críticos de la Institución,
2. Se debe investigar la presencia de archivos no aprobados o parches no autorizados en el sistema.

3. Se debe verificar la presencia de códigos maliciosos en todos los archivos, medios ópticos o electrónicos y archivos recibidos en las redes antes de su uso.
4. Se debe verificar la presencia de códigos maliciosos en los adjuntos y las descargas del correo electrónico antes del uso; esta verificación se debe efectuar en diferentes lugares, como servidores de correo electrónico, los computadores de escritorio y cuando ingresan a la red de la Institución.
5. No se deben visitar, consultar y descargar archivos de páginas Web de dudosa procedencia.
6. Se deben definir responsabilidades y procedimientos de gestión para tratar la protección contra códigos maliciosos, la formación sobre su uso, el reporte y la recuperación debido a ataques de códigos maliciosos.
7. Se deben preparar planes adecuados para la continuidad operativa de la Institución con el fin de recuperarse de los ataques de códigos maliciosos, incluyendo todos los datos y el soporte de software necesario y las disposiciones para la recuperación.
8. El Oficial de Seguridad Informática de cada unidad debe implementar los procedimientos para recolectar información con regularidad, como la suscripción a sitios Web de verificación y / o listados de correo que suministren información sobre los códigos maliciosos nuevos.
9. Los antivirus se deben controlar en los servidores como en las estaciones de trabajo.

6.3.2 Control contra códigos móviles

Se deben tener en cuenta las siguientes consideraciones para la protección contra códigos móviles que ejecutan acciones no autorizadas:

1. Cuando se va a trabajar en un entorno con códigos móviles, se debe identificar el código móvil y la función o servicio que ejecuta en el software personalizado y ejecutarlo en un entorno con aislamiento lógico para verificar su funcionamiento correcto y su autenticidad con técnicas de hash.
2. Se debe bloquear el sistema para que no ejecute o use o reciba cualquier código móvil.
3. Se deben controlar los recursos disponibles para el acceso de los códigos móviles. Los controles criptográficos sirven para autenticar de forma única el código móvil.

6.4 MANTENIMIENTO

Se debe mantener la integridad y disponibilidad de la información y de los servicios de procesamiento de información, para lo cual se deben tener en cuenta tanto para el hardware como el software, los siguientes aspectos:

6.4.1 Respaldo de la información

Se deben considerar los siguientes elementos para el respaldo de la información:

1. Definir el nivel necesario para la información de respaldo.
2. Se deben hacer registros exactos y completos de las copias de respaldo y los procedimientos documentados de restauración.
3. La frecuencia de los respaldos deben reflejar los requisitos de seguridad de la información involucrada y la importancia de la operación continua de la Institución.
4. Los respaldos se deben almacenar en un sitio lejano apropiado con protección física, lógica y ambiental, a una distancia suficiente para escapar a cualquier daño debido a desastres en la unidad principal.
5. Los procedimientos de restauración tanto como los medios de respaldo, se deben verificar y probar con regularidad para garantizar su eficacia y que se pueden completar dentro del tiempo designado en los procedimientos operativos para la recuperación en caso de contingencia o desastre.
6. Se debe designar a una persona como operario de copias de respaldo de los servidores de red y Bases de Datos de las Fuerzas Militares. Esta persona será la encargada de realizar esta labor en las horas no hábiles de la Institución, con el fin de independizar este proceso de los administradores de los sistemas, quienes solo designaran a qué segmentos de sus máquinas se realizaran dichas copias. Este operador debe tener acceso de operador (solamente) a los sistemas operativos con el fin de realizar su labor.

6.4.2 Registro de actividades del personal operativo

Se debe establecer un perfil y registro de las personas que operan los sistemas y el operador de backups de los servidores, con el fin de determinar la confiabilidad de estas personas. Es importante que las personas que integren este grupo sean personas que estén amparadas bajo cláusulas de confidencialidad.

6.4.3 Registro de fallas

1. Se deben registrar las fallas reportadas por los usuarios o por los programas del sistema relacionadas con problemas de procesamiento de la información o con los sistemas de comunicación.
2. Se deben revisar los registros de fallas para garantizar que éstas se han resuelto satisfactoriamente.
3. Se deben registrar las medidas correctivas para garantizar que no se han puesto en peligro los controles y que la acción tomada está totalmente autorizada.

4. Se debe asegurar que el registro de errores está habilitado, si esta función del sistema está disponible.

6.5 ADMINISTRACIÓN DE LA RED

Las redes de las Fuerzas Militares se deben mantener y controlar adecuadamente para protegerlas de las amenazas y mantener la seguridad de los sistemas y aplicaciones que usan la red, incluyendo la información en tránsito.

6.5.1 Controles de redes

Los administradores de red y Oficiales de Seguridad Informática, deben implementar controles que garanticen la seguridad de la información en las redes y la protección de los servicios conectados contra el acceso no autorizado.

Se deben tener en cuenta los siguientes elementos:

1. La responsabilidad operativa por las redes debe estar separada de las operaciones del computador.
2. Es necesario establecer las responsabilidades y los procedimientos para la gestión de equipos remotos, incluyendo los equipos en áreas de usuarios.
3. Se deben establecer controles especiales para salvaguardar la confidencialidad y la integridad de los datos que pasan por redes públicas o redes inalámbricas y para proteger los sistemas y las aplicaciones conectadas, también se deben tener controles especiales para mantener la disponibilidad de los servicios de la red y los computadores conectados.
4. Se debe aplicar el registro y el monitoreo adecuado, para permitir el registro de acciones de seguridad pertinentes.
5. Se deben coordinar actividades de gestión para optimizar el servicio de la Institución y para garantizar que los controles se aplican consistentemente en toda la infraestructura del procesamiento de información de las Fuerzas Militares.

6.5.1.1 Switches

Se deben activar todas las opciones de seguridad del Switch y deshabilitar todos los servicios del Switch que no se van a usar tales como TFTP para un cliente remoto.

La configuración del Switch solo se debe realizar localmente, o en su defecto designar mediante listas de control de acceso (ACL) a un IP único remoto, asociado a la Mac de la estación remota.

6.5.1.2 Enlaces de redes

1. Se debe tener un control del personal que se comunica con redes externas (Internet, Intranet, Extranet), así como clasificar el tipo de información a intercambiar entre las entidades interconectadas.
2. Se deben documentar todas las comunicaciones con entidades externas a través de accesos commutados, dedicados o públicos, teniendo en cuenta los equipos activos, medio de comunicación, direcciones IP y diagramas de conexión.
3. Ni FTP Ni TELNET: deben ser usados para transferencia de datos y apertura de sesión remota. En su lugar se debe utilizar SFTP para transferir archivos, SSH con ciframiento para emulación de terminales, tanto al interior de las unidades como en la Intranet.

6.5.1.2.1 Implementación y encripción sobre los enlaces

1. La comunicación con entidades internas y externas a través de accesos dedicados, commutados o públicos deben ser encriptados.
2. Se debe implementar un sistema de detección de intrusos IDS dentro de la red, con el fin de detectar cualquier tipo de actividad contra los sistemas presentes.
3. Se debe mantener un sistema único de identificación de direcciones IP fijos para cada equipo. No es recomendable el uso de DHCP para validación de trazas y registros de auditoria.

6.5.1.3 Comunicación remota

1. Se deben restringir al máximo los recursos que se van a autorizar a los usuarios remotos, se debe contar con sistemas de autenticación fuertes para dichos accesos. En el caso que sea necesario compartir grandes volúmenes de datos a través de estas conexiones, se deben implementar redes privadas virtuales VPN, con el fin de garantizar la integridad de la comunicación y sistemas de detección de intrusos IDS para cada conexión. Se deben tener en cuenta reglas de autenticación para evitar posibles ataques.
2. Cuando se realicen comunicaciones remotas a través de antenas parabólicas para transmisión vía satélite, ó conexiones inalámbricas, éstas se deben instalar o ubicar en un sitio especialmente protegido, con base en las recomendaciones del fabricante, teniendo en cuenta las medidas de seguridad necesarias.

6.5.1.4 Firewall

1. En la instalación y configuración inicial de firewalls, se debe partir del principio que todos los servicios y puertos están negados y cerrados, a menos que expresamente sean habilitados y abiertos según el diseño preestablecido para la red.
2. Se deben configurar las reglas del Firewall, de acuerdo con los servicios que se necesiten, además se deben tener presentes los puntos vulnerables de toda la red, los servicios que se disponen como públicos al exterior de ella (WWW, FTP, TELNET,

entre otros) y conexiones por modem (dial-up modem calling) ó conexiones inalámbricas.

3. Este elemento debe mantener un control de las conexiones provenientes del interior y exterior de las Fuerzas Militares a las redes internas y viceversa. Garantizando la autenticación y autorización.

6.5.1.5 Monitoreo, sistemas de detección de intrusos (IDS) y de vulnerabilidades

1. La red debe ser monitoreada de manera permanente y se deben instalar sistemas de detección de intrusos en todos los puntos críticos de la red, para detectar posibles ataques o incidentes informáticos.
2. Se deben hacer análisis de vulnerabilidades a la red, documentar los resultados y tomar las acciones correctivas a que haya lugar.

6.5.1.6 Virtual Private Network (VPN)

Las comunicaciones que se establezcan entre usuarios externos y la red interna deben hacerse a través de un canal virtual privado que permita establecer una comunicación segura, garantizando los siguientes fundamentos de autenticación, confidencialidad e integridad.

6.5.1.7 Secure Socket Layer (SSL)

Cuando se ingrese a sitios que utilicen el protocolo SSL, el usuario debe verificar que el certificado sea valido, para acceder o enviar información con seguridad.

6.5.1.8 Seguridad a nivel de servidores

Los servidores deben cumplir con los servicios de auditoría, rehuso de objetos y debe existir un Administrador del Sistema con cuenta en cada uno de los servidores y será independiente del Oficial de Seguridad Informática.

6.5.1.8.1 Servidores de red

Se debe estudiar periódicamente la información contenida en los discos del servidor, a qué usuarios pertenece, prioridades, distribución de usuarios, grupos de usuarios, derechos de usuarios, políticas de cuentas, claves de acceso y auditar todos los procesos: (ingresos al sistema, intentos de accesos fallidos, fallas en entrada al sistema).

6.5.1.8.2 Servidores WEB

1. Los Servidores Web deben ser administrados por el grupo técnico correspondiente. La edición y contenido de la información de dicho servidor quedará bajo responsabilidad de la persona que procese y administre la información y contenido del mismo.
2. El servidor Web que permita el acceso a Bases de Datos desde la red pública (Internet) debe estar registrado y autenticado ante una unidad certificadora. Los Servicios Web deben basarse en SOAP, UDDI y WDSL

6.5.1.9 Listas de Control de Acceso (ACL)

Las listas de control de acceso deben estar configuradas en los equipos de comunicaciones asociadas en una tabla, de manera que los usuarios y/o redes en ella registrados, son los que el sistema autoriza o niega el acceso.

6.5.1.10 Encripción simétrica y asimétrica

1. Cuando se utilice criptografía simétrica, se debe asegurar que la metodología para el envío de la clave sea segura y que esta solo sea conocida por el emisor y el receptor.
2. Cuando se utilicen sistemas de encripción asimétricos, se debe cumplir con los siguientes aspectos:
 3. El par de llaves debe ser generado con algoritmos que usen criptografía de 156 bits o superior y el tamaño de las llaves sea de 3K o superior.
 4. Verificar que en el intercambio de llaves solo se envíe la llave pública.
 5. La copia de las llaves públicas y privadas deberá ser guardada en sitio seguro con llave ó la bóveda de seguridad de la unidad.
 6. Los procesos de encripción y desencripción se deben realizar siempre en equipos que no estén conectados a redes públicas o externas ó tengan servicios de acceso a Internet.
 7. Todos los textos en claro de documentos que se han encryptado o desencriptado, deben ser almacenados si se requiere, con las medidas de seguridad pertinentes a su grado de clasificación o sensibilidad. Para la eliminación de los mismos, se deberá usar siempre un método de borrado seguro.

6.6 ADMINISTRACIÓN Y SEGURIDAD DE LOS MEDIOS DE ALMACENAMIENTO

Se deben establecer procedimientos operativos adecuados para proteger documentos, medios de almacenamiento (por ejemplo cintas, discos), datos de entrada / salida y documentación del sistema contra divulgación, modificación, remoción y destrucción no autorizadas.

6.6.1 Administración de Medios Informáticos Removibles

Se deben tener en cuenta los siguientes aspectos:

1. Si ya no son necesarios, los contenidos de todos los medios reutilizables que se van a retirar de la Institución, se deben destruir de manera que sean irrecuperables.
2. Se debe exigir autorización para retirar los medios de la Institución y conservar un registro de tales retiros para mantener una prueba de auditoría.

3. Todos los medios se deben almacenar en un ambiente seguro y vigilado, según las especificaciones del fabricante, y tener un control sobre la vida útil del elemento.
4. Todos los dispositivos de almacenamiento removibles, deben ser rotulados y controlados mediante un registro especial de los mismos.
5. Las unidades de medios removibles sólo se deben habilitar si existen razones para hacerlo.

6.6.2 Eliminación de medios informáticos

Cuando ya no se requieren estos medios, su eliminación se debe hacer de forma segura y sin riesgo, utilizando los siguientes procedimientos formales:

1. Los medios que contienen información sensible se deben almacenar y eliminar de forma segura, mediante incineración o trituración, o borrar los datos de manera segura, para evitar el uso por parte de otra aplicación.
2. Se debe registrar la eliminación de los elementos sensibles con el objeto de mantener una prueba de auditoría.

6.6.3 Procedimientos del manejo de la información

Para manejar, procesar, almacenar y transmitir la información de acuerdo con su clasificación, se deben considerar los siguientes aspectos:

1. Manejo y etiquetado de todos los medios hasta su nivel indicado de clasificación.
2. Restricciones de acceso para evitar el acceso de personal no autorizado.
3. Mantenimiento de un registro formal de los receptores autorizados de los datos.
4. Garantizar que los datos estén completos, en el procesamiento y que se aplica la validación de la salida.
5. Protección, según el nivel de sensibilidad de los datos.
6. Almacenamiento de los medios según las especificaciones del fabricante.
7. Revisión de las listas de distribución y las listas de receptores autorizados a intervalos regulares.

6.6.4 Seguridad de la documentación del sistema

Para asegurar la documentación del sistema, se debe tener en cuenta los siguientes aspectos:

1. La documentación del sistema se debe almacenar con seguridad.

2. La lista de acceso a la documentación del sistema debe estar autorizada por el dueño de la aplicación.
3. La documentación del sistema que se suministra a través de una red pública, debe tener la protección adecuada.

6.7 INTERCAMBIOS DE INFORMACIÓN Y SOFTWARE

Para el intercambio de información se debe tener en cuenta su grado de clasificación y los procedimientos establecidos que garanticen la integridad, confidencialidad y disponibilidad.

Se deben realizar procedimientos claros y controles para la utilización de servicios de comunicación electrónica en el intercambio de información, teniendo en cuenta los siguientes aspectos:

1. Procedimientos para proteger la información a intercambiar contra interceptación, copiado, modificación, enrutamiento inadecuado y destrucción.
2. Procedimientos para detección y protección contra códigos maliciosos que se pueden transmitir con el uso de comunicaciones elestrónicas.
3. Procedimientos para proteger la información electrónica sensible, que está en forma de archivo adjunto.
4. Políticas o directrices que enfaticen el uso aceptable de los servicios de comunicación electrónica.
5. Procedimientos para el uso de comunicaciones inalámbricas, pensando en los riesgos particulares involucrados.
6. Establecer responsabilidades de funcionarios, contratistas y cualquier otro usuario que comprometan a la Institución, por ejemplo a través de difamación, acoso, suplantación de identidad, envío de cartas de cadena, adquisición no autorizada, etc.
7. Uso de técnicas criptográficas, para proteger la confidencialidad, la integridad y la autenticidad de la información.
8. No dejar información sensible o crítica en los dispositivos de impresión como copiadoras, impresoras y máquinas de facsímil.
9. Controles y restricciones con el envío de servicios de comunicación, como el envío automático de correo electrónico a direcciones de correo externas.
10. Evitar dar información que pueda ser utilizada por personas externas al área de trabajo ó a la institución con el fin de hacer ingeniería social.

6.7.1 Acuerdos de intercambios de información y software

En los acuerdos de intercambio de información y software se deben tomar en consideración las siguientes condiciones de seguridad:

1. Responsabilidades de los Jefes de las Unidades, Administradores de Sistemas, Oficiales de Seguridad Informática, Usuarios, para controlar y notificar la transmisión, el despacho y la recepción de la información Institucional.
2. Procedimientos para notificar a quien envía la transmisión, el despacho y la recepción.
3. Procedimientos para garantizar la trazabilidad y el no-repudio.
4. Normas técnicas para el empaquetado y la transmisión de datos.
5. Normas para identificar los servicios de mensajería.
6. Propiedad y responsabilidades para la protección de datos, derechos de copia, conformidad de las licencias de software y consideraciones similares.
7. Referenciar en los acuerdos de intercambio las políticas, procedimientos y normas para proteger la información y los medios físicos en tránsito.

6.7.2 Seguridad de los medios en tránsito

Se deben tener en cuenta los siguientes aspectos para la protección de los medios que se transportan entre los lugares:

1. Se debe utilizar transporte confiable o servicios de mensajería certificados, los cuales deberán garantizar la integridad y confidencialidad de los medios.
2. Se deben establecer los procedimientos necesarios para identificar y autenticar los servicios autorizados, así como verificar los procedimientos empleados por el transportador para garantizar la aplicación de las medidas o controles de seguridad.

6.7.3 Seguridad del correo electrónico

1. Para el caso del correo proveniente de INTERNET o de redes externas, los sistemas de Firewalls instalados en las redes de las Fuerzas Militares deben ser los encargados de recibir dicho correo y re-enviarlo al servidor de correo respectivo (store and forward), con el fin de prevenir los ataques comunes vía este medio.
2. Para el correo saliente, con información clasificada y/o sensible se debe utilizar un software de encripción autorizado. Así mismo, se deben emplear firmas digitales y sistemas de certificación de correo.

6.7.4 Sistemas de acceso público

1. La integridad de la información de las Fuerzas Militares, que se pone a disposición en sistemas públicos debe estar protegida con mecanismos apropiados como firmas digitales, para evitar la modificación y/o intrusión no autorizada.
2. Los sistemas de acceso público, se deben probar frente a debilidades y fallas antes de que la información esté disponible y debe existir un proceso de aprobación previo para que se publique la información Institucional. Así mismo, se deben analizar y corregir periódicamente las vulnerabilidades del sistema.

7. CONTROL DE ACCESO

7.1 REQUERIMIENTOS PARA EL CONTROL DE ACCESO

Esta sección describe cómo acceder a los sistemas informáticos de las Fuerzas Militares, teniendo en cuenta mecanismos de protección para la red, los datos, los periféricos y la información.

7.1.1 Políticas del control de acceso

Los controles de acceso son tanto lógicos como físicos y se deben considerar en conjunto teniendo en cuenta los siguientes aspectos:

1. Requisitos de seguridad de las aplicaciones individuales de la Institución e Identificación de toda la información relacionada con las aplicaciones y los riesgos a los que se enfrenta la información.
2. Políticas para la distribución y autorización de la información
3. Consistencia entre el control del acceso y las políticas de clasificación de la información de sistemas y redes diferentes.
4. Legislación pertinente y obligaciones contractuales relacionadas con la protección del acceso a los datos o los servicios.
5. Perfiles de acceso de usuario para funciones laborales comunes en la Institución.
6. Gestión de los derechos de acceso en un entorno distribuido y con red que reconozca todos los tipos de conexiones posibles.
7. Separación de las funciones de control del acceso. La solicitud de acceso, autorización del acceso y administración del acceso deben ser desarrolladas por personas diferentes.

8. Se deben establecer los requisitos para la autorización formal de las solicitudes de acceso, así como para la revisión periódica de los controles de acceso y el retiro de los derechos de acceso a los usuarios.
9. Establecer las reglas basadas en la premisa "En general, todo está prohibido, a menos que esté expresamente permitido" y no en la regla más débil de "En general, todo está permitido, a menos que esté expresamente prohibido".

7.2 ADMINISTRACIÓN DE ACCESO DE USUARIOS

1. Se deben establecer procedimientos formales para controlar la asignación de los derechos de acceso a los sistemas y servicios de información.
2. Los procedimientos deben comprender todas las fases del ciclo de vida del acceso del usuario, desde el registro inicial de los usuarios nuevos hasta la cancelación final del registro de usuarios que ya no requieren acceso a los servicios y sistemas de información. Se debe poner atención a la asignación de derechos de acceso privilegiado, que permiten a los usuarios anular los controles del sistema.

7.2.1 Registro de usuarios

El procedimiento de control del acceso para el registro y cancelación de registro de usuarios debe incluir:

1. Uso de la identificación única de usuario (ID) para permitir que los usuarios queden vinculados y sean responsables de sus acciones; el uso de identificadores (ID) de grupo únicamente se debe permitir cuando son necesarios por razones operativas de la Institución, y deben estar aprobadas y documentadas.
2. Verificación de que el usuario tenga autorización del dueño del sistema para el uso del sistema o servicio de información.
3. Verificación de que el nivel de acceso otorgado sea adecuado para los propósitos de la Institución y que sea consistente con la política de seguridad informática de la Institución, es decir, no pone en peligro la separación de funciones.
4. Dar a los usuarios una declaración escrita de sus derechos de acceso.
5. Exigir a los usuarios firmar declaraciones que indiquen que ellos entienden las condiciones del acceso.
6. Asegurar que los proveedores del servicio no otorguen el acceso hasta que se hayan terminado los procedimientos de autorización.
7. Mantener un registro formal de todas las personas autorizadas para usar el servicio.
8. Retirar o bloquear inmediatamente los derechos de acceso de los usuarios que han cambiado de función, de trabajo o que han dejado la Institución.

9. Verificar, retirar o bloquear periódicamente las identificaciones (ID) y cuentas redundantes de usuarios.
10. Garantizar que las identificaciones (ID) de usuario redundantes no se otorguen a otros usuarios.
11. Se debe considerar la inclusión de cláusulas en los contratos del personal y de los servicios, que especifiquen las sanciones si el personal o los proveedores del servicio intentan el acceso no autorizado.

7.2.2 Administración de privilegios

Los sistemas de usuario que requieren protección contra el acceso no autorizado deben controlar la asignación de privilegios a través de un proceso formal de autorización. Se deben tener en cuenta los siguientes elementos:

1. Los privilegios de acceso asociados con cada producto del sistema, como sistema operativo, sistema de gestión de bases de datos y de aplicación, deben identificar a los usuarios que tienen acceso privilegiado.
2. Los privilegios de administrador de cualquier equipo de cómputo (servidor, estación de trabajo, desktop, portátil, ó equipo activo de red), deben ser asignados exclusivamente al Administrador del Sistema en la Unidad Informática respectiva ó al funcionario designado oficialmente para su administración. En ningún caso se deben asignar autorizar estos privilegios de acceso al usuario del equipo.
3. Los privilegios se deben asignar a usuarios con base en la necesidad de utilizarlos y evento por evento, y de manera acorde con la política de control del acceso, es decir, el requisito mínimo para su función, sólo cuando sea necesario.
4. Se debe conservar un proceso de autorización y un registro de todos los privilegios asignados. Los privilegios no se deben otorgar hasta que el proceso de autorización esté completo.
5. Es conveniente promover el desarrollo y empleo de rutinas del sistema para evitar la necesidad de otorgar privilegios a los usuarios.
6. Se debe promover el desarrollo y empleo de programas que eviten la necesidad de funcionar con privilegios.
7. Los privilegios se deben asignar a un identificador de usuario (ID) diferente a los utilizados para el uso normal del sistema.
8. No se debe usar en el inicio de sesión de la red la contraseña de administrador, para evitar la intercepción de la contraseña en texto claro, que daría a un intruso acceso total al sistema.

7.2.3 Administración de contraseñas de usuario

La asignación de contraseñas se debe controlar a través de un proceso formal de gestión. El proceso debe incluir los siguientes requisitos:

1. Se debe exigir a los usuarios la firma de una declaración para mantener confidenciales las contraseñas personales, esta declaración firmada se puede incluir en los términos y condiciones laborales.
2. Cuando se exige a los usuarios mantener sus propias contraseñas, inicialmente se les debe suministrar una contraseña temporal segura que estén forzados a cambiar inmediatamente.
3. Se deben establecer procedimientos para verificar la identidad de un usuario antes de proporcionarle una contraseña temporal, de reemplazo o nueva.
4. Las contraseñas temporales se deben suministrar de forma segura a los usuarios; se deben evitar mensajes de correo electrónico de terceras partes o sin protección (texto claro).
5. Las contraseñas temporales deben ser únicas para un individuo y no descifrables.
6. Los usuarios deben acusar el recibo de las contraseñas.
7. Las contraseñas nunca se deben almacenar en sistemas de computador en un formato no protegido.
8. Las contraseñas predeterminadas por el vendedor se deben cambiar inmediatamente después de la instalación de los sistemas o del software.

7.2.4 Revisión de derechos de acceso a usuario

El Oficial de Seguridad Informática de cada Unidad, debe revisar los derechos de acceso de los usuarios empleando un proceso formal que considere en la revisión los siguientes aspectos:

1. Los derechos de acceso de los usuarios se deben revisar a intervalos regulares y modificar o reasignar estos derechos cuando se presenten cambios en el perfil de usuario, por promociones, ascensos, traslados, cambios de cargo o terminación de la relación laboral.
2. Se deben revisar las autorizaciones para derechos de acceso privilegiado a intervalos frecuentes para garantizar que no se tengan privilegios no autorizados o que no correspondan a las funciones del usuario.

7.3 RESPONSABILIDADES DEL USUARIO

1. El usuario debe proteger los recursos asignados por las Fuerzas Militares, guardar el secreto de su contraseña, no prestar su clave de usuario bajo ninguna circunstancia.

2. El usuario debe hacer copias de seguridad de sus archivos importantes, borrar periódicamente sus correos y archivos no utilizados.
3. El usuario debe cambiar su contraseña periódicamente, de acuerdo con las políticas establecidas por el Administrador del Sistema.
4. El usuario debe notificar o informar al Oficial de Seguridad Informática, cualquier novedad o incidente informático, que observe en el funcionamiento de su cuenta o en la aplicación de las políticas de seguridad informática en los sistemas de información de las Fuerzas Militares.

7.4 RESPONSABILIDAD DE LOS ADMINISTRADORES DEL SISTEMA

1. Los administradores del sistema deben hacer respaldos periódicos de la información de los servidores, así como la depuración de los discos duros.
2. Realizar auditorías periódicas al sistema con el fin de localizar intrusos o usuarios que estén haciendo mal uso de los recursos informáticos existentes.
3. Decidir sobre el uso de los recursos del sistema restricción de directorios y programas ejecutables para los usuarios.
4. Revisar el tráfico de paquetes que se estén generando dentro de su segmento de red, a fin de determinar si se está haciendo mal uso de la red o se está generando algún problema que pueda llevar a que se colapsen los sistemas.
5. Crear los perfiles y cuentas de usuario, permitir el acceso correspondiente a los sistemas y revisar las cuentas periódicamente para estar seguros de que no hay usuarios ficticios.
6. Recomendar sobre el uso e implementación de nuevas tecnologías para administración de los sistemas y la red.
7. Reportar las fallas en el desempeño de la red. Solucionar los problemas que se generan en su red local.
8. Determinar qué programas tendrán permisos de ejecución para los usuarios en los servidores.
9. Establecer la encriptación de la información que fluya dentro de la red del Fuerzas Militares.
10. Auditarse las cuentas para verificar que no haya alguna copia de programas y acceso a archivos no autorizados
11. Procurar que el respaldo de la información sea redundante, es decir; que la información sea respaldada en dos medios diferentes y que una de estas copias permanezca en un lugar aparte y seguro del sistema.

12. Tener el inventario de los sistemas de información así como los usuarios autorizados a utilizarlos.
13. Capacitar y responsabilizar al personal (usuarios) del manejo de la información del Fuerzas Militares.
14. Apoyar al Oficial de Seguridad Informática en la implementación de nuevas tecnologías que propendan por la seguridad de la información de las Fuerzas Militares.
15. Reportar los incidentes de seguridad informática al Oficial de Seguridad Informática de cada unidad.

7.5 USO DE CONTRASEÑAS

1. Los passwords y/o contraseñas deben ser frases de mínimo quince (15) caracteres de longitud, combinación de mayúsculas, minúsculas, caracteres especiales y números.
2. Se deben configurar las políticas de claves, en los sistemas operativos cambiando la contraseña autoasignada regularmente (cada treinta (30) días y con más frecuencia si se tienen privilegios de administrador) evitando reutilizar contraseñas antiguas.
3. Siempre que se ingrese o digite la clave de acceso en el sistema se debe tener cuidado que no haya sido observado por otra(s) persona(s), si se tienen dudas hay que proceder a su cambio inmediato.
4. No se deben escoger palabras del diccionario, palabras que estén relacionadas con el usuario (nombres propios, domicilio, fecha de nacimiento, etc.).
5. Si se tiene más de una cuenta en distintos sistemas no es aconsejable utilizar la misma contraseña en todas.
6. La clave es personal e intransferible, se debe mantener en sobre sellado y en custodia del Jefe de cada Dependencia. Cuando por ausencia forzosa o retiro de algún funcionario, se requiera abrir el sobre sellado, esta será cambiada lo antes posible por el funcionario responsable.
7. Mantener la confidencialidad de la contraseña (por ejemplo no escribirla en un papel si no existe forma segura de guardarla) cambiar la contraseña si se tiene algún indicio o posibilidad de que su confidencialidad pueda verse comprometida.
8. No incluir la contraseña en ningún procedimiento automático de conexión o que requiera un cambio de identificador de usuario (por ejemplo en 'scripts' o 'guiones', macros, teclas de función, etc.).

7.5.1 Uso de cuentas sin password ó passwords por defecto

1. Se deben Cambiar todas las contraseñas instaladas por defecto en el proceso de instalación del sistema operativo.

2. Escanear el archivo de contraseñas periódicamente en busca de cuentas con UID igual a 0 (reservado para el usuario privilegiado de Administrador).
3. Escanear el archivo de contraseñas en busca de cuentas nuevas de las que no se tiene conocimiento y que en la mayoría de los casos son indicativo de intrusión.
4. No permitir la existencia de cuentas sin contraseña.
5. Eliminar cuentas de usuarios que se hayan ido de la Institución y cuentas que no se estén utilizando.

7.5.2 Uso de passwords reusables

Se debe reducir o eliminar la transmisión de contraseñas reusables en texto claro sobre la red. De esta forma se evita que las contraseñas sean capturados por lo que se denomina packet sniffers (código para identificar contraseñas).

7.5.3 Uso de one-time passwords

Se debe utilizar el plan de cuentas del sistema, en la introducción de palabras clave para la validación de acceso autenticado. Se deben establecer algunos valores por defecto como son el número mínimo de caracteres que debe tener una contraseña, el máximo período de tiempo en el cual es válido, el mínimo período antes de que la contraseña sea cambiada, bloquear la cuenta después de tres inicios de sesión incorrectos.

7.5.4 Uso de cuentas de guest (ó invitados)

1. Se debe evitar la existencia de cuentas "guest" de invitados. En este sentido, muchos sistemas instalan cuentas para invitados por defecto, por lo que es necesario desactivar o eliminar del sistema este tipo de cuentas.
2. Comprobar el archivo de contraseñas del sistema una vez haya terminado el proceso de instalación del sistema operativo a fin de asegurarse de que todas las cuentas predeterminadas tienen contraseñas válidas o han sido desactivadas o eliminadas.

7.6 EQUIPOS DESATENDIDOS EN ÁREAS DE TRABAJO

1. Los usuarios deben asegurarse de que los equipos desatendidos tengan protección apropiada y responsabilizarse de la implementación de dicha protección.
2. Se deben cerrar las sesiones activas cuando finalice el trabajo, a menos que se puedan asegurar por medio de un mecanismo de bloqueo, como un protector de pantalla protegido por contraseña.
3. Se debe realizar el registro de cierre en computadoras principales, servidores y computadores personales de oficina al terminar la sesión (es decir, no sólo apagar el interruptor de la pantalla del computador o terminal).

7.7 ESTACIONES DE TRABAJO Ó COMPUTADORES DESKTOP

1. Sobre los equipos más críticos de la red se deben definir políticas de arranque del sistema tales como password del setup. Adicionalmente considerar la implementación de sistemas de autenticación basados en huellas digitales, sistemas biométricos, de acuerdo a lo crítico de la función del PC en la red y del personal que valide su acceso a través de este.
2. Se deben asegurar las partes físicas de los equipos y periféricos sobre el escritorio en el caso que estos equipos sean críticos para la red.
3. Los equipos asignados al personal administrativo o a los digitadores de Bases de Datos ó sistemas sensibles o clasificados, deben tener habilitados solo los dispositivos de entrada y salida estrictamente necesarios para cumplir con sus funciones, con el fin de prevenir la sustracción o copia de información no autorizada. Esta habilitación puede ser dada por periodos de tiempo programados y autorizados.
4. Se debe limitar el uso de los recursos compartidos, de ser necesario se deben habilitar los mecanismos de control en el sistema para dar acceso a usuarios autorizados.
5. Todo acceso para lectura o ejecución de programas, documentos o aplicaciones que se haga desde dispositivos de almacenamiento externos, debe ser previamente revisado por un sistema antivirus o anti-spyware para evitar la infección con código malicioso. Las novedades presentadas durante esta inspección rutinaria, deben ser documentadas e informadas al Oficial de Seguridad Informática.
6. Efectuar copias de seguridad (backup) de todos los archivos importantes que son actualizados regularmente.
7. Identificar las copias de respaldo, mediante un rotulo adherido al medio, que indique la fecha, tipo de información, clasificación de la información y nombre del equipo.
8. El mantenimiento, modificación o cualquier tipo de arreglo a los equipos de computo, periféricos, debe ser realizado únicamente por personal autorizado, bajo la supervisión del usuario. Al final del trabajo debe quedar copia del informe técnico respectivo. Cualquier novedad debe ser reportada al administrador de los servicios informáticos de la unidad.
9. Los equipos de cómputo que contengan información clasificada y/o sensible pueden ser retirados de su sitio original, para mantenimiento correctivo, teniendo en cuenta que las unidades de almacenamiento de este equipo deben ser retiradas del equipo, y guardadas de forma segura por el usuario responsable mientras dure el proceso de mantenimiento. Estos procedimientos deben tener autorización del Jefe de la Dependencia. En todos los casos, es necesario informar a la Dependencia o persona encargada de los inventarios fiscales.

10. Si por razones de trabajo los funcionarios que tengan a su cargo un equipo de cómputo necesitan llevarlo a sitios fuera de las instalaciones, deben estar previamente autorizados por el Jefe de la Dependencia, y la información sensible y clasificada que contengan, debe estar encriptada en el disco duro y/o borrada en forma segura. Estos funcionarios deben aplicar todas las políticas de seguridad establecidas para estos casos.
11. Se prohíbe la instalación de juegos y/o software diferente al instalado y autorizado por los funcionarios de las Unidades de Informática y/o Oficial de Seguridad Informática de las Fuerzas Militares.
12. Todos los usuarios deben aplicar las normas y prácticas de seguridad establecidas por el Comité de Seguridad Informática, en el equipo de cómputo asignado.
13. El usuario debe cancelar todas las sesiones activas antes de dejar el equipo desatendido, salvo si se dispone de una herramienta de bloqueo general. El equipo debe tener configurada la opción de protector de pantalla con contraseña, con un tiempo mínimo de activación.
14. El usuario debe desconectarse (Log-off) de todas las sesiones con los servidores antes de apagar el equipo. Los equipos de los usuarios deben quedar apagados al término de labores.
15. El usuario debe verificar de manera permanente que su equipo tenga actualizado el antivirus y software de seguridad como anti_spam, anti-spyware, anti_keyloggers, firewall personal, para evitar perdida de información y daños en el sistema del equipo. Cualquier novedad debe ser informada al Administrador del Sistema o al Oficial de Seguridad Informática.
16. Los equipos que almacenen información clasificada y/o sensible, no deben tener salida a Internet y aplicar las políticas de seguridad para manejo de información establecidas.
17. Todos los equipos de cómputo de las Fuerzas Militares deben tener instalado el logo de ADVERTENCIA DE USO para manejo de los recursos informáticos Institucionales.

7.8 SITIOS DE TRABAJO

1. El sitio de trabajo debe tener el acceso controlado durante las horas laborales. Los fines de semana, días festivos y horas no laborales. En lo posible, cada sitio deberá estar protegido adicionalmente, por un sistema para detección de intrusos (IDS) instalado y supervisado. El IDS emplea seguridad de multi-anillo, usando los sensores de la puerta, los sensores de movimiento y las cámaras de video. Todas las aberturas y ventanas dentro de la Unidad deben ser controladas mediante alarmas y sensores de movimiento y/o sensores de la rotura del cristal. Los sitios se deben supervisar sobre una base de 7x24 (siete días a la semana por veinticuatro horas al día).
2. Además del control de acceso al sitio, el acceso al área que contiene la red, debe contar con un control de acceso perimetral mediante puertas con cerradura.

3. Para proteger la información frente a accesos no autorizados, pérdida, robo u otros daños, los documentos, medios de almacenamiento e información sensible ó clasificada deben guardarse en armarios bajo llave cuando no se usen y especialmente fuera del horario normal de trabajo.

7.9 CONTROL DE ACCESO A LA RED

El acceso de los usuarios a las redes y a los servicios de red no debe poner en peligro la seguridad de los servicios de red, para lo cual:

1. Deben existir interfaces apropiadas entre la red de la Institución y las redes que pertenecen a otras organizaciones, y las redes públicas.
2. Se deben aplicar mecanismos adecuados de autenticación para los usuarios y los equipos.
3. Se debe exigir el control del acceso de los usuarios a los servicios de información.

7.9.1 Utilización de los servicios de red

1. Se deben definir claramente las redes y los servicios de red a los cuales se permite el acceso; así mismo, se deben definir los procedimientos de autorización para determinar a quién se le permite el acceso a qué redes y a qué servicios en red.
2. Se debe tener documentados todos los accesos autorizados, mediante un registro físico que facilite la gestión de administración y control.
3. Se deben definir y documentar los controles y procedimientos de gestión para proteger el acceso a las conexiones de red y los servicios de red. Tanto de los usuarios internos como los externos o remotos
4. Se debe tener un estricto control sobre los administradores en especial los que tienen asignados privilegios especiales autorizados para accesos remotos.

7.9.2 Autenticación de usuarios para conexiones externas

1. Se deben emplear métodos apropiados de autenticación para controlar el acceso de usuarios remotos, tales como: líneas privadas dedicadas, redes privadas virtuales (VPN), autenticación fuerte para acceso a la red, ó la asociación de cuenta, dirección IP e identificación MAC del equipo para su acceso, procedimientos y controles de devolución de marcación, -módem de retorno-, cuando se usa este control, no se deben utilizar los servicios de red que incluyen envío de llamada o, si se hace, se debe desactivar el uso de dichas características para evitar las debilidades asociadas con el envío de llamada.
2. Se deben implementar controles de autenticación adicionales para controlar el acceso a redes inalámbricas. En particular, es necesario tener cuidado en la selección de los

controles para redes inalámbricas debido a las grandes oportunidades para la interceptación e inserción no detectadas en el tráfico de la red.

7.9.3 Autenticación de nodos

La autenticación del nodo puede servir como un medio alterno para la autenticación de grupos de usuarios remotos cuando están conectados a un servicio seguro de red. Para la autenticación del nodo se deben emplear técnicas criptográficas, por ejemplo las basadas en certificados de máquina.

7.9.4 Protección de los puertos de diagnóstico remoto.

1. Se debe garantizar que los puertos de diagnóstico y configuración sólo sean accesibles mediante acuerdo entre el Oficial de Seguridad Informática, el Administrador de Red y el personal de soporte de hardware ó software que requiere el acceso.
2. Los puertos, servicios y prestaciones similares instaladas en un servicio de computador o de red, que no se requieren específicamente para la funcionalidad de la Institución se deben inhabilitar o retirar.

7.9.5 Subdivisión de redes

1. Se deben separar los grupos de servicios de información, usuarios y sistemas de información, por dominios de red internos y dominios de red externos, cada uno protegido por un perímetro de seguridad definido., aplicando un conjunto graduado de controles en los diferentes subdominios.
2. La separación de las redes se debe basar en el valor y la clasificación de la información almacenada o procesada en la red, los niveles de confianza o los lineamientos de la red con el fin de reducir el impacto total de una interrupción del servicio.
3. Se deben separar las redes inalámbricas procedentes de redes internas y/o privadas. Puesto que los perímetros de las redes inalámbricas no están bien definidos, se debe llevar a cabo una evaluación de riesgos en tales casos para identificar los controles (por ejemplo, autenticación fuerte, métodos criptográficos y selección de frecuencia) para mantener la separación de la red.

7.9.6 Control de conexión a la red

1. Se debe restringir la capacidad de los usuarios para conectarse a la red.
2. Se deben restringir los servicios de mensajería instantánea, correo electrónico, transferencia de archivos ftp, acceso a las aplicaciones.
3. Se deben configurar los horarios de los servicios de red –*horas y fechas*- de acuerdo con las funciones de los usuarios y servicios de las aplicaciones. Estos horarios deben estar documentados y autorizados previamente.

7.9.7 Control de ruteo de red

1. Se deben implementar controles de enrutamiento para las redes con el fin de asegurar que las conexiones entre computadores y los flujos de información no incumplan la política de control del acceso de las aplicaciones de la Institución.
2. Las puertas de enlace (gateway) de seguridad se deben usar para validar la fuente y la dirección de destino en los puntos de control de las redes internas y externas, si se emplean tecnologías proxy y / o de traducción de dirección de red.
3. Las redes compartidas, especialmente aquellas que van más allá de las fronteras de la Institución, deben tener controles adicionales de enrutamiento. Esto se aplica particularmente cuando las redes son compartidas por usuarios de terceras partes

7.9.8 Seguridad de los servicios de red

Los servicios de red que incluyen la provisión de conexiones, servicios de red privada y redes con valor agregado, así como soluciones de seguridad de red, como barreras de fuego (firewalls) y sistemas de detección de intrusos deben cumplir con las siguientes características:

1. Tecnología aplicada para la seguridad de los servicios de red, como la autenticación, la encriptación y los controles de conexión de red.
2. Parámetros técnicos requeridos para la conexión segura con los servicios de red según las reglas de seguridad y conexión de red.
3. Procedimientos para la utilización de los servicios de red y restringir los servicios de red o a las aplicaciones, cuando sea necesario.

7.9.9 Control de acceso al sistema operativo

Se deben utilizar medios de seguridad para restringir el acceso de usuarios no autorizados a los sistemas operativos. Tales medios deben tener la capacidad para:

1. Autenticar usuarios autorizados, de acuerdo con una política definida de control del acceso.
2. Registrar intentos exitosos y fallidos de autenticación del sistema.
3. Registrar el uso de privilegios especiales del sistema.
4. Emitir alarmas cuando se violan las políticas de seguridad del sistema.
5. Suministrar medios adecuados para la autenticación.
6. Restringir el tiempo de conexión de los usuarios.

7.9.10 Identificación automática de terminales

Se debe usar la identificación del equipo y/o Mac Address, si la comunicación únicamente se puede iniciar desde un equipo o lugar específico. Un identificador en el equipo o acoplado a éste se puede usar para indicar si está permitido que este equipo se conecte a la red. Estos identificadores deben indicar con claridad a qué red está permitido conectarse el equipo, si existe más de una red y si estas redes tienen sensibilidad diferente. Se debe considerar la protección física del equipo para mantener la seguridad del identificador de éste.

7.9.11 Identificación y autenticación de usuarios

1. Todos los usuarios deben tener un identificador único (ID del usuario) para su uso personal.
2. Este control se debe aplicar a todos los tipos de usuarios (incluyendo el personal de soporte técnico, operadores, administradores de red, programadores de sistemas y administradores de bases de datos).
3. Los identificadores de usuario (ID) se deben utilizar para rastrear las actividades de la persona responsable.
4. Cuando exista un acceso externo y en beneficio para las Fuerzas Militares, se puede usar un identificador de usuario único. La aprobación de este debe ser avalado por el Jefe de la Unidad, los directores de Informática y el oficial de seguridad y estar documentadas para dichos casos.
5. Cuando se requiera verificación de identidad y autenticaciones sólidas, se deben utilizar métodos alternos a la contraseña, como los medios criptográficos, las tarjetas electrónicas, señales (token) o medios biométricos.

7.9.12 Sistema de administración de contraseñas

El sistema de gestión de contraseñas debe:

1. Hacer cumplir el uso de identificadores de usuario (ID) individual y de contraseñas para conservar la responsabilidad.
2. Permitir a los usuarios la selección y el cambio de sus contraseñas e incluir un procedimiento de confirmación para tener en cuenta los errores en las entradas.
3. Imponer una elección de contraseñas de calidad.
4. Imponer cambios de contraseña.
5. Forzar a los usuarios a cambiar las contraseñas temporales en el primer inicio de sesión.
6. Conservar un registro de las contraseñas de usuario previas y evitar su reutilización.

7. No mostrar contraseñas en la pantalla cuando se hace su ingreso.

7.9.13 Uso de utilitarios del sistema

Se deben considerar los siguientes aspectos para el uso de las utilidades del sistema:

1. Los utilitarios del sistema solo deben ser utilizados por los administradores teniendo en cuenta su registro y uso.
2. Retiro o inhabilitación de todas las utilidades o el software del sistema basado en software innecesario.
3. No poner a disposición las utilidades del sistema a usuarios sin privilegios y funciones de administrador.

7.9.14 Alarmas silenciosas para la protección de los usuarios

Se deben instalar y/o implementar alarmas silenciosas en los dispositivos activos de red (Firewall, IDS), para proteger el perímetro y la integridad de las redes de las Fuerzas Militares.

7.9.15 Desconexión de terminales por tiempo muerto

1. Se debe cerrar la sesión de red después de un periodo definido de inactividad. El tiempo de inactividad debe reflejar los riesgos de seguridad del área, la clasificación de la información que se maneja y las aplicaciones que se utilizan, así como los riesgos relacionados con los usuarios del equipo.
2. Este control es importante en lugares de alto riesgo, los cuales incluyen áreas públicas o externas fuera de la gestión de seguridad de la Institución. Las sesiones se deben cerrar para evitar el acceso de personas no autorizadas y negar ataques al servicio.

7.9.16 Limitación del horario de conexión

1. Se deben tener en cuenta los controles de tiempo para las aplicaciones sensibles de computador, especialmente las de lugares de alto riesgo, por ejemplo áreas públicas o externas que están fuera de la gestión de seguridad de la Institución.
2. Restricción de los tiempos de conexión a las horas normales de oficina, si no se requiere tiempo extra u operaciones de horario prolongado;

7.10 CONTROL DE ACCESO A LAS APLICACIONES

1. El acceso lógico al software de aplicación y a la información debe ser restringido de acuerdo al perfil del usuario.

2. Se debe suministrar protección contra acceso no autorizado por una utilidad del software del sistema operativo y software malicioso que pueda anular o desviar los controles del sistema o de la aplicación.

7.10.1 Restricción del acceso a la información

1. Se deben proporcionar menús para controlar el acceso a las funciones de los sistemas de aplicación.
2. Se deben controlar los derechos de acceso de los usuarios, de manera particular, sobre cada uno de los sistemas por ejemplo, leer, escribir, eliminar y ejecutar.
3. Garantizar que los datos de salida de los sistemas de aplicación que manejan información sensible sean solo los solicitados y que se envían únicamente a terminales o sitios autorizados; esto debe incluir revisiones periódicas de dichas salidas para garantizar la seguridad de la información.

7.10.2 Aislamientos de sistemas sensibles

1. La sensibilidad de un sistema de aplicación se debe identificar y documentar por el dueño de la aplicación.
2. Cuando una aplicación se ha de ejecutar en un entorno compartido, los sistemas de aplicación con los cuales compartirá recursos y los riesgos correspondientes deben ser identificados y aceptados por el dueño de la aplicación sensible.
3. La sensibilidad indica que el sistema de aplicación debe ejecutarse en un computador dedicado y únicamente debe compartir recursos con sistemas de aplicación confiables.

7.10.3 Monitoreo del acceso y uso de los sistemas

1. Se deben instalar sistemas de monitoreo de la red, detección de intrusos y detección de vulnerabilidades para realizar labores encaminadas a obtener información respecto al uso de la red, rendimiento, acceso a los sistemas y detectar posibles ataques al sistema y la forma de realizarlos.
2. Se debe llevar un registro de la administración de configuración de todo el equipo (hardware, software, soporte lógico inalterable –firmware-, interfaces de comunicaciones, procedimientos de funcionamiento y estructuras de la instalación). Incluido en el expediente de administración de la configuración y un listado detallado de todos los cambios temporales a los lineamientos aprobados de la red.
3. Se debe llevar un registro de todo el mantenimiento y reparaciones del hardware de la red de las Fuerzas Militares, incluyendo la instalación o el retiro de los equipos activos y de sus dispositivos, así como un registro de todos los visitantes autorizados y un registro de los chequeos de seguridad realizados y el comienzo y cierre de cada día de trabajo.

7.10.4 Sincronización de relojes

Se debe implementar un servidor de sincronización de tiempo para todos los equipos activos de la red de las Fuerzas Militares. Esta sincronización debe ser verificada periódicamente por el Oficial de Seguridad Informática de los Sistemas de Información.

7.10.5 Registro de eventos

1. Los registros de eventos de la red de las Fuerzas Militares deben ser revisados por el Administrador del Sistema y el Oficial de Seguridad Informática de cada unidad, sobre una base mensual ó eventual ante la presencia ó sospecha de incidentes informáticos.
2. Todos los registros de auditoria serán mantenidos en archivo por un período de 12 meses para revistas y como referencia.
3. Los registros de eventos deben indicar el momento exacto y el usuario (persona o proceso) que lo realizó, para garantizar que la información relacionada con las acciones y actividades de los usuarios se encuentre debidamente registrada y monitoreada.

7.11 COMPUTACIÓN MÓVIL Y TRABAJO REMOTO

1. Cuando se usen servicios de computación y de comunicaciones móviles, por ejemplo, computadores portátiles (notebooks y laptops), microcomputadores de bolsillo (palmtops), tarjetas electrónicas y teléfonos móviles se debe tener cuidado especial para asegurarse que la información no se pone en peligro.
2. Se debe tener especial cuidado cuando se utilizan servicios de computación móvil en lugares públicos, salas de reuniones y otras áreas en entornos sin protección fuera de las instalaciones de la Institución. Se debe establecer la protección física y lógica necesaria para evitar el robo del equipo, el acceso o la divulgación no autorizados de la información almacenada y procesada por estos servicios, usando técnicas criptográficas, la disponibilidad de copias de respaldo y la protección contra virus o software malicioso. En caso de tener dispositivos inalámbricos, se deben bloquear los servicios de conexión cuando no se estén usando y no servicios compartidos.
3. Se debe establecer un procedimiento en el que se tengan presentes los requisitos legales, de seguros y otros de seguridad de la Institución para los casos de robo o pérdida de los servicios de computación móvil.
4. El equipo que porte información sensible y / o crítica importante de la Institución no se debe dejar desatendido, debe tener el disco duro encriptado y se debe bloquear y anclar con algún medio físico o usar software de encripción para asegurar los archivos almacenados.
5. El Oficial de Seguridad Informática, debe disponer de la información del personal que utiliza computación móvil para concientizarlo sobre los riesgos adicionales que se originan en este tipo de trabajo y los controles que se deben implementar.

6. Las conexiones inalámbricas o de red móvil son similares a otros tipos de conexión de red, pero tienen diferencias importantes que se deben considerar al identificar los controles, ya que algunos protocolos de seguridad inalámbrica son inmaduros y tienen debilidades conocidas.
7. Se deben considerar los siguientes aspectos cuando se trabaja remotamente:
 - a. La seguridad física existente en el sitio de trabajo remoto, tomando en consideración la seguridad física de la edificación y del entorno físico local.
 - b. Los requisitos de seguridad de las comunicaciones, pensando en la necesidad de acceso remoto a los sistemas internos de la Institución, la sensibilidad de la información a la cual se tendrá acceso y de sobrepassar el enlace de comunicación y la sensibilidad del sistema interno.
 - c. La amenaza del acceso no autorizado a la información o de los recursos por parte de otras personas que usan el mismo espacio (terceras partes).
 - d. El uso de redes domésticas y los requisitos o restricciones en la configuración de servicios de red inalámbrica.
 - e. Las políticas y los procedimientos para evitar disputas con respecto a los derechos de propiedad intelectual desarrollados o al equipo de propiedad privada.
 - f. El acceso a equipo de propiedad privada (para verificar la seguridad de la máquina o durante una investigación), el cual puede estar prohibido por la ley.
 - g. Protección antivirus y requisitos de barreras contra fuego (firewall).
 - h. Disposición de equipo adecuado y medios de almacenamiento para las actividades de trabajo remoto, en las que no se permite el uso de equipo de propiedad privada que no esté bajo el control de la Institución.
 - i. Definición del trabajo que se permite realizar, las horas laborables, la confidencialidad de la información que se conserva y los sistemas y servicios internos para los cuales el trabajador tiene acceso autorizado;
 - j. Disposición de equipo de comunicación apropiado, incluyendo los métodos para asegurar el acceso remoto y la seguridad física.
 - k. Reglas y procedimientos sobre el acceso de familiares y visitantes al equipo y a la información;
 - l. Disposición de soporte y mantenimiento de hardware y software.
 - m. Disposición de pólizas de seguros.
 - n. Procedimientos para el respaldo y manejo de contingencias

- o. Auditoría y monitoreo de seguridad.
- p. Revocación de autoridad y derechos de acceso, y la devolución del equipo al finalizar las actividades de trabajo remoto.

8. DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN

8.1 REQUERIMIENTOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN

- 1. Se debe garantizar que la seguridad es una parte integral de los sistemas de Información, dentro de los cuales se incluyen sistemas operativos, infraestructura, aplicaciones servicios y aplicaciones desarrolladas para usuarios. El diseño y la implementación del sistema de información que da soporte a los procesos de las Fuerzas Militares que pueden ser críticos para la seguridad.
- 2. Se deben identificar y acordar los requisitos de seguridad antes del desarrollo y / o la implementación de los sistemas de información.
- 3. Todos los requisitos de seguridad se deben identificar en la fase inicial de un proyecto y se deben justificar, acordar y documentar como parte de todo el proyecto para un sistema de información.

8.1.1 Análisis y especificación de los requisitos de seguridad

- 1. Se deben declarar los requisitos para nuevos sistemas de información, mejoras a los sistemas existentes especificando los requisitos para los controles de seguridad.
- 2. Se debe considerar los controles automatizados que se han de incorporar en el sistema de información y la necesidad de controles manuales de soporte; de igual manera aplica cuando se evalúan los paquetes de software, desarrollados o adquiridos, los requisitos de seguridad y los controles deben reflejar el valor de los activos de información involucrados y el daño potencial que se puede presentar debido a una falla o a la ausencia de seguridad.
- 3. Los requisitos del sistema para la seguridad de los activos y la información y los procesos para implementarla se deben documentar e integrar en las fases iniciales de los proyectos del sistema de información y deben ser objeto de pruebas de aceptación.
- 4. Los contratos con el proveedor deberán abordar los requisitos de seguridad identificados.
- 5. Cuando la funcionalidad de la seguridad de un producto determinado no satisface el requisito específico, entonces se debe considerar la inclusión de los controles a los riesgos, introducidos y asociados, antes de adquirir el producto.

6. Cuando los productos requeridos proporcionan una funcionalidad adicional y ello causa un riesgo de seguridad, tal funcionalidad se debe inhabilitar o se deberá revisar la estructura del control propuesto para determinar si se puede obtener ventaja de la funcionalidad mejorada disponible.

8.2 SEGURIDAD EN LOS SISTEMAS DE APLICACIÓN

1. Se deben evitar errores, pérdidas, modificaciones no autorizadas o uso inadecuado de la "información en las aplicaciones".
2. Se deben diseñar controles apropiados en las aplicaciones, incluyendo las aplicaciones desarrolladas por el usuario para garantizar el procesamiento correcto, estos controles deben incluir la validación de los datos de entrada, del procesamiento interno y de los datos de salida.
3. Se pueden necesitar controles adicionales para los sistemas que procesan o tienen "impacto en la información sensible, de valor o crítica. Dichos controles se deberían determinar con base en los requisitos de seguridad y en la evaluación de riesgos.

8.2.1 Validación de los datos de entrada

1. Se deben realizar verificaciones de las entradas de las transacciones de los datos permanentes o requeridos (por ejemplo, nombres y direcciones).
2. Se deben verificar las entradas duales u otras entradas, tales como verificación de fronteras o campos limitantes para especificar los rangos de los datos de entrada, con el fin de detectar los siguientes errores: valores fuera de rango, caracteres no válidos en los campos de datos, datos incompletos o ausentes, exceso en los límites superiores e inferiores del volumen de datos, datos de control inconsistentes o no autorizados.
3. Se deben hacer revisiones periódicas del contenido de los campos clave o de los archivos de datos para confirmar su validez e integridad.
4. Se deben inspeccionar los documentos de entrada impresos para determinar cambios no autorizados (todos los cambios en los datos de entrada deben estar autorizados).
5. Se deben diseñar y documentar los procedimientos de respuesta ante errores de validación y procedimientos para probar la credibilidad de los datos de entrada.
6. Se deben definir las responsabilidades para todo el personal que participa en el proceso de entrada de datos y se debe crear un registro de las actividades implicadas en el proceso de entrada de datos.
7. Se debe pensar en la validación y el examen automático de los datos de entrada, cuando se puedan aplicar, para reducir el riesgo de errores y evitar ataques normales, incluyendo desbordamiento de búfer o inyección de códigos.

8.2.2 Control del procesamiento interno

1. El diseño y la implementación de las aplicaciones debe garantizar que se minimizan los riesgos de falla en el procesamiento, que originan pérdida de la integridad y disponibilidad, para lo cual deben tener en cuenta como mínimo, procedimientos tales como: evitar que los programas se ejecuten en orden erróneo, utilización de programas para la recuperación después de fallas, protección contra ataques empleando desbordamiento / exceso en el buffer, controles de sesión o de lotes, para conciliar los balances de archivos de datos después de actualizar las transacciones, controles para cada ejecución, totales de actualizaciones de archivos, controles programa-a-programa, validación de los datos de entrada generados por el sistema, verificaciones de la integridad, la autenticidad o cualquier otra característica de seguridad de los datos o del software descargado o actualizado entre el computador central y el remoto, totales de verificación (hash) de registros y archivos, verificaciones para garantizar que los programas de aplicación se ejecutan en el tiempo y orden correcto y terminan en caso de falla, deteniendo el procesamiento posterior hasta que se resuelve el problema, creación de un registro de las actividades implicadas en el procesamiento.
2. Los datos que se han ingresado correctamente se pueden corromper por errores de software, de procesamiento o a través de actos deliberados, por tal razón se deben realizar verificaciones de validación que dependen de la naturaleza de la aplicación y del impacto de la corrupción de los datos en la organización.

8.2.3 Autenticación de los mensajes

1. Se deben identificar los requisitos para asegurar la autenticidad y proteger la integridad del mensaje en las aplicaciones, así como identificar e implementar los controles adecuados.
2. Se deben realizar una evaluación de los riesgos de seguridad para determinar si se requiere integridad del mensaje y para identificar el método más apropiado de implementación, haciendo uso de técnicas criptográficas como un medio de autenticación del mensaje.

8.2.4 Validación de los datos de salida

Comúnmente, los sistemas y las aplicaciones se construyen asumiendo que al realizar la validación, la verificación y las pruebas adecuadas, la salida siempre será correcta. Sin embargo, esta suposición no siempre es válida; es decir, los sistemas que se han sometido a prueba aún pueden producir salidas incorrectas en algunas circunstancias.

1. Se deben validar los datos de salida de una aplicación para asegurar que el procesamiento de la información almacenada es correcto y adecuado a las circunstancias.
2. La validación de los datos de salida puede incluir:
 - a. Verificaciones de la calidad y razonabilidad de los datos de salida.

- b. Suministro de información suficiente para que un lector o un sistema de procesamiento posterior determine la exactitud, totalidad, precisión y clasificación de la información.
- c. Procedimientos para responder las pruebas de validación de salidas.
- d. Definición de las responsabilidades de todo el personal que participa en el proceso de la salida de datos.
- e. Creación de un registro de las actividades del proceso de validación de la salida de datos.

8.3 SEGURIDAD DE LOS ARCHIVOS DEL SISTEMA

8.3.1 Control del software operativo

- 1. La actualización del software operativo, las aplicaciones y las librerías de los programas sólo se debe realizar por administradores capacitados.
- 2. Los sistemas operativos únicamente deben contener códigos ejecutables aprobados.
- 3. El software de las aplicaciones y del sistema operativo sólo se deben implementar después de pruebas de funcionalidad y de tiempos de respuesta.
- 4. Se debe usar un sistema de control de configuración, para mantener el control del software implementado, así como de la documentación del sistema.
- 5. Se debe conservar un registro para auditoría de todas las actualizaciones de las librerías de los programas operativos.
- 6. Es conveniente conservar las versiones anteriores del software de aplicación como medida de contingencia.
- 7. Las versiones antiguas de los aplicativos se deben archivar junto con toda la información requerida y los parámetros, procedimientos, detalles de configuración y software de soporte, en la medida en que los datos se retengan en archivo.
- 8. Ningún software debe estar en producción sin soporte y se debe prever que en la contratación quede establecida la transferencia tecnológica.
- 9. El acceso físico o lógico únicamente se debe dar a los proveedores para propósitos de soporte, cuando sea necesario, y con la respectiva aprobación. Las actividades del proveedor se deben monitorear.

8.3.2 Protección de los datos de prueba del sistema

- 1. Los procedimientos de control del acceso a los sistemas de aplicación operativos también se deben ejecutar a los sistemas de pruebas.

2. La información operativa se debe borrar del sistema de aplicación de prueba inmediatamente después de terminada.
3. El copiado y utilización de la información operativa se debe registrar para brindar un rastro de auditoría.

8.3.3 Control de acceso a las bibliotecas de programas fuente

1. El código fuente y las librerías de los aplicativos desarrollados para la Fuerzas Militares, así como el software para su servicio, se debe considerar como información clasificada y su acceso debe ser restringido y en caso necesario debe ser autorizado por el Jefe del área informática de la Unidad dueña de los derechos del aplicativo.
2. Se debe conservar un registro de todos los accesos al código fuente y las librerías de los aplicativos con el fin de facilitar las labores de auditoría.
3. El mantenimiento y el copiado de las librerías fuente de programas deben estar sujetos a un procedimiento estricto de control de cambios.

8.4 SEGURIDAD EN LOS PROCESOS DE DESARROLLO Y SOPORTE

8.4.1 Procedimientos de control de cambios

1. Los procedimientos formales de control de cambios deben ser documentados y solo entran en producción después de la aprobación por el dueño del aplicativo y cumplimiento del control de calidad.
2. Los controles de cambio deben incluir una evaluación de riesgos, análisis de los impactos de los cambios y especificación de los controles de seguridad necesarios.
3. Se debe dar acceso a los programadores de soporte sólo a aquellas partes del sistema necesarias para su trabajo y que existe un acuerdo y aprobación formal para cualquier cambio.
4. Siempre que sea factible, en los procedimientos de control de cambios operativos y de aplicación se deben tener en cuenta los siguientes aspectos:
 - a. La verificación de los niveles acordados de autorización.
 - b. La garantía de que los cambios son realizados por personal autorizado y capacitado.
 - c. La revisión de los controles y de los procedimientos de integridad para asegurar que no se pondrán en peligro debido a los cambios.
 - d. La identificación de todo el software, la información, las entidades de bases de datos y del hardware que requieran mejora.
 - e. La obtención de la aprobación formal de las propuestas detalladas antes de iniciar el trabajo.
 - f. Actualizar la documentación del sistema al finalizar cada cambio.

- g. Verificar que la documentación operativa y los procedimientos de usuario se cambian en función de la necesidad con el objeto de mantener su idoneidad.
- h. Realizar la implementación de los cambios en el momento oportuno y verificar que no se perturban los procesos de los servicios involucrados.

8.4.2 Revisión técnica de las aplicaciones después de los cambios en el sistema operativo

- 1. Se deben revisar los procedimientos de integridad y control de la aplicación para asegurarse de que no se han puesto en peligro, debido a los cambios en el sistema operativo.
- 2. Se debe incluir en el plan y el presupuesto de soporte anual las revisiones y pruebas del sistema que resulten de cambios en el sistema operativo.
- 3. Se debe notificar oportunamente sobre los cambios en el sistema operativo para permitir la realización de las pruebas y las revisiones apropiadas antes de la implementación.
- 4. Se deben monitorear las vulnerabilidades y las nuevas versiones de parches y arreglos (fixes) ofrecidos por el distribuidor.

8.4.3 Restricciones en los cambios a los paquetes de software

- 1. Se deben controlar todos los cambios ó modificaciones a los paquetes de software, y limitarlos a los cambios necesarios.
- 2. Los paquetes de software suministrados por terceras partes, se deben usar sin modificaciones. Cuando sea necesario modificar un paquete de software, se deben tener en cuenta los siguientes puntos:
 - a. El riesgo de que los procesos de integridad y de control incorporados se vean comprometidos.
 - b. Si es necesario, obtener el consentimiento del vendedor.
 - c. La posibilidad de obtener los cambios requeridos del vendedor como un programa estándar de actualizaciones.
 - d. El impacto, si la Institución se hace responsable del mantenimiento futuro del software como resultado de los cambios. Si los cambios son necesarios, el software original se deberá conservar y los cambios se deben aplicar a una copia claramente identificada.
- 3. Se debe implementar un proceso de gestión de las actualizaciones del software para asegurarse de que los últimos parches aprobados y mejoras de las aplicaciones están instalados en todo el software autorizado. Todos los cambios se deben probar y documentar en su totalidad de manera que se puedan volver a aplicar, si es necesario, para mejoras futuras del software.

8.4.4 Canales ocultos y código troyano

1. Exploración de los medios y comunicaciones de salida para determinar la información oculta
2. Comportamiento de las comunicaciones y del sistema de modulación y enmascaramiento para reducir la probabilidad de que una tercera parte pueda deducir información a partir de tal comportamiento.
3. Utilización de sistemas y software que se consideran con integridad alta, por ejemplo usar productos evaluados.
4. Monitoreo regular de las actividades del personal y del sistema, cuando está permitido por la legislación o los reglamentos existentes.
5. Monitoreo del uso de los recursos en los sistemas de computador.
6. Evitar que los usuarios accedan a los dispositivos de lectura desde donde puedan de manera intencional, involuntaria o accidental, contaminar los sistemas con código malicioso.

8.4.5 Desarrollo de software contratado externamente

1. Acuerdos sobre licencias, propiedad de los códigos y derechos de propiedad intelectual.
2. Certificación de la calidad y exactitud del trabajo realizado.
3. Convenios de fideicomiso en caso de falla de la tercera parte.
4. Derechos de acceso para auditar la calidad y exactitud del trabajo realizado.
5. Requisitos contractuales para la calidad y la funcionalidad de la seguridad del código.
6. Realización de pruebas antes de la instalación para detectar códigos troyanos o maliciosos.

9. GESTIÓN DE LA CONTINUIDAD DE LOS SERVICIOS INFORMÁTICOS

9.1 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN

9.1.1 Inclusión de la seguridad de la información en el proceso de gestión de la continuidad de los servicios informáticos

1. Se debe documentar los riesgos que enfrenta la Institución en términos de la probabilidad y el impacto en el tiempo, incluyendo la identificación y la determinación de la prioridad de los procesos críticos.

2. Se debe crear una lista de identificación de todos los activos involucrados en los procesos críticos.
3. Se debe documentar el impacto que puedan tener las interrupciones causadas por incidentes de seguridad de la información (es importante encontrar soluciones para manejar los incidentes que producen impactos menores, así como los incidentes graves que puedan amenazar la viabilidad de la Institución);
4. En las contrataciones se deben adquirir pólizas de seguros adecuadas que puedan formar parte de todo el proceso de continuidad y de la gestión de riesgos operativos;
5. Se debe crear una lista de identificación de riesgos e implementación de controles preventivos y mitigantes adicionales.
6. Se deben identificar y documentar los recursos informáticos, organizacionales, técnicos y ambientales suficientes para tratar los requisitos identificados de la seguridad de la información;
7. Se debe garantizar la seguridad del personal y la protección de los servicios de procesamiento de información y de la propiedad de la Institución;
8. Se debe formular y documentar los planes de continuidad de los servicios informáticos de la Institución que abordan los requisitos de seguridad de la información.
9. Se deben hacer pruebas y actualización regular de los planes y procesos establecidos.

9.1.2 Continuidad de los servicios informáticos y evaluación de riesgos

1. Se deben identificar y documentar los eventos (o secuencia de eventos) que pueden causar interrupciones en los procesos de la organización, por ejemplo fallas de los equipos, errores humanos, robo, desastres naturales y actos terroristas.
2. Se deberá continuar con una evaluación de riesgos para determinar la probabilidad y el impacto de tales interrupciones, en términos de tiempo, escala de daño y periodo de recuperación.
3. Se debe hacer una evaluación donde se identifique, cuantifique y prioricé los riesgos frente a los criterios y los objetivos pertinentes para la Institución, incluyendo los recursos críticos, impactos de las interrupciones, duración permitida de corte y prioridades de recuperación.
4. Se debe desarrollar una estrategia de continuidad de los servicios informáticos para determinar el enfoque global. Una vez se ha creado esta estrategia, el Jefe de la unidad Informática debe aprobarla y crear y respaldar un plan de contingencia para la implementación de esta estrategia.

9.1.3 Desarrollo e implementación de planes de continuidad que incluyan la seguridad de la información

1. Se debe identificar, acordar y documentar todas las responsabilidades y los procedimientos para la continuidad de los servicios informáticos.
2. Se deben implementar los procedimientos que permitan recuperar y restaurar los sistemas de información y la disponibilidad de los datos en las escalas de tiempo requeridas; es necesario atender la evaluación de las dependencias internas y externas y de los contratos establecidos.
3. Se deben documentar los procedimientos y procesos acordados (manual de Funciones y Procedimientos).
4. Se deben hacer pruebas periódicas y actualización de los planes de contingencia.

9.1.4 Estructura para la planificación de la continuidad de los servicios Informáticos

1. Identificar los requisitos de seguridad de la información.
2. Identificar las condiciones para la activación de los planes que describan el proceso a seguir (por ejemplo, la forma de evaluar la situación y quién se va a involucrar) antes de activar cada plan.
3. Documentar los procedimientos de emergencia que describan las acciones a realizar tras un incidente que ponga en peligro las operaciones informáticas.
4. Documentar los procedimientos de respaldo que describan las acciones a realizar para desplazar las actividades esenciales o los servicios de soporte a lugares temporales alternos y devolver la operatividad de los procesos informáticos en los plazos requeridos.
5. Documentar los procedimientos operativos temporales a seguir mientras se terminan la recuperación y la restauración.
6. Programar el mantenimiento que especifique cómo y cuándo se realizarán pruebas al plan y el proceso para el mantenimiento del mismo.
7. Realizar actividades de concientización, educación y formación diseñadas para comprender los procesos de continuidad del negocio y garantizar que los procesos siguen siendo eficaces.
8. Identificar y responsabilizar a las personas, encargadas de la ejecución de cada componente del plan; si se requiere se deberán nombrar los suplentes.
9. Identificar los activos y recursos críticos necesarios para ejecutar los procedimientos de emergencia, respaldo y reanudación.

9.1.5 Pruebas, mantenimiento y reevaluación de los planes de continuidad de los servicios informáticos

1. Se debe hacer una prueba sobre papel de varios escenarios, analizando las disposiciones de recuperación con ayuda de ejemplos de interrupciones.
2. Se deben realizar simulaciones, particularmente para la formación del personal en sus funciones de gestión de crisis / post-incidentes.
3. Se deben realizar pruebas de recuperación técnica, garantizando que los sistemas de información se pueden restaurar eficazmente.
4. Se deben realizar pruebas de los recursos y servicios del proveedor, asegurando que los servicios y productos proporcionados externamente cumplirán el compromiso contraído.
5. Se deben realizar ensayos completos del plan, probando que la organización, el personal, el equipo, las instalaciones y los procesos puedan hacer frente a las interrupciones.

10. REQUERIMIENTOS LEGALES

10.1 PRESUNCIÓN

Las Fuerzas Militares, han puesto todos sus esfuerzos en la mitigación de los riesgos informáticos para evitar la fuga de información.

10.2 EN CUANTO A LOS PERJUICIOS

1. Los usuarios exoneran a las Fuerzas Militares de toda responsabilidad en relación con los perjuicios que puedan ocaſionarse a terceros o a la entidad que representan por el uso indebido o no autorizado de los mecanismos de seguridad y sus componentes, o del incumplimiento por parte del usuario de las órdenes que sean impartidas utilizando los mecanismos de seguridad.

10.3 RESPECTO A LA ENTREGA

1. Todo mecanismo de seguridad y componentes será entregado a los respectivos usuarios mediante documentos denominados "Actas de entrega" donde se estipula claramente el nombre de los usuarios, su documento de identidad, cargo, el mecanismo de seguridad al que está autorizado y el componente técnico que se está entregando.
2. Una vez terminado el contrato de servicio con las Fuerzas Militares, se debe hacer la devolución de los componentes entregados.

10.4 RESPONSABILIDADES

1. Uso adecuado de los mecanismos de seguridad: Dado que el usuario conoce las graves implicaciones que podría ocasionar el uso indebido o no autorizado de los mecanismos de seguridad y sus componentes, se obligan a limitar el acceso a estos únicamente a las personas señaladas en las respectivas "Actas de entrega" y a mantener los componentes de los mecanismos de seguridad bajo estrictas medidas de seguridad.
2. Respeto a los reglamentos y circulares: Los usuarios se obligan a dar estricto cumplimiento a los reglamentos directivas y circulares que establezcan las Fuerzas Militares, en relación con los dispositivos de seguridad, con el manejo y utilización de los mecanismos de seguridad y sus componentes.
3. Los usuarios se comprometen a mantener estricta confidencialidad frente a terceros, respecto a los detalles de los mecanismos de seguridad ofrecidos por las Fuerzas Militares y cualquier comunicación que se requiera emitir al respecto debe ser autorizada formalmente por el Comité de Seguridad Informática de las Fuerzas Militares

10.5 EFECTOS LEGALES DE LA INFORMACIÓN

Para todos los efectos legales, las comunicaciones que utilicen los mecanismos de seguridad ofrecidos por las Fuerzas Militares y este a su vez las haya validado, se considerarán auténticas y en consecuencia el emisor de la comunicación responderá plenamente por su contenido. De tal manera, que los usuarios autorizan a la Fuerzas Militares a actuar conforme a las órdenes enviadas mediante la utilización de los mecanismos de seguridad, comprometiéndose a responder por las operaciones que éste ejecute en cumplimiento de tales instrucciones.

10.6 AUTORIZACIONES

Los usuarios autorizan a las Fuerzas Militares para monitorear y supervisar toda la información que se produzca, almacene ó viaje a través de los activos informáticos propios o en custodia de las Fuerzas Militares, por los esquemas de comunicación posibles con las redes de las Fuerzas Militares.

AUTENTICA:

Mayor General **JORGE ENRIQUE PARGA PARGA**
Jefe Inteligencia y Contrainteligencia Militar Conjunta