



TECNOLOGÍAS DE LA INFORMACIÓN

ENTREGA, SERVICIO Y SOPORTE DE TI

GESTIÓN DE LOS SERVICIOS DE SEGURIDAD


MANUAL DE SEGURIDAD INFORMÁTICA

Código
A01-SO-02-UI.MAN01

Versión No. 01


Página 1 de 16

MANUAL DE SEGURIDAD INFORMÁTICA

	TECNOLOGÍAS DE LA INFORMACIÓN	Código
	ENTREGA, SERVICIO Y SOPORTE DE TI	A01-SO-02-UI.MAN01
	GESTIÓN DE LOS SERVICIOS DE SEGURIDAD	Versión No. 01
	MANUAL DE SEGURIDAD INFORMÁTICA	Página 2 de 16

INDICE

1.	INTRODUCCION	3
2.	OBJETIVOS	4
3.	ALCANCE	4
4.	DEFINICIONES.....	4
5.	SIGLAS	6
6.	DESARROLLO O CONTENIDO	7
6.1	GENERALES	7
6.2	LINEAMIENTOS DE SEGURIDAD	7
6.3	DEL EQUIPO	7
6.4	DEL CONTROL DE ACCESOS.....	9
6.5	DE LA UTILIZACION DE RECURSOS DE REDES.....	12
6.6	DEL SOFTWARE	12
6.7	DE LA SUPERVISION Y EVALUACION	16

	TECNOLOGÍAS DE LA INFORMACIÓN	Código
	ENTREGA, SERVICIO Y SOPORTE DE TI	A01-SO-02-UI.MAN01
	GESTIÓN DE LOS SERVICIOS DE SEGURIDAD	Versión No. 01
	MANUAL DE SEGURIDAD INFORMÁTICA	Página 3 de 16


1. INTRODUCCION

Los requerimientos de seguridad que involucran las tecnologías de la información, en pocos años han cobrado un gran auge y más aun con las de carácter globalizador como lo son la de internet y en particular, la relacionada con el Web, situación que ha llevado a la aparición de nuevas amenaza a los sistemas computarizados.

Por lo anterior, la Dirección Nacional de Medicamentos, en adelante “la Dirección “o “la DNM”, identifico la necesidad de normar el uso adecuado de estas destrezas tecnológicas para aprovechar estas ventajas, evitar su uso indebido y problemas en los bienes y servicios del instituto.

De esta manera, estos lineamientos de seguridad para los equipos y programas de informática, emergen como el instrumento de apoyo a los servidores públicos de la DNM, acerca de la importancia y sensibilidad de la información y servicios críticos y de la superación de las posibles fallas.

Los presentes lineamientos deberán seguir un proceso de actualización cada dos años o cuando sea necesario sujetos a los cambios organizacionales relevantes: crecimiento de la planta personal, cambio en la infraestructura informática, desarrollo de nuevos servicios, entre otros.

	TECNOLOGÍAS DE LA INFORMACIÓN	Código
	ENTREGA, SERVICIO Y SOPORTE DE TI	A01-SO-02-UI.MAN01
	GESTIÓN DE LOS SERVICIOS DE SEGURIDAD	Versión No. 01
	MANUAL DE SEGURIDAD INFORMÁTICA	Página 4 de 16

2. OBJETIVOS

2.1 GENERAL

Establecer lineamientos de trabajo para la Unidad de Informática con el fin seguir los procedimientos adecuados para proporcionar seguridad en el manejo y resguardo de información e infraestructura.

2.2 ESPECIFICOS


- Dar a conocer a cada técnico sobre los procedimientos y normativas a seguir en la UI.
- Exponer a las demás unidades los lineamientos que se pueden y deben seguir para el manejo adecuado de software y hardware.

3. ALCANCE

Estos lineamientos aplican para el uso tanto de software como hardware, para todas las unidades y para el manejo de la información crítica de la institución, desde los accesos a datos hasta la eliminación de los mismos, instalaciones de equipos y servicios, y mantenimientos.


4. DEFINICIONES

- **Área Crítica:** Es el área física donde se encuentra instalado el equipo de informática y telecomunicaciones que requiere de cuidados especiales y que son indispensables para el funcionamiento continuo de los sistemas de comunicación a los están conectados.
- **Auditoria:** Llevar a cabo una inspección y examen independiente de los registros del sistema y actividades para probar la eficiencia de la seguridad de datos y procedimientos de integridad de datos, para asegurar el cumplimiento con la política establecida y procedimientos operativos y para recomendar cualquier cambio que se estime necesario.
- **Backup (copia de seguridad):** Los programas y/o técnicas de respaldo (backup), son las que permiten realizar una copia espejo de la información alojada en una base

	TECNOLOGÍAS DE LA INFORMACIÓN	Código
	ENTREGA, SERVICIO Y SOPORTE DE TI	A01-SO-02-UI.MAN01
	GESTIÓN DE LOS SERVICIOS DE SEGURIDAD	Versión No. 01
	MANUAL DE SEGURIDAD INFORMÁTICA	Página 5 de 16

de datos, servidor y/o computadora personal, almacenándola en un dispositivo de almacenamiento masivo como disco duro externo u otro dispositivo de red destinado para este fin, con el objetivo de realizar la recuperación de la información y evitar pérdidas de información críticas.

- **Bases de Datos:** (Database). Conjunto de datos relacionados que se almacenan de forma que se pueda acceder a ellos de manera sencilla, con la posibilidad de relacionarlos y ordenarlos en base a diferentes criterios, etc. Las bases de datos son uno de los grupos de aplicaciones de productividad personal más extendidos. Entre las más conocidas pueden citarse MySQL, Postgres, dBase, Paradox, Access y Aproach, Oracle, ADABAS, DB/2, Informix o Ingres, para sistemas medios y grandes.
- **Control de acceso:** Técnica usada para definir el uso de programas o limitar la obtención y almacenamiento de datos a una memoria. Una característica o técnica en un sistema de comunicaciones que permite o niega el uso de algunos componentes o algunas de sus funciones.
- **Equipo de telecomunicaciones:** Todo dispositivo capaz de transmitir y/o recibir señales digitales o analógicas para comunicación de voz, datos y video, ya sea individualmente o de forma conjunta.
- **Equipo de informática:** Dispositivo con la capacidad de aceptar y procesar información con base a programas establecidos o instrucciones previas, teniendo la oportunidad de conectarse a una red de equipos o computadoras para compartir datos y recursos, entregando resultados mediante despliegues visuales, impresos o audibles.
- **Enrutador:** Es un dispositivo que proporciona conectividad a nivel de red. Su función principal consiste en enviar o encaminar paquetes de datos de una red a otra, es decir, interconectar subredes, entendiéndose por subred un conjunto de máquinas IP que se pueden comunicar sin la intervención de un enrutador y que por tanto tiene prefijos de red distintos.
- **Firewall (cortafuegos):** Sistema colocado entre una red local e internet que asegura dicha red local y mantiene a los usuarios no autorizados fuera de la misma. Firewall en un sistema operativo, es un programa especializado en resguardar la información


	TECNOLOGÍAS DE LA INFORMACIÓN	Código
	ENTREGA, SERVICIO Y SOPORTE DE TI	A01-SO-02-UI.MAN01
	GESTIÓN DE LOS SERVICIOS DE SEGURIDAD	Versión No. 01
	MANUAL DE SEGURIDAD INFORMÁTICA	Página 6 de 16

que se aloja en la computadora local de cualquier acceso remoto de tipo malicioso o ataques informáticos.

- **Internet:** Es una convergencia de conceptos computacionales para presentar y enlazar información que se encuentra dispersa a través de páginas Web en una forma fácilmente accesible.
- **Programas Freeware:** Programas que se ofrecen al público sin ningún costo, pero que mantiene un copyright sobre ellos. Es decir se pueden usar sin problemas, pero no se pueden utilizar como parte de otros programas o modificarlos de ninguna manera.
- **Red informática:** Conjunto de ordenadores conectados directamente por cable, remotamente vía conmutadores de paquetes, o por otro procedimiento de comunicación.
- **Software de distribución gratuita:** Programas que se distribuyen a través de internet de forma gratuita.
- **Servidor:** Genéricamente, dispositivos de un sistema que resuelve las peticiones de otros elementos del sistema, denominados clientes. Computadora conectada a una red que pone sus recursos a disposición del resto de los integrantes de la red. Suele utilizarse para mantener datos centralizados o para gestionar recursos compartidos. Internet es en ultimo termino, un conjunto de servidores que proporcionan servicios de transferencias de ficheros, correo electrónico o páginas Web, entre otros.

5. SIGLAS

- **DNM:** Dirección Nacional de Medicamentos
- **UI:** Unidad de Informática

	TECNOLOGÍAS DE LA INFORMACIÓN	Código A01-SO-02-UI.MAN01
	ENTREGA, SERVICIO Y SOPORTE DE TI	
	GESTIÓN DE LOS SERVICIOS DE SEGURIDAD	Versión No. 01
	MANUAL DE SEGURIDAD INFORMÁTICA	Página 7 de 16

6. DESARROLLO O CONTENIDO

6.1 GENERALES

1. Cada una de las unidades organizativas de la DNM, deberá elaborar los planes de contingencia que correspondan a las actividades críticas que realicen a través de los sistemas de información.
2. Los presentes lineamientos deberán ser divulgados por la unidad de informática a través de la gerencia, a todo el personal involucrado que utilice equipos y programas informáticos.
3. La unidad de informática, podrá acceder a la información de un servidor público cuando se presuma alguna falta grave que amerite una sanción.
4. Cuando a un servidor público se le esté realizando un proceso de investigación por alguna falta o negligencia y este, para realizar sus funciones, requiera tener acceso a la información y a las operaciones que se realicen en la DNM, la Unidad de Informática podrá restringirle el acceso a los equipos informáticos de la dirección.


6.2 LINEAMIENTOS DE SEGURIDAD

La unidad de informática es la responsable de brindar servicio directo al usuario, en lo que respecta al equipamiento, instalación, actualización, cambio de lugar y programación informática, a fin de permitirle el uso de los equipos, de la infraestructura de red y servicios asociados a ellos, en forma eficaz y eficiente.

6.3 DEL EQUIPO

a) DE LA INSTALACION DE EQUIPOS INFORMATICA

1. Todo el equipo de informática (computadoras, estaciones de trabajo, accesorios y partes), que esté conectado a la red de la dirección aquel que en forma autónoma se tenga y sea propiedad de la dirección, deberá de sujetarse a las configuraciones de la red que se conectan.

	TECNOLOGÍAS DE LA INFORMACIÓN	Código A01-SO-02-UI.MAN01
	ENTREGA, SERVICIO Y SOPORTE DE TI	
	GESTIÓN DE LOS SERVICIOS DE SEGURIDAD	Versión No. 01
	MANUAL DE SEGURIDAD INFORMÁTICA	Página 8 de 16

2. La protección física y uso adecuado de los equipos es responsabilidad de quienes en un principio se les asigna.

b) DE LA ATENCION DE FALLAS O PROBLEMAS CON HARDWARE Y SOFTWARE


1. La atención de fallas o problemas menores de los equipos informáticos, se hará por vía telefónica o correo electrónico (atención inmediata y una solución a la falla detectada en hardware y software). Para los casos en que se tuviese que solicitar servicios de reparación o cambios de partes en los equipos y/o actualizaciones en hardware o software, se solicitara por escrito a la Unidad de Informática.
2. La unidad de informática atenderá las fallas o problemas de los equipos informáticos que estén o no con mantenimiento preventivo y correctivo, documentara la causa de la falla, emitirá un diagnóstico y dará las recomendaciones a los usuarios de las posibles soluciones para la rehabilitación o reparación de los equipos.
3. La atención de fallas o problemas podrá realizarse en el lugar de trabajo dependiendo del problema presentado y de la factibilidad para solucionarlo.

c) DEL MANTENIMIENTO DE EQUIPO DE INFORMATICA

1. La unidad de informática, coordinara y verificara que los servicios de mantenimiento preventivo y correctivo para los equipos de informática propiedad de la DNM, sean ejecutados según la orden de compra y contrato de servicio, por parte de la empresa contratada para que proporcione estos servicios.
2. Queda estrictamente prohibido dar mantenimiento preventivo y correctivo al equipo de informática que no es propiedad de la DNM.

d) DE LA ACTUALIZACION DEL EQUIPO

1. La unidad de informática, es la responsable de proponer a las máximas autoridades de la DNM la actualización de los equipos de informática y red.

	TECNOLOGÍAS DE LA INFORMACIÓN	Código
	ENTREGA, SERVICIO Y SOPORTE DE TI	A01-SO-02-UI.MAN01
	GESTIÓN DE LOS SERVICIOS DE SEGURIDAD	Versión No. 01
	MANUAL DE SEGURIDAD INFORMÁTICA	Página 9 de 16

2. Todo agregado o adhesión de repuestos incrementa la vida útil del equipo informático, debe de ser reportado al encargado de bienes muebles.

e) DE LA REUBICACION DEL EQUIPO DE INFORMATICA

1. En caso de existir, en las áreas organizativas, personal con conocimientos básicos en el área informática, la jefatura o dirección correspondiente deberá informar a la unidad de informática, los cambios o reubicaciones tanto de hardware como del software por escrito, en dicho documento se deberá agregar el nombre del encargado que realice el movimiento.
2. En caso de no existir dicho personal, la jefatura o dirección correspondiente deberá solicitar a la unidad informática, la realización de los cambios o reubicaciones tanto de hardware como del software.
3. Se deberá notificar a la unidad de informática, de los cambios o sustituciones del equipo inventariado (cambio de monitores, de impresores etc. Entre ambientes que se realicen), así como también si se cambiara de responsable del equipo.


6.4 DEL CONTROL DE ACCESOS

a) DEL ACCESO A LAS AREAS CRITICAS

1. La unidad de información, identificará las áreas críticas o de acceso restringido para el personal.
2. El jefe del área organizativa correspondiente, será el responsable de autorizar o no el ingreso de personal a las áreas consideradas críticas.

b) DEL CONTROL DE ACCESO AL EQUIPO DE INFORMATICA

1. El servidor público a quien se le asigne un equipo será el responsable de su custodia y buen uso del mismo y responderá a su extravío o daño no justificable.

	TECNOLOGÍAS DE LA INFORMACIÓN	Código
	ENTREGA, SERVICIO Y SOPORTE DE TI	A01-SO-02-UI.MAN01
	GESTIÓN DE LOS SERVICIOS DE SEGURIDAD	Versión No. 01
	MANUAL DE SEGURIDAD INFORMÁTICA	Página 10 de 16

2. Dada la naturaleza de los sistemas operativos y su conectividad en red, la Unidad de Informática, tiene la facultad de acceder a cualquier equipo de informática que esté conectado en la red aun cuando no esté bajo la responsabilidad de la sección.

c) DEL CONTROL DE ACCESO LOCAL A LA RED


1. La Unidad de Informática, es la responsable de proporcionar a los usuarios el acceso a los recursos informáticos que estén o no en red.
2. Dado el carácter unipersonal del acceso a la red, la unidad informática, verificara, a través de visitas periódicas a los usuarios, el uso responsable de los recursos informáticos que se comparten en la red.
3. El acceso a equipo especializado en informática (servidores, enrutadores, bases de datos, etc.) conectado a la red será administrado por la Unidad Informática.
4. Todo el equipo de informática que este o sea conectado a la red, o aquellos que en forma autónoma se tengan y que sean propiedad de la DNM, deberán sujetarse a los procedimientos de acceso que emita la Unidad de Informática.

d) DEL CONTROL DE ACCESO REMOTO

1. La Unidad de Informática, será la responsable de proporcionar los servicios de acceso a los recursos informáticos de la DNM, disponibles a través de la red.
2. Los usuarios de estos servicios deberán sujetarse a las configuraciones y especificaciones ya instaladas y no podrán hacer cambios a éstas.

e) DEL ACCESO A LOS SISTEMAS DE INFORMACION


1. La instalación y uso de los sistemas de información se regirán por lo establecido en la definición de políticas y procedimientos de controles generales en los sistemas de información de las normas técnicas de control interno específicas de la DNM.

	TECNOLOGÍAS DE LA INFORMACIÓN	Código A01-SO-02-UI.MAN01
	ENTREGA, SERVICIO Y SOPORTE DE TI	
	GESTIÓN DE LOS SERVICIOS DE SEGURIDAD	Versión No. 01
	MANUAL DE SEGURIDAD INFORMÁTICA	Página 11 de 16

2. El control de acceso a cada sistema de información será determinado por la jefatura de unidad responsable de generar y procesar los datos, sobre la base de los niveles de responsabilidad asignados a cada servidor público para su lugar de trabajo.
3. La creación de nuevas cuentas con acceso a los sistemas de información deberá ser solicitado vía correo electrónico o por escrito, esta solicitud deberá contener el nombre del servidor público, nivel de acceso a la información (solo consulta, ingreso, modificación de datos, etc.). unidad que solicita, firma y sello de jefe inmediato así como la autorización de la gerencia general.

f) DEL ACCESO A INTERNET

1. La dirección nacional, será el responsable de autorizar la información a publicar en el sitio Web Institucional.
2. La Unidad de informática, en coordinación con la Unidad de Publicidad y Comunicaciones, será la responsable de actualizar las veces que sea necesario hacerlo, la información que se publique en el sitio web institucional.
3. Los accesos a las páginas web a través de los equipos autorizados, deben utilizarse responsablemente y no descargar programas o información que pueda dañar a los programas y equipos propiedad de la DNM.
4. Los servicios de internet estarán sujetos a la disponibilidad en la infraestructura de red de datos en la DNM.
5. El servicio de internet no deberá utilizarse para navegar por páginas con información obscena o para enviar correos electrónicos que dañen la integridad moral de las personas. El mal uso del internet será sancionado con la suspensión del servicio. El tiempo de la sanción será determinado de acuerdo a lo estipulado en el reglamento interno de trabajo de la DNM.
6. Se proporcionará acceso a internet: a las autoridades y a las jefaturas de la DNM y a los que las jefaturas determinen que es necesario para su desarrollo laboral de igual forma la cuenta de correo institucional.

	TECNOLOGÍAS DE LA INFORMACIÓN	Código
	ENTREGA, SERVICIO Y SOPORTE DE TI	A01-SO-02-UI.MAN01
	GESTIÓN DE LOS SERVICIOS DE SEGURIDAD	Versión No. 01
	MANUAL DE SEGURIDAD INFORMÁTICA	Página 12 de 16

7. La unidad de informática, no se hará responsable por problemas externos de conectividad y comunicación por parte del proveedor del servicio, más sin embargo se comunicara con el proveedor para hacer el reclamo respectivo.


6.5 DE LA UTILIZACION DE RECURSOS DE REDES

1. Corresponde a la unidad de informática el administrar, mantener y actualizar la infraestructura de la red de la DNM.
2. Los recursos disponibles a través de la red, serán de uso exclusivo para asuntos relacionados con las actividades del puesto de trabajo y del lugar donde está asignado.

6.6 DEL SOFTWARE


a) DE LA ADQUISICION DE SOFTWARE

1. La unidad de informática, establecerá los mecanismos de sustitución de sistemas y programas informáticos.
2. Corresponderá a la unidad de informática, el proporcionar asesoría y apoyo a técnico para licenciamiento, cobertura, transferencia, certificación y vigencia de los programas informáticos.
3. La unidad de informática, será encargada de recomendar la adquisición de programas informáticos de vanguardia, de acuerdo a lo estipulado en los lineamientos sobre especificaciones técnicas para la adquisición de equipos y programas de informática de la DNM.
4. La unidad informática, será la encargada de asesor y apoyar técnicamente para mantener actualizado los estándares de configuración de los sistemas operativos, programas comerciales, base de datos y comunicación.
5. Para la adquisición de nuevas licencias o actualizaciones de sistemas operativos, programas comerciales, base de datos y comunicaciones, equipos, accesorios y repuestos informáticos, será la unidad de informática quien proporcione la asesoría y opinión técnica, además de autorizar la adquisición de lo descrito anteriormente.

	TECNOLOGÍAS DE LA INFORMACIÓN	Código A01-SO-02-UI.MAN01
	ENTREGA, SERVICIO Y SOPORTE DE TI	
	GESTIÓN DE LOS SERVICIOS DE SEGURIDAD	Versión No. 01
	MANUAL DE SEGURIDAD INFORMÁTICA	Página 13 de 16

b) DE LA INSTALACION DE SOFTWARE.

1. Corresponde a la unidad de informática, la instalación y supervisión del software básico para cualquier tipo de equipo informático.
2. La unidad de informática, es la responsable de brindar asesoría y supervisión para la instalación de software informático y de telecomunicaciones.
3. La unida de informática, será responsable de que en los equipos de informática, de telecomunicaciones y en dispositivos basados en sistemas informáticos, únicamente se instalen software con licenciamiento propiedad de la DNM y acorde a los derechos que la licencia delimite.
4. La instalación y uso de paquetes y programas informáticos gratuitos (freeware) o sin costo alguno para la DNM, será autorizado por la unidad de informática, respetando la ley de propiedad intelectual.
5. La unidad de informática, proporcionara asesoría y apoyo técnico por medio de la instalación de versiones actualizadas, que ayuden a solventar problemas detectados o modificaciones que contribuyen a mejorar la utilización de los equipos informáticos para las unidades.
6. Se prohíbe la instalación de programas que no posean su licencia de software, juegos u otro programa informático que no tengan relación con las funciones y actividades que el servidor público desempeñe en su lugar de trabajo. La unidad de informática, monitoreara su cumplimiento.
7. Es prohibida la instalación de software que pudiera poner en riesgo los recursos o la información de la Dirección. El no cumplimiento de este numeral será sancionado de acuerdo al reglamento interno de trabajo vigente.
8. Para proteger la integridad de los sistemas informáticos y de telecomunicaciones, es imprescindible que todos y cada uno de los equipos involucrados dispongan como mínimo de software de seguridad (antivirus, vacunas, firewall software, etc.), u otros.
9. Que aplique y que tenga relación con las funciones y actividades que el servidor público desempeñe en su lugar de trabajo.

	TECNOLOGÍAS DE LA INFORMACIÓN	Código A01-SO-02-UI.MAN01
	ENTREGA, SERVICIO Y SOPORTE DE TI	
	GESTIÓN DE LOS SERVICIOS DE SEGURIDAD	Versión No. 01
	MANUAL DE SEGURIDAD INFORMÁTICA	Página 14 de 16


10. La protección y manejo de los sistemas y programas informáticos, corresponde a las personas o grupos que se les asigna y les compete notificar cualquier problema de estos a su jefe inmediato superior, quien deberá informar a la unidad de informática para proporcionar una solución oportuna a dicho problema.

c) DE LA ACTUALIZACION DE SOFTWARE

1. Corresponde a la Gerencia General a través de la unidad de informática autorizar cualquier adquisición y actualización de software.
2. Las actualizaciones del software de uso común lo llevara a cabo la unidad de informática, y se hará de acuerdo a las necesidades institucionales.


d) DE LA AUDITORIA DE SOFTWARE INSTALADO

1. La unidad de informática, será la responsable de realizar la auditoria de software instalado.
2. La unidad de informática, realizara, al menos dos veces al año, revisiones de los equipos informáticos, para asegurar que los programas instalados, en caso de necesitar licencia, cuenten con una licencia vigente.
3. Los servidores públicos, cuyas computadoras cuenten con software instalado de versión de prueba, en caso de necesitar licencia valida, deberá presentar la necesidad y justificación para adquisición del software a la unidad de informática a través de la Gerencia General.

	TECNOLOGÍAS DE LA INFORMACIÓN	Código A01-SO-02-UI.MAN01
	ENTREGA, SERVICIO Y SOPORTE DE TI	
	GESTIÓN DE LOS SERVICIOS DE SEGURIDAD	Versión No. 01
	MANUAL DE SEGURIDAD INFORMÁTICA	Página 15 de 16

e) DEL SOFTWARE PROPIEDAD DE LA INSTITUCION

1. Todo programa adquirido por la Dirección sea por compra, donación o cesión, es propiedad de la Dirección y mantendrá los derechos que la ley de propiedad Intelectual le confiera.
2. Todos los programas, bases de datos, sistemas operativos, interfaces, desarrollados a través de los recursos de la DNM, se mantendrán como propiedad de la Dirección respetando la propiedad intelectual del mismo.
3. El software disponible en cada equipo informático es propiedad de la DNM, quedando prohibida su distribución y reproducción.
4. Los códigos fuentes de los sistemas de información, deberán estar en la unidad de informática para efectos de custodia y control.
5. La unidad de informática, en coordinación con la unidad de control de Bienes Muebles, a través del sistema de inventario de la DNM, podrá verificar el registro de las licencias, sistemas y programas informáticos propiedad de la DNM.
6. Es obligación de todos los usuarios que manejen información, mantener el respaldo correspondiente de la misma, ya que se considerara como un activo de la DNM que debe preservarse.
7. Corresponderá a la DNM, el promover y difundir los mecanismos para realizar el respaldo de los datos y los sistemas de información existente, de acuerdo a las políticas para la ejecución de backup y recuperación de información, según lo estipulado en las políticas y procedimientos de los Controles Generales de los Sistemas de Información de las Normas Técnicas de Control Interno Especificas de la DNM.
8. Los datos, las bases de datos, la información generada por el personal y los recursos informáticos de la Dirección deberán estar debidamente resguardados.

	TECNOLOGÍAS DE LA INFORMACIÓN	Código A01-SO-02-UI.MAN01
	ENTREGA, SERVICIO Y SOPORTE DE TI	
	GESTIÓN DE LOS SERVICIOS DE SEGURIDAD	Versión No. 01
	MANUAL DE SEGURIDAD INFORMÁTICA	Página 16 de 16

6.7 DE LA SUPERVISION Y EVALUACION

1. Es responsabilidad de la unidad de informática, la supervisión y evaluación de los sistemas de información que involucren aspectos de seguridad lógica y física, las cuales deberá realizarse cada año.
2. Los sistemas de información institucional deben estar bajo monitoreo y actualización permanente.