



GOBIERNO DE  
**MÉXICO**

**SALUD**  
SECRETARÍA DE SALUD

**SECRETARÍA DE SALUD  
SUBSECRETARÍA DE PREVENCIÓN Y  
PROMOCIÓN DE LA SALUD  
DIRECCIÓN GENERAL DE INFORMACIÓN EN SALUD**

---

**GIIS-A004-01-07**

**GUÍA PARA EL INTERCAMBIO DE  
INFORMACIÓN EN SALUD PARA UN  
SISTEMA DE GESTIÓN DE SEGURIDAD  
DE LA INFORMACIÓN (SGSI) EN SALUD**



|                                                                                                                                                                   |                                                                          |                                        |                                                    |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------|----------------------------------------|----------------------------------------------------|
|  <b>GOBIERNO DE MÉXICO</b><br><b>SALUD</b><br><small>SECRETARÍA DE SALUD</small> | <b>GUÍA DE INTERCAMBIO DE INFORMACIÓN EN SALUD PARA UN SGSI EN SALUD</b> |                                        |                                                    |
|                                                                                                                                                                   | <b>CLAVE DEL DOCUMENTO:</b><br>GIIS-A004-01-07                           | <b>VERSIÓN DEL DOCUMENTO:</b><br>01.07 | <b>FECHA DEL DOCUMENTO:</b><br>07 de junio de 2013 |

## PREFACIO

### Información de contacto

Para más información sobre el documento que se muestra a continuación, favor de contactar a la Dirección General de Información en Salud, ubicada en Homero No. 213, Piso 2, Col. Chapultepec Morales, Alcaldía Miguel Hidalgo, C.P. 11570, Ciudad de México, México; Teléfono. +52 (55) 6392 2300, Ext. 52584, o bien, por medio de correo electrónico a [dgis@salud.gob.mx](mailto:dgis@salud.gob.mx) con el asunto “GUÍAS DE INTERCAMBIO DE INFORMACIÓN”.

### Historial de revisiones

| Fecha      | Versión | Madurez          | Descripción                 | Autor          |
|------------|---------|------------------|-----------------------------|----------------|
| 29/04/2013 | 01      | Borrador interno | Creación del documento      | SAOO           |
| 15/05/2013 | 02      | Borrador interno | Revisión del documento      | ECJ            |
| 29/05/2013 | 03      | Borrador interno | Corrección del documento    | SAOO, PCF      |
| 30/05/2013 | 04      | Borrador Oficial | Revisión del documento      | ECJ, PCF, AHMA |
| 05/06/2013 | 05      | Borrador Oficial | Corrección del documento    | SSA            |
| 06/06/2013 | 06      | Borrador Oficial | Revisión del documento      | SAOO           |
| 07/06/2013 | 07      | Oficial          | Versión final del documento | SAOO, ECJ      |

### Participantes

| Institución, dependencia u organismo       | Nombre y Cargo                                                                    | Iniciales |
|--------------------------------------------|-----------------------------------------------------------------------------------|-----------|
| Dirección General de Información en Salud  | Ana Hilda Morales Aranda, Directora de Proyectos                                  | AHMA      |
|                                            | Sergio Arturo Ortiz Orcasas, Jefe del Departamento de Seguridad de la Información | SAOO      |
|                                            | Efraín Cruz Jiménez, Subdirector de Proyectos Electrónicos en Salud               | ECJ       |
|                                            | Pablo Corona Fraga                                                                | PCF       |
|                                            | Salvador Sánchez Abarca                                                           | SSA       |
| Normalización y Certificación Electrónica. | Pablo Corona Fraga                                                                | PCF       |
|                                            | Salvador Sánchez Abarca                                                           | SSA       |



## CONTENIDO

|                                                             |    |
|-------------------------------------------------------------|----|
| Prefacio                                                    | 2  |
| Información de contacto                                     | 2  |
| Historial de revisiones                                     | 2  |
| Participantes                                               | 2  |
| Contenido                                                   | 3  |
| Presentación de la Guía                                     | 5  |
| Introducción                                                | 5  |
| Audiencia                                                   | 5  |
| Alcance                                                     | 6  |
| Justificación                                               | 6  |
| Términos y Definiciones                                     | 7  |
| Referencias                                                 | 9  |
| Ligas Web                                                   | 9  |
| Bibliografía                                                | 9  |
| Archivos anexos                                             | 9  |
| SEGURIDAD DE LA INFORMACION EN SALUD                        | 10 |
| SISTEMA DE GESTIÓN                                          | 10 |
| VERIFICACIÓN DE APEGO A ESTA GUÍA Y FORMATOS                | 11 |
| Planeación del SGSI                                         | 11 |
| Implementación y operación del SGSI                         | 14 |
| Supervisión y revisión del SGSI                             | 15 |
| Mantenimiento y mejora del SGSI                             | 16 |
| CONTROLES DE SEGURIDAD                                      | 18 |
| 1. POLÍTICA DE SEGURIDAD                                    | 18 |
| 1.1. Política de Seguridad de la Información                | 18 |
| 2. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN | 19 |
| 2.1. Organización interna                                   | 19 |
| 2.2. Terceros                                               | 21 |
| 3. GESTIÓN DE ACTIVOS                                       | 23 |
| 3.1. Responsabilidad sobre los activos de Salud             | 23 |
| 3.2. Clasificación de la información de salud               | 24 |
| 4. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS                  | 24 |
| 4.1. Antes del empleo                                       | 24 |
| 4.2. Durante el empleo                                      | 25 |
| 4.3. Cese del empleo o cambio de puesto de trabajo          | 26 |





|       |                                                                                        |    |
|-------|----------------------------------------------------------------------------------------|----|
| 5.    | SEGURIDAD FÍSICA Y DEL ENTORNO                                                         | 27 |
| 5.1.  | Áreas seguras                                                                          | 27 |
| 5.2.  | Seguridad de los equipos                                                               | 29 |
| 6.    | GESTIÓN DE COMUNICACIONES Y OPERACIONES                                                | 30 |
| 6.1.  | Responsabilidades y procedimientos de operación                                        | 30 |
| 6.2.  | Gestión de la provisión de servicios por terceros                                      | 31 |
| 6.3.  | Planificación y aceptación del sistema                                                 | 32 |
| 6.4.  | Protección contra el código malicioso y descargable                                    | 33 |
| 6.5.  | Copia de seguridad de información de salud                                             | 33 |
| 6.6.  | Gestión de la seguridad de las redes                                                   | 34 |
| 6.7.  | Manipulación de los medios                                                             | 34 |
| 6.8.  | Intercambio de información                                                             | 35 |
| 6.9.  | Servicios de comercio electrónico en salud                                             | 36 |
| 6.10. | Supervisión                                                                            | 37 |
| 7.    | CONTROL DE ACCESO                                                                      | 38 |
| 7.1.  | Requisitos de control de acceso en salud                                               | 38 |
| 7.2.  | Gestión de acceso de usuario                                                           | 39 |
| 7.3.  | Responsabilidades de usuario                                                           | 41 |
| 7.4.  | Control de acceso a la red                                                             | 41 |
| 7.5.  | Control de acceso al sistema operativo                                                 | 42 |
| 7.6.  | Control de acceso a las aplicaciones y a la información                                | 43 |
| 7.7.  | Equipos de cómputo portátil y teletrabajo                                              | 44 |
| 8.    | ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN                     | 45 |
| 8.1.  | Requisitos de seguridad de los sistemas de información                                 | 45 |
| 8.2.  | Procesamiento correcto en aplicaciones                                                 | 45 |
| 8.3.  | Controles criptográficos                                                               | 47 |
| 8.4.  | Seguridad de los archivos de sistema                                                   | 47 |
| 8.5.  | Seguridad en los procesos de desarrollo y soporte                                      | 48 |
| 8.6.  | Gestión de las vulnerabilidades técnicas                                               | 48 |
| 9.    | GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN                                | 49 |
| 9.1.  | Notificación de eventos y puntos débiles de seguridad de la información                | 49 |
| 9.2.  | Gestión de incidentes y mejoras de seguridad de la información                         | 49 |
| 10.   | GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO                                                  | 50 |
| 10.1. | Aspectos de la Seguridad de la Información en la Gestión de la Continuidad del Negocio | 50 |
| 11.   | CUMPLIMIENTO                                                                           | 52 |
| 11.1. | Cumplimiento de los requisitos legales                                                 | 52 |
| 11.2. | Cumplimiento de las políticas y normas de seguridad y cumplimiento técnico             | 53 |
| 11.3. | Consideraciones sobre las auditorías de los sistemas de información de salud           | 54 |



|                                                                                                                                                                  |                                                                   |                                 |                                             |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------|---------------------------------|---------------------------------------------|
|  <b>GOBIERNO DE MÉXICO</b>   <b>SALUD</b><br><small>SECRETARÍA DE SALUD</small> | GUÍA DE INTERCAMBIO DE INFORMACIÓN EN SALUD PARA UN SGSI EN SALUD |                                 |                                             |
|                                                                                                                                                                  | CLAVE DEL DOCUMENTO:<br>GIIS-A004-01-07                           | VERSIÓN DEL DOCUMENTO:<br>01.07 | FECHA DEL DOCUMENTO:<br>07 de junio de 2013 |

## PRESENTACIÓN DE LA GUÍA

---

### Introducción

La necesidad de la gestión eficaz de las Tecnologías de la Información en el cuidado de la salud se hace cada vez más urgente por el incremento de su uso en la prestación de servicios de salud. Si no se implementan apropiadamente, estas complejas tecnologías incrementarían los riesgos de la confidencialidad, integridad y disponibilidad de la información. Independientemente del tamaño, ubicación y modelo de la entrega del servicio, todas las organizaciones de salud necesitan tener estrictos controles implementados para proteger la información de salud que se les ha confiado, aun cuando muchos profesionales de la salud trabajan como proveedores independientes de salud o en clínicas pequeñas que carecen de recursos tecnológicos dedicados a gestionar la seguridad de la información. Las organizaciones de salud además deben tener una guía específica, clara y concisa sobre la implementación de esos controles.

Finalmente, con el incremento del intercambio electrónico de información de salud entre profesionales de la salud, hay un claro beneficio en la adopción de un marco de referencia común para la gestión de seguridad en el cuidado de la salud, por ello el presente documento se adapta a un amplio rango de tamaños, ubicaciones y modelos de la prestación de servicios de salud.

Autoridades del sector salud nacional o regional como Australia, Canadá, Francia, Holanda, Nueva Zelanda, África del Sur y Reino Unido utilizan ampliamente los Sistemas de Gestión de Seguridad de la información en materia de salud.

La presente guía está basada en la norma internacional ISO 27799, misma que retoma la norma internacional ISO/IEC 27002, la cual considera el uso de controles de seguridad con el propósito de proteger la información personal de salud.

### Audiencia

Esta guía está dirigida al personal designado por los Prestadores de Servicios de Salud responsable de asegurar la implantación del Sistema de Gestión de la Seguridad de la Información en su organización y que se lleven a cabo revisiones al mismo, a fin de verificar su cumplimiento.



|                                                                                                             |                                                                          |                                             |                                 |
|-------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------|---------------------------------------------|---------------------------------|
|  <b>GOBIERNO DE MÉXICO</b> | <b>GUÍA DE INTERCAMBIO DE INFORMACIÓN EN SALUD PARA UN SGSI EN SALUD</b> |                                             |                                 |
|                                                                                                             | <b>SALUD</b><br><small>SECRETARÍA DE SALUD</small>                       | CLAVE DEL DOCUMENTO:<br>GIIS-A004-01-07     | VERSIÓN DEL DOCUMENTO:<br>01.07 |
|                                                                                                             |                                                                          | FECHA DEL DOCUMENTO:<br>07 de junio de 2013 |                                 |

## Alcance

Esta guía es de uso obligatorio para todos aquellos Prestadores de Servicios de Salud del sector público, privado y social, custodios de información en salud que utilicen Sistemas de Información de Registro Electrónico para la Salud (SIRES).

Es posible para un Prestador de Servicios de Salud estar certificado bajo la norma ISO/IEC 27001 sin requerir la Evaluación de la Conformidad de los requisitos de esta Guía, siempre y cuando el alcance del SGSI certificado cubra la implantación del SIRES en el Prestador de Servicios de Salud.

## Justificación

El marco legal que justifica la obligación por parte de los Prestadores de Servicios de Salud de Implementar un Sistema de Gestión de Seguridad de la Información es:

- NOM-024-SSA3-2012, Sistemas de información de registro electrónico para la salud. Intercambio de información en salud.
- LFTAIPG, Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental.
- LFPDPPP, Ley Federal de Protección de Datos Personales en Posesión de los Particulares.
- Ley General de Salud.
- NOM-004-SSA2-2012, Del expediente clínico
- MAAGTIC-SI, Manual Administrativo de Aplicación General en Materia de Tecnologías de la Información y Comunicaciones y Seguridad de la Información.



## Términos y Definiciones

| Término                             | Acrónimo   | Definición                                                                                                                                                                                                                                                                                                                   |
|-------------------------------------|------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Activo</b>                       |            | Es cualquier cosa que tiene valor para la organización. Existe muchos tipos de activos, incluyendo: Información; Software, como un programa informático; Físicos, como una computadora; Servicios; Personas y sus cualidades, habilidades y experiencia; e Intangibles, como la reputación e imagen.                         |
| <b>Amenaza</b>                      |            | Una causa potencial de un incidente no deseado, la cual puede resultar en daños a un sistema u organización.                                                                                                                                                                                                                 |
| <b>Control</b>                      |            | Significa gestionar el riesgo, incluyendo políticas, procedimientos directrices, prácticas o estructuras organizacionales, las cuales pueden ser de carácter administrativo, técnico, de gestión o legal.                                                                                                                    |
| <b>Declaración de Aplicabilidad</b> | <b>DDA</b> | Se refiere al documento anexo a la presente guía, en el que el Prestador de Servicios de Salud establece y justifica aquellos controles de seguridad que le aplican y aquellos que no para la implementación del SGSI en su organización.                                                                                    |
| <b>Dirección</b>                    |            | Persona o grupo de personas en el más alto nivel dentro de una organización. Se refiere a la gente que coordina, dirige y controla la organización.                                                                                                                                                                          |
| <b>Dominio</b>                      |            | Áreas funcionales del sistema de gestión de seguridad de la información.                                                                                                                                                                                                                                                     |
| <b>ECE</b>                          |            | Expediente Clínico Electrónico                                                                                                                                                                                                                                                                                               |
| <b>Evidencia</b>                    |            | Información que muestra o prueba que algo existe o es verdadero. Puede ser colectada por medio de observación directa, mediciones o uso de métodos específicos.                                                                                                                                                              |
| <b>FGSI</b>                         |            | Foro de Gestión de Seguridad de la Información                                                                                                                                                                                                                                                                               |
| <b>Impacto</b>                      |            | Medida de la criticidad sobre el negocio derivada por un cambio o incidente.                                                                                                                                                                                                                                                 |
| <b>ISO</b>                          |            | Organización Internacional de Normalización por sus siglas en inglés (International Organization for Standardization)                                                                                                                                                                                                        |
| <b>MAAGTIC-SI</b>                   |            | Manual Administrativo de Aplicación General en Materia de Tecnologías de la Información y Comunicaciones y Seguridad de la Información.                                                                                                                                                                                      |
| <b>Propietario</b>                  |            | Se refiere a un individuo o una entidad al que se le ha asignado la responsabilidad administrativa para el control de la producción, el desarrollo, el mantenimiento, el uso y la seguridad de los activos. El término "propietario" no significa que la persona tenga realmente algún derecho de propiedad sobre el activo. |



| Término                | Acrónimo     | Definición                                                                                                                           |
|------------------------|--------------|--------------------------------------------------------------------------------------------------------------------------------------|
| <b>Riesgo</b>          |              | El riesgo remanente después del tratamiento del riesgo original.                                                                     |
| <b>Riesgo residual</b> |              | Es aquel riesgo que prevalece o resulta aun cuando se tomaron acciones para manejar el riesgo original.                              |
| <b>Routing</b>         |              | Proceso de selección de rutas dentro de una red a través de las cuales se envía información. Traducido al español como enrutamiento. |
| <b>SGSI</b>            |              | Sistema de Gestión de Seguridad de la Información.                                                                                   |
| <b>SIRES</b>           | <b>SIRES</b> | Sistemas de Información de Registro Electrónico para la Salud.                                                                       |
| <b>Vulnerabilidad</b>  |              | Es la debilidad de un activo o grupo de activos que pueden ser explotados por una o más amenazas.                                    |





## REFERENCIAS

### Ligas Web

<http://www.27000.org/iso-27799.htm>

<http://www.27000.org/>

<http://www.iso27000.es/>

<http://www.iso27002.es/>

### Bibliografía

ISO 27799, Health Informatics – Information security management in health using ISO/IEC 27002.

NMX-I-27001-NYCE, Tecnologías de la Información – Sistema de Gestión de Seguridad de la Información.

NMX-I-27002-NYCE, Tecnologías de la Información – Códigos de buenas Prácticas para la gestión de la Seguridad de la Información.

NMX-I-27005-NYCE, Tecnologías de la Información – Gestión del Riesgo en Seguridad de la Información.

### Archivos anexos

| Id. | Nombre del archivo                                                     | Descripción                       | Formato / Aplicación para su visualización |
|-----|------------------------------------------------------------------------|-----------------------------------|--------------------------------------------|
| 1   | Declaración de Aplicabilidad (DDA)                                     | GIIS-A004-SGSI-01-07-Anexo-A.xlsx | Hoja de Calculo                            |
| 2   | Anexo de Lineamientos para la implementación de controles de seguridad | GIIS-A004-SGSI-01-07-Anexo-B.pdf  | Adobe Acrobat Reader                       |





## SEGURIDAD DE LA INFORMACION EN SALUD

Esta guía está basada en la Norma Internacional ISO 27799 que proporciona los lineamientos sobre cómo asegurar la confidencialidad, integridad y disponibilidad de la información mediante la implementación de un Sistema de Gestión de Seguridad de la Información, la cual aborda las necesidades de gestión de seguridad de la información sobre el sector salud y sus ambientes de operación, de conformidad con el numeral 6.6 de la Norma Oficial Mexicana NOM-024-SSA3-2012, el cual se refiere a las consideraciones universales de manejo y seguridad de la información.

## SISTEMA DE GESTIÓN

Una organización tiene que definir y gestionar numerosas actividades para funcionar con eficacia. Cualquier actividad que utiliza recursos y se gestiona de modo que permite la transformación de unos elementos de “entrada” en unos elementos de “salida” puede considerarse un proceso. A menudo, la salida de un proceso se convierte directamente en la entrada del proceso siguiente.

El modelo “Planificar – Hacer – Verificar – Actuar” (Plan – Do – Check – Act, conocido como modelo PDCA), se aplica para estructurar todos los procesos del SGSI. La figura 1 muestra cómo un SGSI, partiendo de los requisitos y expectativas de seguridad de la información de las partes interesadas y a través de las acciones y procesos necesarios, produce los elementos de salida de seguridad de la información que responden a dichos requisitos y expectativas.

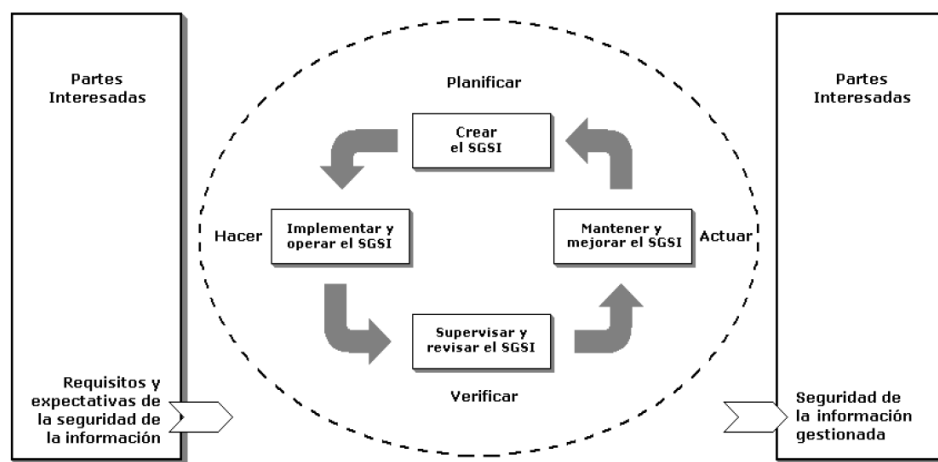


FIGURA 1.- Modelo PDCA aplicado a los procesos del SGSI

|                                                    |                                                                                                                                                                                                                                                       |
|----------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Planificar (creación del SGSI)</b>              | Definir la política, objetivos, procesos y procedimientos del SGSI relevantes para gestionar el riesgo y mejorar la seguridad de la información, con el fin de obtener resultados acordes con las políticas y objetivos generales de la organización. |
| <b>Hacer (implementación y operación del SGSI)</b> | Implementar y operar la política, controles, procesos y procedimientos del SGSI.                                                                                                                                                                      |
| <b>Verificar (suspensión y revisión del SGSI)</b>  | Evaluar y, en su caso, medir el rendimiento del proceso contra la política, los objetivos y la experiencia práctica del SGSI, e informar de los resultados a la Dirección para su revisión.                                                           |
| <b>Actuar (mantenimiento y mejora del SGSI)</b>    | Adoptar medidas correctivas y preventivas, en función de los resultados de la auditoría interna del SGSI y de la revisión por parte de la Dirección, o de otras informaciones relevantes, para lograr la mejora continua del SGSI.                    |

De acuerdo con el PDCA, la organización debe crear, implementar, operar, supervisar, revisar, mantener y mejorar un SGSI documentado dentro del contexto de las actividades generales de la organización y de los riesgos que ésta afronta. Para efectos de esta Guía, el proceso utilizado se basa en el modelo PDCA descrito en la figura 1.

## VERIFICACIÓN DE APEGO A ESTA GUÍA Y FORMATOS

Para cumplir con la presente Guía referente a los requerimientos de Sistema de Gestión de la Seguridad, el prestador de servicios de salud deberá observar lo establecido en esta sección.

Todos aquellos enunciados y sus respectivos numerales redactados a continuación, en los que se incluyan las palabras; debe, deben, y/o deberán, el personal responsable de asegurar la implementación de un SGSI dentro de la organización del Prestador de Servicios de Salud deberá interpretarlo como un requisito y a su vez, un elemento a evaluar durante la verificación de apego a esta Guía.

### Planeación del SGSI

La organización debe hacer lo siguiente:

- Definir el alcance y los límites del SGSI en términos de las características de la actividad de la organización, su ubicación, sus activos y tecnología, incluyendo los detalles y la justificación de cualquier exclusión del alcance;



|                                                                                                                                                                  |                                                                          |                                        |                                                    |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------|----------------------------------------|----------------------------------------------------|
|  <b>GOBIERNO DE MÉXICO</b>   <b>SALUD</b><br><small>SECRETARÍA DE SALUD</small> | <b>GUÍA DE INTERCAMBIO DE INFORMACIÓN EN SALUD PARA UN SGSI EN SALUD</b> |                                        |                                                    |
|                                                                                                                                                                  | <b>CLAVE DEL DOCUMENTO:</b><br>GIIIS-A004-01-07                          | <b>VERSIÓN DEL DOCUMENTO:</b><br>01.07 | <b>FECHA DEL DOCUMENTO:</b><br>07 de junio de 2013 |

b) Definir una política del SGSI acorde con las características de la actividad de la organización, su ubicación sus activos y tecnología, que:

- 1) Incluya un marco para la fijación de objetivos y establezca una orientación general sobre las directrices y principios de actuación en relación con la seguridad de la información;
- 2) Tenga en cuenta los requisitos de la actividad de la organización, los requisitos legales o reglamentarios y las obligaciones de seguridad contractuales;
- 3) Esté alineada con el contexto de la estrategia de gestión de riesgos de la organización contexto en el que tendrá lugar la creación y el mantenimiento del SGSI;
- 4) Establezca criterios de estimación del riesgo; y
- 5) Sea aprobada por la Dirección.

c) Definir el enfoque de la evaluación de riesgos de la organización:

- 1) Especificar una metodología de evaluación de riesgos adecuada para el SGSI, las necesidades de negocio identificadas en materia de seguridad de la información de la organización y los requisitos legales y reglamentarios;
- 2) Desarrollar criterios de aceptación de riesgo y fijar los niveles de riesgo aceptables.

La metodología seleccionada para la evaluación de riesgos debe asegurar que las evaluaciones de riesgos generen resultados comparables y reproducibles.

**NOTA:** Hay diferentes metodologías para la evaluación de riesgos. En la NMX-I-27005-NYCE, se encuentran ejemplos de metodologías para la evaluación de riesgos.

d) Identificar los riesgos;

- 1) Identificar los activos que están dentro del ámbito de aplicación del SGSI y a los propietarios de estos activos;
- 2) Identificar las amenazas a que están expuestos esos activos;
- 3) Identificar las vulnerabilidades bajo las que podrían actuar dichas amenazas;
- 4) Identificar los impactos que sobre los activos puede tener una pérdida de confidencialidad, integridad y disponibilidad en los mismos.



|                                                                                                                                                                  |                                                                          |                                 |                                             |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------|---------------------------------|---------------------------------------------|
|  <b>GOBIERNO DE MÉXICO</b>   <b>SALUD</b><br><small>SECRETARÍA DE SALUD</small> | <b>GUIA DE INTERCAMBIO DE INFORMACIÓN EN SALUD PARA UN SGSI EN SALUD</b> |                                 |                                             |
|                                                                                                                                                                  | CLAVE DEL DOCUMENTO:<br>GIIIS-A004-01-07                                 | VERSIÓN DEL DOCUMENTO:<br>01.07 | FECHA DEL DOCUMENTO:<br>07 de junio de 2013 |

e) Analizar y valorar los riesgos;

- 1) Evaluar los efectos en la actividad de la organización que pudieran derivarse de eventuales fallos de seguridad, teniendo en cuenta las consecuencias de una pérdida de confidencialidad, integridad o disponibilidad de los activos;
- 2) Evaluar la probabilidad, de una forma realista, de que se produzcan fallos de seguridad a luz de las amenazas y vulnerabilidades existentes, los impactos asociados a los activos y los controles implementados;
- 3) Estimar los niveles de riesgo;
- 4) Determinar si los riesgos son aceptables o si requieren un tratamiento conforme a los criterios de aceptación de riesgos establecidos por la organización.

f) Identificar y evaluar las opciones para el tratamiento de riesgos. Las posibles acciones a realizar, entre otras, son las siguientes:

- 1) Aplicar controles adecuados;
  - 2) Asumir los riesgos de manera consistente y objetiva, conforme a las políticas de la organización y a los criterios de aceptación de riesgos;
  - 3) Evitar los riesgos; y
  - 4) Transferir los riesgos asociados a la actividad de la organización a otras partes, como por ejemplo compañías de seguros y proveedores.
- g) Seleccionar los objetivos de control y los controles para el tratamiento de los riesgos. Los objetivos de control y los controles deben seleccionarse e implementarse para cumplir los requisitos identificados en la evaluación de riesgos y en el proceso de tratamiento de riesgos. Esta selección debe tener en cuenta los criterios de aceptación de riesgos, además de los requisitos legales, reglamentarios y contractuales.

Los objetivos de control y los controles de la sección “Controles de Seguridad” de la presente guía, deben seleccionarse como parte de este proceso en la medida en que sirvan para satisfacer los requisitos identificados.

Los objetivos de control y los controles enumerados en la sección “Controles de Seguridad” no son exhaustivos, por lo que pueden seleccionarse otros objetivos de control y otros controles adicionales.



|                                                                                                                                                                  |                                                                          |                                        |                                                    |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------|----------------------------------------|----------------------------------------------------|
|  <b>GOBIERNO DE MÉXICO</b>   <b>SALUD</b><br><small>SECRETARÍA DE SALUD</small> | <b>GUÍA DE INTERCAMBIO DE INFORMACIÓN EN SALUD PARA UN SGSI EN SALUD</b> |                                        |                                                    |
|                                                                                                                                                                  | <b>CLAVE DEL DOCUMENTO:</b><br>GIIIS-A004-01-07                          | <b>VERSIÓN DEL DOCUMENTO:</b><br>01.07 | <b>FECHA DEL DOCUMENTO:</b><br>07 de junio de 2013 |

- h) Obtener la aprobación, por parte de la Dirección, de los riesgos residuales propuestos;
- i) Obtener la autorización de la Dirección para implementar y operar el SGSI;
- j) Elaborar una declaración de aplicabilidad (DDA).

Una DDA debe incluir lo siguiente:

- 1) Los objetivos de control, los controles seleccionados y las justificaciones de su selección;
- 2) Los objetivos de control y los controles actualmente implementados o por implementar; y
- 3) Los objetivos de control, los controles excluidos y la justificación de su exclusión.

**NOTA:** La declaración de aplicabilidad proporciona un resumen de las decisiones relativas al tratamiento de los riesgos. La justificación de las exclusiones facilita una comprobación cruzada de que no se ha omitido inadvertidamente ningún control.

## Implementación y operación del SGSI

La organización debe:

- a) Formular un plan de tratamiento de riesgos que identifique las acciones de la Dirección, los recursos, las responsabilidades y las prioridades adecuadas para gestionar los riesgos de la seguridad de la información;
- b) Implementar el plan de tratamiento de riesgos para lograr los objetivos de control identificados, que tenga en cuenta la financiación y la asignación de funciones y responsabilidades;
- c) Implementar los controles seleccionados en el DDA, para cumplir los objetivos de control;
- d) Definir el modo de medir la eficacia de los controles o de los grupos de controles seleccionados y especificar cómo tienen que usarse estas mediciones para evaluar la eficacia de los controles de cara a producir resultados comparables y reproducibles.

**NOTA:** La medición de la eficacia de los controles permite a los directivos y al personal determinar hasta qué punto los controles cumplen los objetivos de control planificados.



|                                                                                                                                                                   |                                                                          |                                        |                                                    |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------|----------------------------------------|----------------------------------------------------|
|  <b>GOBIERNO DE MÉXICO</b><br><b>SALUD</b><br><small>SECRETARÍA DE SALUD</small> | <b>GUÍA DE INTERCAMBIO DE INFORMACIÓN EN SALUD PARA UN SGSI EN SALUD</b> |                                        |                                                    |
|                                                                                                                                                                   | <b>CLAVE DEL DOCUMENTO:</b><br>GIIS-A004-01-07                           | <b>VERSIÓN DEL DOCUMENTO:</b><br>01.07 | <b>FECHA DEL DOCUMENTO:</b><br>07 de junio de 2013 |

- e) Implementar programas de formación y concienciación;
- f) Gestionar la operación del SGSI;
- g) Gestionar los recursos del SGSI;
- h) Implementar procedimientos y otros controles que permitan una detección temprana de eventos de seguridad y una respuesta ante cualquier incidente de seguridad.

## Supervisión y revisión del SGSI

La organización debe:

- a) Ejecutar procedimientos de supervisión y revisión, así como otros mecanismos de control para:
  - 1) Detectar lo antes posible los errores en los resultados del procesado;
  - 2) Identificar lo antes posible las debilidades del sistema de seguridad así como el aprovechamiento de éstas tanto con o sin éxito, y los incidentes;
  - 3) Permitir a la Dirección determinar si las actividades de seguridad delegadas en otras personas o llevadas a cabo por medios informáticos o a través de tecnologías de la información, dan los resultados esperados;
  - 4) Ayudar a detectar eventos de seguridad y por tanto a prevenir incidentes de seguridad mediante el uso de indicadores; y
  - 5) Determinar si las acciones tomadas para resolver una violación de la seguridad han sido eficaces.
- b) Realizar revisiones periódicas de la eficacia del SGSI teniendo en cuenta los resultados de las auditorías de seguridad, los incidentes, los resultados de las mediciones de la eficacia, las sugerencias, así como los comentarios de todas las partes interesadas. Estas revisiones incluyen el cumplimiento de la política, los objetivos del SGSI y la revisión de los controles de seguridad;
- c) Medir la eficacia de los controles para verificar si se han cumplido los requisitos de seguridad;



|                                                                                                                                                                  |                                                                          |                                 |                                             |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------|---------------------------------|---------------------------------------------|
|  <b>GOBIERNO DE MÉXICO</b>   <b>SALUD</b><br><small>SECRETARÍA DE SALUD</small> | <b>GUIA DE INTERCAMBIO DE INFORMACIÓN EN SALUD PARA UN SGSI EN SALUD</b> |                                 |                                             |
|                                                                                                                                                                  | CLAVE DEL DOCUMENTO:<br>GIIS-A004-01-07                                  | VERSIÓN DEL DOCUMENTO:<br>01.07 | FECHA DEL DOCUMENTO:<br>07 de junio de 2013 |

- d) Revisar las evaluaciones de riesgos en intervalos planificados, revisar los riesgos residuales y los niveles de riesgo aceptables que han sido identificados, teniendo en cuenta los cambios en:
- 1) La organización;
  - 2) La tecnología;
  - 3) Los objetivos y requisitos de negocio;
  - 4) Las amenazas identificadas;
  - 5) La eficacia de los controles implementados; y
  - 6) Los factores externos, por ejemplo: los cambios del entorno legal o reglamentario, las obligaciones contractuales y el clima social.
- e) Realizar las auditorías internas del SGSI en intervalos planificados;

**NOTA:** Las auditorías internas, a veces denominadas auditorías de primera parte, las lleva a cabo la propia organización, o bien se realizan por encargo de ésta, con fines internos.

- f) Realizar, por parte de la Dirección una revisión del SGSI, con carácter regular para asegurar que el ámbito de aplicación sigue siendo adecuado y que se identifican mejoras del proceso del SGSI;
- g) Actualizar los planes de seguridad teniendo en cuenta las conclusiones de las actividades de supervisión y revisión;
- h) Registrar las acciones e incidencias que pudieran afectar a la eficacia o al funcionamiento del SGSI.

## Mantenimiento y mejora del SGSI

Periódicamente, la organización debe:

- a) Implementar en el SGSI las mejoras identificadas;
- b) Aplicar las medidas correctivas y preventivas adecuadas, sobre la base de la experiencia en materia de seguridad de la propia organización y de otras organizaciones;





|                                                                                                                                                                  |                                                                          |                                        |                                                    |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------|----------------------------------------|----------------------------------------------------|
|  <b>GOBIERNO DE MÉXICO</b>   <b>SALUD</b><br><small>SECRETARÍA DE SALUD</small> | <b>GUÍA DE INTERCAMBIO DE INFORMACIÓN EN SALUD PARA UN SGSI EN SALUD</b> |                                        |                                                    |
|                                                                                                                                                                  | <b>CLAVE DEL DOCUMENTO:</b><br>GIIS-A004-01-07                           | <b>VERSIÓN DEL DOCUMENTO:</b><br>01.07 | <b>FECHA DEL DOCUMENTO:</b><br>07 de junio de 2013 |

- c) Comunicar las acciones y mejoras a todas las partes interesadas con nivel de detalle acorde con las circunstancias;
- d) Asegurar que las mejoras alcancen los objetivos previstos.

La organización debe establecer las condiciones para:

- Gestionar los documentos y registros derivados de la puesta en marcha del modelo PDCA. Deben definirse las condiciones para aprobar, revisar, actualizar y eliminar los documentos de acuerdo a las necesidades de la organización.
- Gestionar los recursos humanos, materiales y financieros relacionados con el SGSI.
- Concientizar, formar y capacitar al personal al que se le hayan asignado responsabilidades definidas en el SGSI de forma que sea competente para llevar a cabo tareas requeridas.
- Llevar a cabo auditorías internas al SGSI de acuerdo a un procedimiento definido.
- Llevar a cabo revisiones por la Dirección a intervalos planificados para asegurar que el SGSI mantiene su conveniencia, adecuación y eficacia.
- Documentar e implementar acciones correctivas y preventivas que aseguren la mejora continua y eliminen la causa de las no conformidades con los requisitos del SGSI.



|                                                                                                                                                                   |                                                                   |                                 |                                             |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------|---------------------------------|---------------------------------------------|
|  <b>GOBIERNO DE MÉXICO</b><br><b>SALUD</b><br><small>SECRETARÍA DE SALUD</small> | GUÍA DE INTERCAMBIO DE INFORMACIÓN EN SALUD PARA UN SGSI EN SALUD |                                 |                                             |
|                                                                                                                                                                   | CLAVE DEL DOCUMENTO:<br>GIIS-A004-01-07                           | VERSIÓN DEL DOCUMENTO:<br>01.07 | FECHA DEL DOCUMENTO:<br>07 de junio de 2013 |

## CONTROLES DE SEGURIDAD

Esta sección contiene una lista completa de objetivos de control y controles que se han considerado comúnmente relevantes en las organizaciones, así mismo, proporciona a los usuarios que les aplica la NOM-024-SSA3-2012 un punto de partida para seleccionar los controles, garantizando que no se omiten importantes opciones de control.

Esta guía contiene 39 objetivos de control y 134 controles, agrupados en 11 dominios. Los dominios son áreas funcionales de seguridad. Para cada uno de estos dominios se define una serie de objetivos que reflejan lo que se intenta conseguir a través de la implantación de cada uno de los dominios.

Los controles seleccionados serán recogidos del documento llamado “Declaración de Aplicabilidad – DDA”, el cual es un anexo de la presente guía (GIIS-A004-SGSI-ANEXO-A) y debe ser completado por los Prestadores de Servicios de Salud que implementen un SGSI en el marco de la NOM-024-SSA3-2012.

A continuación, se describen cada uno de los dominios, objetivos y controles a observar en el cumplimiento de esta guía.

### 1. POLÍTICA DE SEGURIDAD

#### 1.1. Política de Seguridad de la Información

**Objetivo:** La Dirección proporcionará indicaciones y dará apoyo a la seguridad de la información de acuerdo con los requisitos del negocio, la legislación y las normativas aplicables.

La Dirección deberá establecer de forma clara la política de actuación en línea con los objetivos de negocio y poner de manifiesto su apoyo y compromiso con la seguridad de la información, publicando y manteniendo una política de seguridad de la información en toda la organización.

##### 1.1.1. Documento de política de seguridad de la información

###### Control

La Dirección deberá aprobar un documento de política de seguridad de la información, publicarlo y distribuirlo a todos los empleados y terceros afectados. Las organizaciones que procesan información de salud, incluida información personal de salud, deberán tener un escrito de política de seguridad de la información que está aprobada por la administración, publicado y en conocimiento de todos los empleados y partes externas relevantes.



|                                                                                                                                                                  |                                                                          |                                 |                                             |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------|---------------------------------|---------------------------------------------|
|  <b>GOBIERNO DE MÉXICO</b>   <b>SALUD</b><br><small>SECRETARÍA DE SALUD</small> | <b>GUÍA DE INTERCAMBIO DE INFORMACIÓN EN SALUD PARA UN SGSI EN SALUD</b> |                                 |                                             |
|                                                                                                                                                                  | CLAVE DEL DOCUMENTO:<br>GIIIS-A004-01-07                                 | VERSIÓN DEL DOCUMENTO:<br>01.07 | FECHA DEL DOCUMENTO:<br>07 de junio de 2013 |

## 1.1.2. Revisión de la política de seguridad de la información

### Control

La política de seguridad de la información deberá revisarse a intervalos planificados o siempre que se produzcan cambios significativos, a fin de asegurar que se mantenga su idoneidad, adecuación y eficacia.

La política de seguridad de la información de las organizaciones de salud deberá ser sujeta a la revisión en curso, organizada de tal manera que la totalidad de la política sea revisada al menos cada año. La política deberá ser revisada después de la presencia de un incidente de seguridad serio.

## 2. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN

La Dirección de una organización de salud es responsable de la seguridad de la información personal de salud y de otros datos protegidos relacionados a la salud procesada por la organización. Esto es especialmente digno de destacar a las organizaciones que confían en los servicios gestionados prestados por terceros. La coordinación eficaz es también un ingrediente esencial en el mantenimiento de la seguridad de la información. Ambos requieren una infraestructura de gestión de seguridad de la información explícita y robusta.

### 2.1. Organización interna

**Objetivo:** Gestionar la seguridad de la información dentro de la organización.

Deberá establecerse una estructura de gestión para iniciar y controlar la implementación de la seguridad de la información dentro de la organización.

La Dirección deberá aprobar la política de seguridad de la información, asignando roles o funciones de seguridad, así como coordinar y revisar la implementación de la seguridad en toda la organización.

De ser necesario, deberá establecerse el asesoramiento de especialistas en seguridad de la información y que el asesoramiento esté disponible en la organización. Deberán desarrollarse contactos con grupos o especialistas externos en seguridad, incluidas las autoridades competentes, para mantenerse al día de las tendencias de la industria, la evolución de las normas y los métodos de evaluación, que proporcionen en punto de enlace adecuado para tratar las incidencias de seguridad de la información. Deberá fomentarse un enfoque multidisciplinario de la seguridad de la información.



|                                                                                                                                                                  |                                                                          |                                        |                                                    |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------|----------------------------------------|----------------------------------------------------|
|  <b>GOBIERNO DE MÉXICO</b>   <b>SALUD</b><br><small>SECRETARÍA DE SALUD</small> | <b>GUÍA DE INTERCAMBIO DE INFORMACIÓN EN SALUD PARA UN SGSI EN SALUD</b> |                                        |                                                    |
|                                                                                                                                                                  | <b>CLAVE DEL DOCUMENTO:</b><br>GIIS-A004-01-07                           | <b>VERSIÓN DEL DOCUMENTO:</b><br>01.07 | <b>FECHA DEL DOCUMENTO:</b><br>07 de junio de 2013 |

## 2.1.1. Compromiso de la Dirección con la seguridad de la información

### Control

La Dirección deberá prestar un apoyo activo a la seguridad dentro de la organización a través de directrices claras, un compromiso demostrado, asignaciones explícitas y el reconocimiento de las responsabilidades de seguridad de la información.

Las organizaciones que procesan información personal de salud deberán:

- Definir claramente y asignar responsables de seguridad de la información;
- Tener un FCSI que asegure que existe una visión clara y visible que soporte la gestión las iniciativas de seguridad incluyendo la seguridad de la información en salud.

Como mínimo, al menos un individuo deberá ser el responsable de la información personal de salud dentro de la organización.

El foro de seguridad de la información de salud se reunirá regularmente, una vez al mes, o cerca de un mes (típicamente, es más eficaz para satisfacer el punto medio entre las reuniones del órgano de gobierno en la que el foro informa. Esto permite que los asuntos de emergencia deban tomarse en una reunión en un corto plazo).

Se debe producir una declaración formal sobre el alcance, el cual defina los límites de la actividad en términos del cumplimiento de personas, procesos, lugares, plataformas y aplicaciones.

## 2.1.2. Coordinación de la seguridad de la información

### Control

Las actividades relativas a la seguridad de la información deberán ser coordinadas entre los representantes de las diferentes partes de la organización con sus correspondientes roles y funciones de trabajo.

## 2.1.3. Asignación de responsabilidades relativas a la seguridad de la información

### Control

Deberán definirse claramente todas las responsabilidades relativas a la seguridad de la información.

## 2.1.4. Proceso de autorización de recursos para el tratamiento de la información

### Control

Para cada nuevo recurso de tratamiento de la información, deberá definirse e implantarse un proceso de autorización por parte de la Dirección.



|                                                                                                                                                                  |                                                                      |                                 |                                             |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------|---------------------------------|---------------------------------------------|
|  <b>GOBIERNO DE MÉXICO</b>   <b>SALUD</b><br><small>SECRETARÍA DE SALUD</small> | GUIA DE INTERCAMBIO DE INFORMACIÓN EN SALUD PARA UN<br>SGSI EN SALUD |                                 |                                             |
|                                                                                                                                                                  | CLAVE DEL DOCUMENTO:<br>GIIS-A004-01-07                              | VERSIÓN DEL DOCUMENTO:<br>01.07 | FECHA DEL DOCUMENTO:<br>07 de junio de 2013 |

## 2.1.5. Acuerdos de confidencialidad

### Control

Deberá determinarse y revisarse periódicamente la necesidad de establecer acuerdos de confidencialidad o no revelación, que reflejen las necesidades de la organización para la protección de la información.

Las organizaciones que procesan información personal de salud deberán tener un acuerdo de confidencialidad en el que se especifique la naturaleza confidencial de esta información. El acuerdo deberá ser aplicable a todo el personal que acceda a la información de salud.

## 2.1.6. Contacto con las autoridades

### Control

Deberán mantenerse los contactos adecuados con las autoridades competentes.

## 2.1.7. Contacto con grupos de especial interés

### Control

Deberán mantenerse los contactos adecuados con grupos de interés especial, u otros foros, y asociaciones profesionales especializadas en seguridad.

## 2.1.8. Revisión independiente de la seguridad de la información

### Control

El enfoque de la organización para la gestión de la seguridad de la información y su implantación (es decir, los objetivos de control, los controles, las políticas, los procesos y los procedimientos para la seguridad de la información), deberá someterse a una revisión independiente a intervalos planificados o siempre que se produzcan cambios significados en la implantación de la seguridad.

## 2.2. Terceros

**Objetivo:** Mantener la seguridad de la información de la organización y de los dispositivos de tratamiento de la información que son objeto de acceso, procesado, comunicación o gestión por terceros.

La seguridad de la información de la organización, así como la de los dispositivos de tratamiento de la información, no deberá verse reducida por la introducción de productos o servicios de terceros.

Deberá controlarse cualquier acceso a los dispositivos de tratamiento de la información, así como al tratamiento y comunicación de la información por terceros.



|                                                                                                                                                                   |                                                                          |                                 |                                             |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------|---------------------------------|---------------------------------------------|
|  <b>GOBIERNO DE MÉXICO</b><br><b>SALUD</b><br><small>SECRETARÍA DE SALUD</small> | <b>GUÍA DE INTERCAMBIO DE INFORMACIÓN EN SALUD PARA UN SGSI EN SALUD</b> |                                 |                                             |
|                                                                                                                                                                   | CLAVE DEL DOCUMENTO:<br>GIIIS-A004-01-07                                 | VERSIÓN DEL DOCUMENTO:<br>01.07 | FECHA DEL DOCUMENTO:<br>07 de junio de 2013 |

Cuando por motivos del negocio se necesita trabajar con terceros para lo que se requiere el acceso de éstos a la información de la organización, así como a los dispositivos de tratamiento de la información, o la obtención o suministro de un producto o servicio por parte de un tercero, se deberá llevar a cabo una evaluación del riesgo para determinar las implicaciones de seguridad y los requisitos de control. Los controles deberán decidirse y definirse en un acuerdo con el tercero.

### 2.2.1. Identificación de los riesgos derivados del acceso de terceros

#### Control

Deberán identificarse los riesgos para la información y para los dispositivos de tratamiento de la información de la organización derivados de los procesos de negocio que requieran de terceros, e implantar los controles apropiados antes de otorgar el acceso.

Las organizaciones que procesen información de salud deberán evaluar los riesgos asociados con el acceso de las partes externas a estos sistemas o a los datos que contienen, a continuación, implementar controles de seguridad adecuados al nivel de riesgo y a las tecnologías empleadas.

### 2.2.2. Tratamiento de la seguridad en la relación con los clientes

#### Control

Deberán tratarse todos los requisitos de seguridad identificados, antes de otorgar acceso a los clientes a los activos o a la información de la organización.

### 2.2.3. Tratamiento de la seguridad en contrato con terceros

#### Control

Los acuerdos con terceros que conlleven acceso, procesamiento, comunicación o gestión, bien de la información de la organización, o de los recursos de tratamiento de la información, o bien la incorporación de productos o servicios a los recursos de tratamiento de la información, deberán cubrir todos los requisitos de seguridad pertinentes.

Las organizaciones de salud usan servicios de terceros, donde los servicios de estas partes procesan información personal de salud, deberán emplear contratos formales que especifiquen:

- La naturaleza de la confidencialidad y el valor de la información personal de salud;
- Las mediciones de seguridad a ser implementadas y/o cumplir;
- Limitar el acceso a estos servicios por terceros;
- Los niveles de servicio a ser alcanzados en los servicios prestados;
- El formato y frecuencia de reportes del FGSI de la información de salud;
- La disposición para la representación de terceros en reuniones de organizaciones apropiadas de salud y grupos de trabajo;
- Los acuerdos de auditoría de cumplimiento de terceros;
- Las sanciones impuestas en caso de cualquier fallo en relación con las anteriores.



|                                                                                                                                                                  |                                                                      |                                 |                                             |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------|---------------------------------|---------------------------------------------|
|  <b>GOBIERNO DE MÉXICO</b>   <b>SALUD</b><br><small>SECRETARÍA DE SALUD</small> | GUIA DE INTERCAMBIO DE INFORMACIÓN EN SALUD PARA UN<br>SGSI EN SALUD |                                 |                                             |
|                                                                                                                                                                  | CLAVE DEL DOCUMENTO:<br>GIIS-A004-01-07                              | VERSIÓN DEL DOCUMENTO:<br>01.07 | FECHA DEL DOCUMENTO:<br>07 de junio de 2013 |

### 3. GESTIÓN DE ACTIVOS

#### 3.1. Responsabilidad sobre los activos de Salud

**Objetivo:** Conseguir y mantener una protección adecuada de los activos de la organización.

Todos los activos deberán estar registrados y tener un propietario designado para cada uno.

Se deberán identificar los propietarios para todos los activos y asignar la responsabilidad del mantenimiento de los controles apropiados. La implantación de los controles específicos puede ser delegada por el propietario según éste considere, pero la responsabilidad de la protección adecuada de los activos permanece en el propietario.

##### 3.1.1. Inventario de activos

###### Control

Todos los activos deberán estar claramente identificados y deberá elaborarse y mantenerse un inventario de todos los activos importantes.

##### 3.1.2. Propiedad de los activos

###### Control

Toda la información y activos asociados con los recursos para el tratamiento de la información deberán tener un propietario que forme parte de la organización y haya sido designado como propietario.

##### 3.1.3. Uso aceptable de los activos de Salud

###### Control

Se deberán identificar, documentar e implantar las reglas para el uso aceptable de la información y de los activos asociados con los recursos para el tratamiento de la información.

Las organizaciones que procesan información personal de salud deberán:

- Contabilizar los activos de información de salud (por ejemplo, mantener un inventario de cada activo);
- Tener un custodio designado para estos activos de información en salud;
- Tener reglas de uso aceptable de estos activos que están siendo definidos, documentado e implementado.



|                                                                                                                                                                  |                                                                          |                                        |                                                    |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------|----------------------------------------|----------------------------------------------------|
|  <b>GOBIERNO DE MÉXICO</b>   <b>SALUD</b><br><small>SECRETARÍA DE SALUD</small> | <b>GUIA DE INTERCAMBIO DE INFORMACIÓN EN SALUD PARA UN SGSI EN SALUD</b> |                                        |                                                    |
|                                                                                                                                                                  | <b>CLAVE DEL DOCUMENTO:</b><br>GIIS-A004-01-07                           | <b>VERSIÓN DEL DOCUMENTO:</b><br>01.07 | <b>FECHA DEL DOCUMENTO:</b><br>07 de junio de 2013 |

## 3.2. Clasificación de la información de salud

**Objetivo:** Asegurar que la información recibe un nivel adecuado de protección.

La información deberá ser clasificada para indicar la necesidad, las prioridades y el grado esperado de protección cuando se maneja dicha información. La información tiene varios grados de sensibilidad y criticidad. Algunos elementos pueden requerir un nivel de protección adicional o un manejo especial. Se deberá utilizar un esquema de clasificación de la información para definir un conjunto adecuado de niveles de protección y comunicar la necesidad de medidas especiales para su manipulación.

### 3.2.1. Lineamientos de clasificación

#### Control

La información deberá ser clasificada según su valor, los requisitos legales, su sensibilidad y criticidad para la organización.

Las organizaciones que procesan información personal de salud deberán uniformemente clasificar cada dato como confidencial.

### 3.2.2. Etiquetado y manipulado de la información

#### Control

Se deberá desarrollar e implantar un conjunto adecuado de procedimientos para etiquetar y manejar la información, de acuerdo con el esquema de clasificación adoptado por la organización.

Todos los sistemas de salud que procesan información personal de salud deberán informar a los usuarios de la confidencialidad de la información personal de salud accesible del sistema (por ejemplo, en el inicio o el acceso) y deberán etiquetar la salida de impresión como confidencial cuando contenga información personal de salud.

## 4. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS

### 4.1. Antes del empleo

**Objetivo:** Asegurar que los empleados, los contratistas y los terceros conocen y comprenden sus responsabilidades, y son adecuados para llevar a cabo las funciones que les corresponden, así como para reducir el riesgo de robo, fraude o de uso indebido de los recursos.

Deberán asignarse las responsabilidades sobre seguridad previamente a la contratación y quedar reflejadas en una descripción adecuada del trabajo y de los términos y condiciones de la contratación.





|                                                                                                                                                                  |                                                                          |                                        |                                                    |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------|----------------------------------------|----------------------------------------------------|
|  <b>GOBIERNO DE MÉXICO</b>   <b>SALUD</b><br><small>SECRETARÍA DE SALUD</small> | <b>GUIA DE INTERCAMBIO DE INFORMACIÓN EN SALUD PARA UN SGSI EN SALUD</b> |                                        |                                                    |
|                                                                                                                                                                  | <b>CLAVE DEL DOCUMENTO:</b><br>GIIS-A004-01-07                           | <b>VERSIÓN DEL DOCUMENTO:</b><br>01.07 | <b>FECHA DEL DOCUMENTO:</b><br>07 de junio de 2013 |

Todos los candidatos para un puesto de trabajo, los contratistas y terceros deberán ser adecuadamente investigados, especialmente para trabajos sensibles.

Los empleados, contratistas y terceros que tengan relación directa con los recursos de tratamiento de la información deberán firmar un compromiso relativo a sus funciones y responsabilidades en lo que a seguridad se refiere.

#### **4.1.1. Funciones y responsabilidades**

Las funciones y responsabilidades de seguridad de los empleados, contratistas y terceros se deberán definir y documentar de acuerdo con la política de seguridad de la información de la organización.

#### **4.1.2. Investigación de antecedentes**

##### Control

La comprobación de los antecedentes de todos los candidatos a un puesto de trabajo, de los contratistas o de los terceros, se deberá llevar a cabo de acuerdo con las legislaciones, normativas y códigos éticos que sean de aplicación de una manera proporcionada a los requisitos del negocio, la clasificación de la información a la que se accede y a los riesgos considerados.

Las organizaciones cuyo personal, contratistas o voluntarios que procesen información personal de salud deberán, como mínimo, verificar la identidad, dirección actual y empleo anterior de dicho personal, contratistas y voluntarios en el momento de solicitar empleo.

#### **4.1.3. Términos y condiciones de empleo**

Como parte de sus obligaciones contractuales, los empleados, los contratistas y los terceros deberán aceptar y firmar los términos y condiciones de su contrato de trabajo, que deberá establecer sus responsabilidades y las de la organización en lo relativo a seguridad de la información.

Las organizaciones que procesan información personal de salud deberán incluir en los términos y condiciones de empleo de los empleados que procesan o procesaran, información personal de salud una declaración acerca de la responsabilidad del empleado de seguridad de la información.

### **4.2. Durante el empleo**

**Objetivo:** Asegurar que todos los empleados, contratistas y terceros son conscientes de las amenazas y problemas que afectan a la seguridad de la información y de sus responsabilidades y obligaciones, y de que están preparados para cumplir la política de seguridad de la organización, en el desarrollo habitual de su trabajo, y para reducir el riesgo de error humano.



|                                                                                                                                                                  |                                                                          |                                        |                                                    |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------|----------------------------------------|----------------------------------------------------|
|  <b>GOBIERNO DE MÉXICO</b>   <b>SALUD</b><br><small>SECRETARÍA DE SALUD</small> | <b>GUÍA DE INTERCAMBIO DE INFORMACIÓN EN SALUD PARA UN SGSI EN SALUD</b> |                                        |                                                    |
|                                                                                                                                                                  | <b>CLAVE DEL DOCUMENTO:</b><br>GIIIS-A004-01-07                          | <b>VERSIÓN DEL DOCUMENTO:</b><br>01.07 | <b>FECHA DEL DOCUMENTO:</b><br>07 de junio de 2013 |

Las responsabilidades de la Dirección deberán estar definidas para asegurar que la seguridad se aplica a la contratación de personas dentro de la organización.

Se deberá proporcionar a todos los empleados, contratistas y terceros, un nivel adecuado de concienciación, formación y capacitación en los procedimientos de seguridad así como en el uso correcto de los recursos de tratamiento de la información, para minimizar los posibles riesgos de seguridad. Se deberá establecer un proceso disciplinario de manera formal.

#### **4.2.1. Responsabilidades de la Dirección**

La Dirección deberá exigir a los empleados, contratistas y terceros, que apliquen la seguridad de la información de acuerdo con las políticas y procedimientos establecidos en la organización.

#### **4.2.2. Concienciación, formación y capacitación en seguridad de la información**

##### Control

Todos los empleados de la organización y, cuando corresponda, los contratistas de terceros, investigadores, estudiantes y voluntarios, deberán recibir la adecuada concienciación y formación, con actualizaciones periódicas, sobre la organización, según corresponda con su puesto de trabajo.

Las organizaciones que procesan información personal de salud deberán asegurar que la educación de seguridad de la información y formación se proporcione en la inducción y que actualizaciones periódicas de las políticas y procedimientos de seguridad de la organización se ofrezcan a todos los empleados y, cuando sea pertinente, los contratistas de terceros, investigadores, estudiantes y voluntarios que procesan información personal de salud.

#### **4.2.3. Proceso disciplinario**

Deberá existir un proceso disciplinario formal para los empleados que hayan provocado alguna violación de la seguridad.

### **4.3. Cese del empleo o cambio de puesto de trabajo**

**Objetivo:** Asegurar que los empleados, contratistas y terceros abandonan la organización o cambian de puesto de trabajo de una manera ordenada.

Las responsabilidades deberán asignarse de modo que aseguren que la salida del empleado, contratista o tercero sea gestionada, y que se completa tanto la devolución de todo el equipamiento, como la retirada de todos los derechos de acceso.



|                                                                                                                                                                   |                                                                      |                                 |                                             |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------|---------------------------------|---------------------------------------------|
|  <b>GOBIERNO DE MÉXICO</b><br><b>SALUD</b><br><small>SECRETARÍA DE SALUD</small> | GUIA DE INTERCAMBIO DE INFORMACIÓN EN SALUD PARA UN<br>SGSI EN SALUD |                                 |                                             |
|                                                                                                                                                                   | CLAVE DEL DOCUMENTO:<br>GIIS-A004-01-07                              | VERSIÓN DEL DOCUMENTO:<br>01.07 | FECHA DEL DOCUMENTO:<br>07 de junio de 2013 |

Los cambios en las responsabilidades y en el puesto de trabajo dentro de una organización deberán gestionarse de igual manera que la finalización de la responsabilidad o del contrato correspondiente en línea con lo establecido en este apartado, y cualquier nueva contratación deberá gestionarse.

#### 4.3.1. Responsabilidad del cese o cambio

Las responsabilidades para proceder al cese en el empleo o al cambio de puesto de trabajo deberán estar claramente definidas y asignadas.

#### 4.3.2. Devolución de activos

Todos los empleados, contratistas y terceros deberán devolver todos los activos de la organización en su poder a la terminación de su empleo, contrato o acuerdo.

#### 4.3.3. Retirada de los derechos de acceso

##### Control

Todos los empleados, contratistas y terceros deberán devolver todos los activos de la organización que estén en su poder al finalizar su empleo, contrato o acuerdo.

Todas las organizaciones que procesan información personal de salud deberán tan pronto sea posible, terminar los privilegios de acceso de usuario con respecto a dicha información para cualquier empleado permanente o temporal que se marcha, contratistas de terceros o voluntario a la terminación de las actividades de empleo, contratación o actividades voluntarias.

## 5. SEGURIDAD FÍSICA Y DEL ENTORNO

### 5.1. Áreas seguras

**Objetivo:** Prevenir los accesos físicos no autorizados, los daños y las intromisiones en las instalaciones y en la información de la organización.

Los recursos de tratamiento de la información crítica y sensible deberán estar situados en áreas seguras y protegidos por perímetros de seguridad definidos mediante barreras de seguridad y controles de entrada adecuados. Deberán estar físicamente protegidos de accesos no autorizados, de daños y de interferencias.

La protección proporcionada deberá ser proporcional a los riesgos identificados.



|                                                                                                                                                                  |                                                                          |                                        |                                                    |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------|----------------------------------------|----------------------------------------------------|
|  <b>GOBIERNO DE MÉXICO</b>   <b>SALUD</b><br><small>SECRETARÍA DE SALUD</small> | <b>GUIA DE INTERCAMBIO DE INFORMACIÓN EN SALUD PARA UN SGSI EN SALUD</b> |                                        |                                                    |
|                                                                                                                                                                  | <b>CLAVE DEL DOCUMENTO:</b><br>GIIS-A004-01-07                           | <b>VERSIÓN DEL DOCUMENTO:</b><br>01.07 | <b>FECHA DEL DOCUMENTO:</b><br>07 de junio de 2013 |

### 5.1.1. Perímetro de seguridad física

#### Control

Se deberán utilizar perímetros de seguridad (barreras, muros, puertas de entrada con control de acceso a través de tarjeta, o puestos de control) para proteger las áreas que contienen la información y los recursos de tratamiento de la información.

Las organizaciones que procesan la información personal de salud deberán usar perímetros de seguridad para proteger las áreas que contienen instalaciones de procesamiento de información de apoyo a este tipo de aplicaciones para la salud. Estas áreas seguras deberán ser protegidas por mandos de entrada apropiados para garantizar que solo el personal autorizado pueda tener acceso.

### 5.1.2. Controles físicos de entrada

Las áreas seguras deberán estar protegidas por controles de entrada adecuados, para asegurar que únicamente se permite el acceso al personal autorizado.

### 5.1.3. Seguridad de oficinas, despachos e instalaciones

Se deberán diseñar y aplicar las medidas de seguridad física para las oficinas, despachos e instalaciones.

### 5.1.4. Protección contra las amenazas externas y de origen ambiental

Se deberá diseñar y aplicar una protección física contra el daño causado por fuego, inundación, terremoto, explosión, revueltas sociales y otras formas de desastres naturales o provocados por el hombre.

### 5.1.5. Trabajo en áreas seguras

Se deberán diseñar e implantar una protección física y una serie de directrices para trabajar en las áreas seguras.

### 5.1.6. Áreas de acceso público y de carga y descarga

Deberán controlarse los puntos de acceso tales como las áreas de carga y descarga y otros puntos, a través de los que personal no autorizado pueda acceder a las instalaciones, y si es posible, dichos puntos se deberán aislar de las instalaciones de tratamiento de la información para evitar accesos no autorizados.



|                                                                                                                                                                   |                                                                          |                                        |                                                    |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------|----------------------------------------|----------------------------------------------------|
|  <b>GOBIERNO DE MÉXICO</b><br><b>SALUD</b><br><small>SECRETARÍA DE SALUD</small> | <b>GUIA DE INTERCAMBIO DE INFORMACIÓN EN SALUD PARA UN SGSI EN SALUD</b> |                                        |                                                    |
|                                                                                                                                                                   | <b>CLAVE DEL DOCUMENTO:</b><br>GIIIS-A004-01-07                          | <b>VERSIÓN DEL DOCUMENTO:</b><br>01.07 | <b>FECHA DEL DOCUMENTO:</b><br>07 de junio de 2013 |

## 5.2. Seguridad de los equipos

**Objetivo:** Evitar pérdidas, daños, robos o circunstancias que pongan en peligro los activos, o que puedan provocar la interrupción de las actividades de la organización.

Los equipos deberán estar protegidos de las amenazas físicas y del entorno.

La protección de los equipos (incluidos el que se utiliza fuera de la oficina y la extracción de pertenencias) es necesaria para reducir el riesgo de acceso no autorizado a la información y para protegerlo contra la pérdida o robo. Esto también deberá tenerse en cuenta para la instalación y retirada del equipamiento. Pueden requerirse controles especiales para proteger contra amenazas físicas y para salvaguardar las instalaciones de apoyo tales como el suministro eléctrico y la infraestructura del cableado.

### 5.2.1. Emplazamiento y protección de equipos

Los equipos deberán situarse o protegerse de forma que se reduzcan los riesgos derivados de las amenazas y peligros de origen ambiental, así como las ocasiones de que se produzcan accesos no autorizados.

### 5.2.2. Instalaciones de suministro

Los equipos deberán estar protegidos contra fallos de alimentación y otras anomalías causadas por fallos en las instalaciones de suministro.

### 5.2.3. Seguridad del cableado

El cableado eléctrico y de telecomunicaciones que transmite datos o que da soporte a los servicios de información deberá estar protegido frente a interceptaciones o daños.

### 5.2.4. Mantenimiento de los equipos

Los equipos deberán recibir un mantenimiento correcto que asegure su disponibilidad y su integridad.

### 5.2.5. Seguridad de los equipos fuera de las instalaciones

#### Control

Teniendo en cuenta los diferentes riesgos que conlleva trabajar fuera de las instalaciones de la organización, deberán aplicarse medidas de seguridad a los equipos situados fuera de dichas instalaciones.

Las organizaciones que procesan información personal de salud deberán asegurar que cualquier uso, fuera de las instalaciones, de dispositivos médicos que graban o reportan información haya sido autorizado. Esto deberá incluir equipo usado por trabajadores remotos, aun donde cada uso sea perpetuo (por ejemplo, personal de ambulancias, terapeutas, etc.).



|                                                                                                                                                                  |                                                                      |                                 |                                             |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------|---------------------------------|---------------------------------------------|
|  <b>GOBIERNO DE MÉXICO</b>   <b>SALUD</b><br><small>SECRETARÍA DE SALUD</small> | GUIA DE INTERCAMBIO DE INFORMACIÓN EN SALUD PARA UN<br>SGSI EN SALUD |                                 |                                             |
|                                                                                                                                                                  | CLAVE DEL DOCUMENTO:<br>GIIIS-A004-01-07                             | VERSIÓN DEL DOCUMENTO:<br>01.07 | FECHA DEL DOCUMENTO:<br>07 de junio de 2013 |

## 5.2.6. Reutilización o retirada segura de equipos

### Control

Todos los medios de almacenamiento deberán ser comprobados para confirmar que todo dato sensible y todas las licencias de software se han eliminado o bien se han borrado o sobrescrito de manera segura, antes de su retirada.

Las organizaciones que procesan información personal de salud deberán sobrescribir o destruir todos los medios que contengan aplicaciones de software con información de salud o información personal de salud cuando los medios no sean requeridos para su uso.

## 5.2.7. Retirada de materiales propiedad de la organización

### Control

Los equipos, la información o el software no deberán extraerse de las instalaciones, sin una autorización previa.

Las organizaciones que prestan o usan equipos, datos o software para soportar aplicaciones de salud conteniendo información personal de salud no deberán permitir dicho equipo, datos o software a ser retirados del sitio o reubicados dentro sin la autorización por la organización.

# 6. GESTIÓN DE COMUNICACIONES Y OPERACIONES

## 6.1. Responsabilidades y procedimientos de operación

**Objetivo:** Asegurar el funcionamiento correcto y seguro de los recursos de tratamiento de la información.

Deberán establecerse las responsabilidades y los procedimientos para la gestión y operación de todos los recursos de información. Esto incluye el desarrollo de procedimientos de funcionamiento adecuados.

Dónde se considere apropiado se deberá implantar una segregación de tareas, para reducir el riesgo de negligencia o de uso incorrecto intencionado.

### 6.1.1. Documentación de los procedimientos de operación

Deberán documentarse y mantenerse los procedimientos de operación y ponerse a disposición de todos los usuarios que los necesiten.



|                                                                                                                                                                  |                                                                          |                                        |                                                    |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------|----------------------------------------|----------------------------------------------------|
|  <b>GOBIERNO DE MÉXICO</b>   <b>SALUD</b><br><small>SECRETARÍA DE SALUD</small> | <b>GUÍA DE INTERCAMBIO DE INFORMACIÓN EN SALUD PARA UN SGSI EN SALUD</b> |                                        |                                                    |
|                                                                                                                                                                  | <b>CLAVE DEL DOCUMENTO:</b><br>GIIIS-A004-01-07                          | <b>VERSIÓN DEL DOCUMENTO:</b><br>01.07 | <b>FECHA DEL DOCUMENTO:</b><br>07 de junio de 2013 |

## 6.1.2. Gestión de cambios

### Control

Deberán controlarse los cambios en los recursos y en los sistemas de tratamiento de la información.

Las organizaciones que procesan información personal de salud deberán, por medio de un proceso, de control de cambio formal y estructurado controlar los cambios a instalaciones de procesamiento y sistemas que procesan información personal de salud para garantizar el control adecuado de aplicaciones y sistemas, así como la continuidad en el proceso de atención al paciente.

## 6.1.3. Segregación de tareas

Las tareas y áreas de responsabilidad deberán segregarse para reducir la posibilidad de que se produzcan modificaciones no autorizadas o no intencionadas o usos indebidos de los activos de la organización.

## 6.1.4. Separación de los recursos de desarrollo, prueba y operación

### Control

Deberán separarse los recursos y aplicativos de desarrollo, pruebas y producción, para reducir los riesgos de acceso no autorizado o los cambios en el sistema en producción.

Las organizaciones que procesan información personal de salud deberán separar (física y virtualmente) ambientes de prueba y desarrollo de aquellos SIREs que procesan dicha información.

## 6.2. Gestión de la provisión de servicios por terceros

**Objetivo:** Implantar y mantener el nivel apropiado de seguridad de la información en la provisión del servicio, en consonancia con los acuerdos de provisión de servicios por terceros.

La organización deberá comprobar el cumplimiento de los acuerdos, vigilar la conformidad con los acuerdos, así como gestionar los cambios necesarios para asegurar que los servicios entregados son conformes con todos los requisitos acordados con los terceros.

### 6.2.1. Provisión de servicios

Se deberá comprobar que los controles de seguridad, las definiciones de los servicios y los niveles de provisión, incluidos en el acuerdo de provisión de servicios por terceros, han sido implementados, puestos en operación y son mantenidos por parte de un tercero.



|                                                                                                                                                                   |                                                                      |                                 |                                             |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------|---------------------------------|---------------------------------------------|
|  <b>GOBIERNO DE MÉXICO</b><br><b>SALUD</b><br><small>SECRETARÍA DE SALUD</small> | GUIA DE INTERCAMBIO DE INFORMACIÓN EN SALUD PARA UN<br>SGSI EN SALUD |                                 |                                             |
|                                                                                                                                                                   | CLAVE DEL DOCUMENTO:<br>GIIS-A004-01-07                              | VERSIÓN DEL DOCUMENTO:<br>01.07 | FECHA DEL DOCUMENTO:<br>07 de junio de 2013 |

### 6.2.2. Supervisión y revisión de los servicios prestados por terceros

Los servicios, informes y registros proporcionados por un tercero deberán ser objeto de supervisión y revisión periódicas, y también deberán llevarse a cabo auditorías periódicas.

### 6.2.3. Gestión del cambio en los servicios prestados por terceros

Se deberán gestionar los cambios en la provisión de los servicios, incluyendo el mantenimiento y la mejora de las políticas, los procedimientos y los controles de seguridad de la información existentes, teniendo en cuenta la criticidad de los procesos y sistemas del negocio afectados, así como la reevaluación de los riesgos.

## 6.3. Planificación y aceptación del sistema

**Objetivo:** Minimizar el riesgo de fallos de los sistemas.

Se requiere una planificación y una preparación por adelantado para asegurar la disponibilidad de una capacidad y unos recursos adecuados para proporcionar el rendimiento requerido del sistema.

Se deberán hacer proyecciones de los requisitos futuros de capacidad, para reducir el riesgo.

Se deberán establecer, documentar y probar los requisitos operacionales de los sistemas nuevos previamente a su aceptación y uso.

### 6.3.1. Gestión de capacidades

La utilización de los recursos se deberá supervisar y ajustar así como realizar proyecciones de los requisitos futuros de capacidad, para garantizar el rendimiento requerido del sistema.

### 6.3.2. Aceptación del sistema

#### Control

Se deberán establecer los criterios para la aceptación de nuevos sistemas de información, de las actualizaciones y de nuevas versiones de los mismos, y se deberán llevar a cabo pruebas adecuadas de los SIRES durante el desarrollo y previamente a la liberación.

Las organizaciones que procesan información personal de salud deberán establecer criterios de aceptación para planear nuevos sistemas, actualizaciones y nuevas versiones.

Se deberán llevar a cabo las pruebas adecuadas del sistema antes de la liberación.





|                                                                                                                                                                   |                                                                      |                                 |                                             |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------|---------------------------------|---------------------------------------------|
|  <b>GOBIERNO DE MÉXICO</b><br><b>SALUD</b><br><small>SECRETARÍA DE SALUD</small> | GUÍA DE INTERCAMBIO DE INFORMACIÓN EN SALUD PARA UN<br>SGSI EN SALUD |                                 |                                             |
|                                                                                                                                                                   | CLAVE DEL DOCUMENTO:<br>GIIIS-A004-01-07                             | VERSIÓN DEL DOCUMENTO:<br>01.07 | FECHA DEL DOCUMENTO:<br>07 de junio de 2013 |

## 6.4. Protección contra el código malicioso y descargable

**Objetivo:** Proteger la integridad del software y de la información.

Se deberán establecer los criterios para la aceptación de nuevos sistemas de información, de las actualizaciones y de nuevas versiones de los mismos, y se deberán llevar a cabo pruebas adecuadas de los sistemas durante el desarrollo y previamente a la aceptación.

Los recursos de tratamiento de la información y del software son vulnerables a la introducción de código malicioso, como virus informáticos, gusanos de red, caballos troyanos y bombas lógicas. Los usuarios deberán ser conscientes del daño del código malicioso. La Dirección deberá, donde sea apropiado, introducir controles para prevenir, detectar y eliminar el código malicioso y controlar el código descargable.

### 6.4.1. Controles contra el código malicioso

#### Control

Se deberán implantar controles de detención, prevención y recuperación que sirvan como protección contra el código malicioso y se deberán implantar procedimientos adecuados de concienciación del usuario.

Las organizaciones que procesan información personal de salud deberán implementar controles de detección, prevención y respuesta apropiados para proteger contra software malicioso y pondrán en práctica la formación adecuada de sensibilización de los usuarios.

### 6.4.2. Controles contra el código descargado en el cliente

Cuando se autorice el uso de código descargado en el cliente, la configuración deberá garantizar que dicho código autorizado funciona de acuerdo con una política de seguridad claramente definida, y se deberá evitar que se ejecute el código no autorizado.

## 6.5. Copia de seguridad de información de salud

**Objetivo:** Mantener la integridad y disponibilidad de la información y de los recursos de tratamiento de la información.

### 6.5.1. Copias de seguridad de la información en Salud

Deberán establecerse procedimientos rutinarios para implantar la política de copias de seguridad acordada y la estrategia para realizar las copias de seguridad de los datos y ensayar periódicamente sus tiempos de recuperación.

#### Control

Se deberán realizar copias de seguridad de la información y del software, y se deberán probar periódicamente conforme a la política de copias de seguridad acordada.



|                                                                                                                                                                   |                                                                      |                                 |                                             |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------|---------------------------------|---------------------------------------------|
|  <b>GOBIERNO DE MÉXICO</b><br><b>SALUD</b><br><small>SECRETARÍA DE SALUD</small> | GUIA DE INTERCAMBIO DE INFORMACIÓN EN SALUD PARA UN<br>SGSI EN SALUD |                                 |                                             |
|                                                                                                                                                                   | CLAVE DEL DOCUMENTO:<br>GIIS-A004-01-07                              | VERSIÓN DEL DOCUMENTO:<br>01.07 | FECHA DEL DOCUMENTO:<br>07 de junio de 2013 |

Las organizaciones que procesan información personal de salud deberán respaldar toda la información de salud y almacenada en ambientes físicos seguros para asegurar su futura disponibilidad.

## 6.6. Gestión de la seguridad de las redes

**Objetivo:** Asegurar la protección de la información en las redes y la protección de la infraestructura de soporte.

La gestión segura de las redes, que puede extenderse hasta las fronteras de la organización, requiere consideraciones cuidadosas relativas a las implicaciones legales, al control y a la protección del flujo de datos.

Pueden requerirse controles adicionales para proteger la información sensible que pase a través de redes públicas.

### 6.6.1. Controles de red

Las redes deberán estar adecuadamente gestionadas y controladas, para que estén protegidas frente a posibles amenazas y para mantener la seguridad de los sistemas y de las aplicaciones que utilizan estas redes, incluyendo la información en tránsito.

### 6.6.2. Seguridad de los servicios de red

Se deberán identificar las características de seguridad, los niveles de servicio, y los requisitos de gestión de todos los servicios de red y se deberán incluir en todos los acuerdos relativos a servicios de red, tanto si estos servicios se prestan dentro de la organización como si se subcontratan.

## 6.7. Manipulación de los medios

**Objetivo:** Evitar la revelación, modificación, retirada o destrucción no autorizada de los activos, y la interrupción de las actividades de la organización.

Los medios deberán ser controlados y protegidos físicamente.

Deberán establecerse procedimientos operativos apropiados para proteger los documentos, los medios informáticos (por ejemplo: cintas, discos), los datos de entrada y salida, y la documentación del sistema, contra la revelación, modificación, eliminación o destrucción no autorizada.

### 6.7.1. Gestión de los medios extraíbles

Se deberán establecer procedimientos para la gestión de los medios extraíbles.



|                                                                                                                                                                  |                                                                          |                                        |                                                    |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------|----------------------------------------|----------------------------------------------------|
|  <b>GOBIERNO DE MÉXICO</b>   <b>SALUD</b><br><small>SECRETARÍA DE SALUD</small> | <b>GUÍA DE INTERCAMBIO DE INFORMACIÓN EN SALUD PARA UN SGSI EN SALUD</b> |                                        |                                                    |
|                                                                                                                                                                  | <b>CLAVE DEL DOCUMENTO:</b><br>GIIS-A004-01-07                           | <b>VERSIÓN DEL DOCUMENTO:</b><br>01.07 | <b>FECHA DEL DOCUMENTO:</b><br>07 de junio de 2013 |

## 6.7.2. Retirada de medios

### Control

Los medios deberán ser retirados de forma segura cuando ya no vayan a ser necesarios, mediante los procedimientos formales establecidos. Toda la información de salud deberá ser sobrescrita o destruida de los medios cuando no sean requeridas para su uso.

## 6.7.3. Procedimientos de manipulación de la información

### Control

Deberán establecerse procedimientos para la manipulación y el almacenamiento de la información, de modo que se proteja dicha información contra la revelación no autorizada o el uso indebido.

Los medios que contengan información personal de salud deberán ser físicamente protegidos o tener sus datos cifrados. El estado y la localización de medios que contengan información personal de salud sin cifrar deberán ser monitoreados.

## 6.7.4. Seguridad de la documentación del sistema

La documentación del sistema deberá estar protegida contra accesos no autorizados

## 6.8. Intercambio de información

**Objetivo:** Mantener la seguridad de la información y del software intercambiados dentro de una organización y con un tercero.

Los intercambios de información y de software entre organizaciones deberán estar basados en una política de intercambio formal, llevada a cabo de acuerdo con los acuerdos de intercambio, y deberá ser conforme con cualquier legislación aplicable.

Se deberán establecer procedimientos y normas para proteger la información y los medios físicos en tránsito que contienen información.

### 6.8.1. Políticas y procedimientos de intercambio de información de salud

Deberán establecerse políticas, procedimientos y controles formales que protejan el intercambio de información mediante el uso de todo tipo de recursos de comunicación.

### 6.8.2. Acuerdos de intercambio

Deberán establecerse acuerdos para el intercambio de información y de software entre la organización y los terceros.



|                                                                                                                                                                   |                                                                      |                                 |                                             |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------|---------------------------------|---------------------------------------------|
|  <b>GOBIERNO DE MÉXICO</b><br><b>SALUD</b><br><small>SECRETARÍA DE SALUD</small> | GUIA DE INTERCAMBIO DE INFORMACIÓN EN SALUD PARA UN<br>SGSI EN SALUD |                                 |                                             |
|                                                                                                                                                                   | CLAVE DEL DOCUMENTO:<br>GIIS-A004-01-07                              | VERSIÓN DEL DOCUMENTO:<br>01.07 | FECHA DEL DOCUMENTO:<br>07 de junio de 2013 |

### 6.8.3. Medios físicos en tránsito

Durante el transporte fuera de los límites físicos de la organización, los medios que contengan información deberán estar protegidos contra accesos no autorizados, usos indebidos o deterioro.

### 6.8.4. Mensajería electrónica

La información que sea objeto de mensajería electrónica deberá estar adecuadamente protegida.

### 6.8.5. Sistemas de información de salud

Deberán formularse e implantarse políticas y procedimientos para proteger la información asociada a la interconexión de los sistemas de información de Salud.

## 6.9. Servicios de comercio electrónico en salud

**Objetivo:** Garantizar la seguridad de los servicios de comercio electrónico, y el uso seguro de los mismos.

Deberán considerarse las implicaciones de seguridad asociadas al uso de los servicios de comercio electrónico, incluyendo las transacciones en línea, y los requisitos para los controles. También deberá tenerse en cuenta la integridad y disponibilidad de la información publicada electrónicamente a través de sistemas públicamente disponibles.

### 6.9.1. Comercio electrónico

La información incluida en el comercio electrónico que se transmita a través de redes públicas deberá protegerse contra las actividades fraudulentas, las disputas contractuales, y la revelación o modificación no autorizada de dicha información.

### 6.9.2. Transacciones en línea

La información contenida en las transacciones en línea deberá estar protegida para evitar transmisiones incompletas, errores de direccionamiento, alteraciones no autorizadas de los mensajes, la revelación, la duplicación o la reproducción no autorizadas del mensaje.

### 6.9.3. Información de salud públicamente disponible

#### Control

La integridad de la información puesta a disposición pública se deberá proteger para evitar modificaciones no autorizadas.

Aquella información de salud públicamente disponible (a diferencia de la información personal de salud) deberá ser archivada.



|                                                                                                                                                                   |                                                                      |                                 |                                             |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------|---------------------------------|---------------------------------------------|
|  <b>GOBIERNO DE MÉXICO</b><br><b>SALUD</b><br><small>SECRETARÍA DE SALUD</small> | GUÍA DE INTERCAMBIO DE INFORMACIÓN EN SALUD PARA UN<br>SGSI EN SALUD |                                 |                                             |
|                                                                                                                                                                   | CLAVE DEL DOCUMENTO:<br>GIIIS-A004-01-07                             | VERSIÓN DEL DOCUMENTO:<br>01.07 | FECHA DEL DOCUMENTO:<br>07 de junio de 2013 |

La integridad de la información de salud públicamente disponible deberá ser protegida para prevenir modificaciones no autorizadas.

La fuente de la información de salud públicamente disponible deberá ser declarada y su integridad deberá ser protegida.

## 6.10. Supervisión

**Objetivo:** Detectar las actividades de tratamiento de la información no autorizadas.

Los sistemas deberán ser monitorizados y los eventos de seguridad de la información deberán ser registrados. Se deberán utilizar diarios de los registros de fallos para asegurar que se identifican los problemas del sistema de información.

### 6.10.1. Registros de auditoría

#### General

De todos los requisitos de seguridad que protegen la información personal de salud, entre los más importantes son aquellos relacionados con la auditoría y registro. Con ello se garantiza la responsabilidad para los sujetos de atención, confiar su información a SIRES y también proporcionan un incentivo fuerte a los usuarios de tales sistemas para cumplir con las políticas sobre el uso aceptable de sistemas. Una auditoría eficaz y registro pueden ayudar a descubrir el mal uso de sistemas de información o de la información personal de salud. Estos procesos también pueden ayudar a las organizaciones y los sujetos de atención a obtener reparación contra usuarios que abusen de sus privilegios de acceso.

Una organización deberá cumplir con todos los requisitos legales que le son de aplicación para las actividades de seguimiento y de registro.

La monitorización del sistema deberá utilizarse para comprobar la eficacia de los controles adoptados y para verificar la conformidad con el modelo de políticas de accesos.

Se deberán generar registros de auditoría de las actividades de los usuarios, las excepciones y eventos de seguridad de la información, y se deberán mantener estos registros durante un periodo acordado para servir como prueba en investigaciones futuras y en la supervisión del control de acceso.

### 6.10.2. Supervisión del uso del sistema

Se deberán establecer procedimientos para supervisar el uso de los recursos de tratamiento de la información y se deberán revisar periódicamente los resultados de las actividades de supervisión.



|                                                                                                                                                                  |                                                                      |                                 |                                             |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------|---------------------------------|---------------------------------------------|
|  <b>GOBIERNO DE MÉXICO</b>   <b>SALUD</b><br><small>SECRETARÍA DE SALUD</small> | GUÍA DE INTERCAMBIO DE INFORMACIÓN EN SALUD PARA UN<br>SGSI EN SALUD |                                 |                                             |
|                                                                                                                                                                  | CLAVE DEL DOCUMENTO:<br>GIIIS-A004-01-07                             | VERSIÓN DEL DOCUMENTO:<br>01.07 | FECHA DEL DOCUMENTO:<br>07 de junio de 2013 |

### 6.10.3. Protección de la información de los registros

#### Control

Los dispositivos de registro y la información de los registros deberán estar protegidos contra manipulaciones indebidas y accesos no autorizados.

Registros de auditoría deberán ser seguros y a prueba de manipulaciones. El acceso a las herramientas de auditoría del sistema y las pistas de auditoría deberán ser protegidas para evitar el mal uso o sea comprometido.

### 6.10.4. Registros de administración y operación

Se deberán registrar las actividades del administrador y del operador del sistema.

### 6.10.5. Registro de fallos

Los fallos deberán ser registrados y analizados y se deberán tomar las correspondientes acciones correctivas.

### 6.10.6. Sincronización del reloj

#### Control

Los relojes de todos los sistemas de tratamiento de la información dentro de una organización o de un dominio de seguridad, deberán estar sincronizados con una única fuente precisa y acordada de tiempo.

Los SIRES que soporten actividades de atención crítica en el tiempo compartido deberán proporcionar servicios de sincronización de tiempo que soporte el seguimiento y la reconstrucción de las actividades de las líneas de tiempo donde se requieran.

## 7. CONTROL DE ACCESO

### 7.1. Requisitos de control de acceso en salud

**Objetivo:** Controlar el acceso a la información

El acceso a la información, los recursos de tratamiento de la información y los procesos de negocio deberán ser controlados sobre la base de los requisitos de negocio y de seguridad.

Las reglas de control de acceso deberán tener en cuenta las políticas para la disseminación y autorización de la información.



|                                                                                                                                                                  |                                                                          |                                        |                                                    |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------|----------------------------------------|----------------------------------------------------|
|  <b>GOBIERNO DE MÉXICO</b>   <b>SALUD</b><br><small>SECRETARÍA DE SALUD</small> | <b>GUIA DE INTERCAMBIO DE INFORMACIÓN EN SALUD PARA UN SGSI EN SALUD</b> |                                        |                                                    |
|                                                                                                                                                                  | <b>CLAVE DEL DOCUMENTO:</b><br>GIIIS-A004-01-07                          | <b>VERSIÓN DEL DOCUMENTO:</b><br>01.07 | <b>FECHA DEL DOCUMENTO:</b><br>07 de junio de 2013 |

### Control

Organizaciones que procesan información personal de salud deberán controlar el acceso a dicha información. En general, los usuarios de los SIREs solo deberán acceder a la información personal de salud en los siguientes casos:

- Cuando una relación de salud exista entre el usuario y el sujeto de datos (el sujeto de atención cuya información personal de salud este siendo accedida);
- Cuando el usuario está realizando una actividad de parte del sujeto de datos;
- Cuando hay una necesidad para datos específicos que soporten esta actividad.

## **7.1.1. Política de control de acceso**

### Control

Se deberá establecer, documentar y revisar una política de control de acceso basada en los requisitos del negocio y de seguridad para el acceso.

Organizaciones que procesan información personal de salud deberán tener una política de control de acceso que rige el acceso a estos datos.

La política de la organización en el control de acceso deberá ser establecida en la base de los roles predefinidos con autoridades que sean compatibles con asociados, pero sin limitarse a las necesidades de ese papel.

La política de control de acceso, reflejará requisitos profesionales, éticos, legales y relacionados con el sujeto de atención y deberá tomar en cuenta las tareas realizadas por profesionales de la salud y el flujo de trabajo de las tareas.

## **7.2. Gestión de acceso de usuario**

**Objetivo:** Asegurar el acceso de un usuario autorizado y prevenir el acceso no autorizado a los sistemas de información.

Se deberán establecer procedimientos formales para controlar la localización de los derechos de acceso a los sistemas de información y los servicios.

Los procedimientos deberán cubrir todas las fases del ciclo de vida del acceso de usuario, desde el registro inicial de nuevos usuarios al registro final de los usuarios que no requieren el acceso a los SIREs y a los servicios por más tiempo. Se deberá poner especial atención, dónde corresponda, a la necesidad de localización de los privilegios de derechos de acceso, que permiten a los usuarios invalidar los controles del sistema.



|                                                                                                                                                                  |                                                                          |                                        |                                                    |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------|----------------------------------------|----------------------------------------------------|
|  <b>GOBIERNO DE MÉXICO</b>   <b>SALUD</b><br><small>SECRETARÍA DE SALUD</small> | <b>GUIA DE INTERCAMBIO DE INFORMACIÓN EN SALUD PARA UN SGSI EN SALUD</b> |                                        |                                                    |
|                                                                                                                                                                  | <b>CLAVE DEL DOCUMENTO:</b><br>GIIIS-A004-01-07                          | <b>VERSIÓN DEL DOCUMENTO:</b><br>01.07 | <b>FECHA DEL DOCUMENTO:</b><br>07 de junio de 2013 |

### 7.2.1. Registro de usuario

#### Control

Deberá establecerse un procedimiento formal de registro y de anulación de usuarios para conceder y revocar el acceso a todos los sistemas y servicios de información.

Los accesos a los SIRES que procesan información personal de salud deberán ser sujetos de un proceso formal de registro de usuarios. Los procedimientos de registro de usuarios deberán asegurar que el nivel de autenticación requerida de usuario sea consistente con el nivel o niveles de acceso disponibles para el usuario.

### 7.2.2. Gestión de privilegios

La asignación y el uso de privilegios deberán estar restringidos y controlados.

A continuación, diversas estrategias de control de acceso son especificadas y pueden ayudar significativamente para asegurar la confidencialidad e integridad de la información personal de salud:

- Control de acceso basado en roles, que se basa en las credenciales profesionales y títulos de trabajo de los usuarios establecido durante el registro para restringir los privilegios de acceso de los usuarios a solo los necesarios para cumplir con uno o más roles definidos;
- Control de acceso basado en grupos de trabajo, que se basaba en la asignación de usuarios de grupos de trabajo (tales como equipos clínicos) para determinar cuáles registros pueden acceder;
- Control de acceso discrecional, el cual habilita a los usuarios de sistemas de información de salud quienes tengan relación legítima con la información personal de salud de los sujetos de atención (por ejemplo, familiares) para garantizar el acceso a otros usuarios quienes no tengan relación previamente establecida con la información personal de salud de dicho sujeto de atención (por ejemplo, un especialista).

### 7.2.3. Gestión de contraseñas de usuarios

La asignación de contraseñas deberá ser controlada a través de un proceso de gestión formal.

Aunque debe tenerse en cuenta que la presión del tiempo encontrada en situaciones de entrega de la salud puede hacer uso efectivo de las contraseñas difíciles de emplear. Muchas organizaciones de salud han considerado la adopción de tecnologías de autenticación alternativas para hacer frente a este problema.





|                                                                                                                                                                  |                                                                          |                                        |                                                    |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------|----------------------------------------|----------------------------------------------------|
|  <b>GOBIERNO DE MÉXICO</b>   <b>SALUD</b><br><small>SECRETARÍA DE SALUD</small> | <b>GUIA DE INTERCAMBIO DE INFORMACIÓN EN SALUD PARA UN SGSI EN SALUD</b> |                                        |                                                    |
|                                                                                                                                                                  | <b>CLAVE DEL DOCUMENTO:</b><br>GIIS-A004-01-07                           | <b>VERSIÓN DEL DOCUMENTO:</b><br>01.07 | <b>FECHA DEL DOCUMENTO:</b><br>07 de junio de 2013 |

#### 7.2.4. Revisión de los derechos de acceso de usuario

La Dirección deberá revisar los derechos de acceso de usuario a intervalos regulares y utilizando un proceso formal.

### 7.3. Responsabilidades de usuario

**Objetivo:** Evitar el acceso de usuarios no autorizados, y el compromiso o el robo a las instalaciones de procesamiento de información y la información.

#### 7.3.1. Uso de contraseñas

Se deberá requerir a los usuarios el seguir las buenas prácticas de seguridad en la selección y uso de las contraseñas.

#### 7.3.2. Equipo de usuario desatendido

Los usuarios deberán asegurarse de que el equipo desatendido tiene la protección adecuada.

#### 7.3.3. Política de puesto de trabajo despejado y pantalla limpia

Deberá adoptarse una política de puesto de trabajo despejado de papeles y de medios de almacenamiento extraíbles junto con una política de pantalla limpia para los recursos de tratamiento de la información.

### 7.4. Control de acceso a la red

**Objetivo:** Prevenir el acceso no autorizado a los servicios en red.

Se deberá controlar el acceso a los servicios en red, tanto internos como externos.

El acceso de usuarios a redes y a servicios en red no deberá comprometer la seguridad de los servicios en red, garantizando los siguientes aspectos:

- La colocación de interfaces adecuadas entre las redes de la organización y las redes de otras organizaciones o las redes públicas;
- Aplicación de mecanismos de autenticación adecuados tanto para los usuarios como para los equipos;
- Respecto de los controles de acceso de usuario a los servicios de información.



|                                                                                                                                                                  |                                                                      |                                 |                                             |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------|---------------------------------|---------------------------------------------|
|  <b>GOBIERNO DE MÉXICO</b>   <b>SALUD</b><br><small>SECRETARÍA DE SALUD</small> | GUIA DE INTERCAMBIO DE INFORMACIÓN EN SALUD PARA UN<br>SGSI EN SALUD |                                 |                                             |
|                                                                                                                                                                  | CLAVE DEL DOCUMENTO:<br>GIIS-A004-01-07                              | VERSIÓN DEL DOCUMENTO:<br>01.07 | FECHA DEL DOCUMENTO:<br>07 de junio de 2013 |

#### **7.4.1. Política de uso de los servicios en red**

Se deberá proporcionar a los usuarios únicamente el acceso a los servicios para los que hayan sido específicamente autorizados.

#### **7.4.2. Autenticación de usuario para conexiones externas**

Se deberán utilizar los métodos apropiados de autenticación para controlar el acceso de los usuarios remotos.

#### **7.4.3. Identificación de los equipos en las redes**

La identificación automática de los equipos se deberá considerar como un medio de autenticación de las conexiones provenientes de localizaciones y equipos específicos.

#### **7.4.4. Protección de los puertos de diagnóstico remoto y protección de los puertos de configuración**

Se deberá controlar el acceso físico y lógico a los puertos de diagnóstico y de configuración.

#### **7.4.5. Segregación de las redes**

Los grupos de servicios de información, usuarios y sistemas de información deberán estar segregados en redes.

#### **7.4.6. Control de la conexión a la red**

En redes compartidas, especialmente en aquellas que traspasen las fronteras de la organización, deberá restringirse la capacidad de los usuarios para conectarse a la red, esto deberá hacerse de acuerdo a la política de control de acceso y a los requisitos de las aplicaciones de Salud.

#### **7.4.7. Control de enrutamiento (routing) de red**

Se deberán implantar controles de enrutamiento (routing) de redes para asegurar que las conexiones de las computadoras y los flujos de información no violan la política de control de acceso de las aplicaciones de la organización.

### **7.5. Control de acceso al sistema operativo**

**Objetivo:** Prevenir el acceso no autorizado a los sistemas operativos.

Se deberán utilizar recursos de seguridad para restringir el acceso de usuarios autorizados a los sistemas operativos. Los recursos deberán ser capaces de lo siguiente:



|                                                                                                                                                                   |                                                                      |                                 |                                             |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------|---------------------------------|---------------------------------------------|
|  <b>GOBIERNO DE MÉXICO</b><br><b>SALUD</b><br><small>SECRETARÍA DE SALUD</small> | GUIA DE INTERCAMBIO DE INFORMACIÓN EN SALUD PARA UN<br>SGSI EN SALUD |                                 |                                             |
|                                                                                                                                                                   | CLAVE DEL DOCUMENTO:<br>GIIS-A004-01-07                              | VERSIÓN DEL DOCUMENTO:<br>01.07 | FECHA DEL DOCUMENTO:<br>07 de junio de 2013 |

- a) Autenticar a los usuarios autorizados, de acuerdo a una política de control de acceso definida;
- b) Registrar los intentos exitosos y fallidos de autenticación del sistema;
- c) Registrar el uso de sistemas especiales de privilegios;
- d) Disparar alarmas cuando se infrinjan las políticas de seguridad;
- e) Proporcionar los medios adecuados de autenticación;
- f) Cuando sea apropiado, restringir el tiempo de conexión a los usuarios.

### 7.5.1. Procedimientos seguros de inicio de sesión

El acceso a los sistemas operativos se deberá controlar por medio de un procedimiento seguro de inicio de sesión.

### 7.5.2. Identificación y autenticación de usuario

Todos los usuarios deberán tener un identificador único (ID de usuario), para su uso personal y exclusivo, y se deberá elegir una técnica adecuada de autenticación para confirmar la identidad solicitada del usuario.

### 7.5.3. Sistema de gestión de contraseñas

Los sistemas para la gestión de contraseñas deberán ser interactivos y establecer contraseñas de calidad.

### 7.5.4. Uso de los recursos del sistema

Se deberá restringir y controlar de una manera rigurosa el uso de programas y utilidades que puedan ser capaces de invalidar los controles del sistema y de la aplicación.

### 7.5.5. Desconexión automática de sesión

Las sesiones inactivas deberán cerrarse después de un periodo de inactividad definido.

### 7.5.6. Limitación del tiempo de conexión

Para proporcionar seguridad adicional a las aplicaciones de alto riesgo, se deberán utilizar restricciones en los tiempos de conexión.

## 7.6. Control de acceso a las aplicaciones y a la información

**Objetivo** Prevenir el acceso no autorizado a la información que contienen las aplicaciones.

Se deberá utilizar recursos de seguridad para restringir el acceso a y dentro de los sistemas de aplicación.



|                                                                                                                                                                  |                                                                          |                                        |                                                    |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------|----------------------------------------|----------------------------------------------------|
|  <b>GOBIERNO DE MÉXICO</b>   <b>SALUD</b><br><small>SECRETARÍA DE SALUD</small> | <b>GUÍA DE INTERCAMBIO DE INFORMACIÓN EN SALUD PARA UN SGSI EN SALUD</b> |                                        |                                                    |
|                                                                                                                                                                  | <b>CLAVE DEL DOCUMENTO:</b><br>GIIS-A004-01-07                           | <b>VERSIÓN DEL DOCUMENTO:</b><br>01.07 | <b>FECHA DEL DOCUMENTO:</b><br>07 de junio de 2013 |

El acceso lógico a las aplicaciones de software y a la información deberá estar restringido a los usuarios autorizados, los SIRES deberán:

- Controlar el acceso del usuario a la información y a las funciones del sistema de aplicación, de acuerdo con una política de control de acceso definida;
- Proporcionar protección contra el acceso no autorizado a través de cualquier recurso, contra el software del sistema operativo, y el software malicioso que es capaz de invalidar o evitar los controles del sistema o de la aplicación;

No comprometer otros sistemas con los que comparte recursos de información.

### 7.6.1. Restricción de acceso a la información

#### Control

Se deberá restringir el acceso a la información y a las aplicaciones a los usuarios y al personal de soporte, de acuerdo con la política de control de acceso definida.

Los sistemas de información que procesan información personal deberán autenticar usuarios y deberán hacerlo por autenticación involucrando al menos dos factores.

### 7.6.2. Aislamiento de sistemas sensibles

Los sistemas sensibles deberán tener un entorno dedicado (aislado) de computadoras.

## 7.7. Equipos de cómputo portátil y teletrabajo

**Objetivo:** Garantizar la seguridad de la información cuando se utilizan computadoras portátiles y servicios de teletrabajo.

La protección requerida deberá ser acorde con los riesgos específicos derivados de la forma de trabajo. Cuando se utilizan computadoras portátiles, deberán considerarse los riesgos del trabajo en un entorno no protegido, y aplicar la protección adecuada. En el caso del teletrabajo, la organización deberá aplicar una protección al lugar desde el que se realiza esta actividad y asegurarse de que han sido implantadas las disposiciones adecuadas para esta forma de trabajo.

### 7.7.1. Equipos de cómputo portátil y comunicaciones móviles

Se deberá implantar una política formal y se deberán adoptar las medidas de seguridad adecuadas para la protección contra los riesgos de la utilización de computadoras portátiles y comunicaciones móviles.

Las organizaciones que procesan información personal de salud deberán:



|                                                                                                                                                                   |                                                                          |                                        |                                                    |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------|----------------------------------------|----------------------------------------------------|
|  <b>GOBIERNO DE MÉXICO</b><br><b>SALUD</b><br><small>SECRETARÍA DE SALUD</small> | <b>GUÍA DE INTERCAMBIO DE INFORMACIÓN EN SALUD PARA UN SGSI EN SALUD</b> |                                        |                                                    |
|                                                                                                                                                                   | <b>CLAVE DEL DOCUMENTO:</b><br>GIIIS-A004-01-07                          | <b>VERSIÓN DEL DOCUMENTO:</b><br>01.07 | <b>FECHA DEL DOCUMENTO:</b><br>07 de junio de 2013 |

- Evaluar específicamente los riesgos involucrados en equipos de cómputo portátil utilizados en el ámbito de la salud;
- Preparar una política sobre las precauciones a ser tomadas cuando se utilizan dispositivos de equipos de cómputo portátil, incluyendo dispositivos inalámbricos;
- Solicitar a los usuarios de equipos portátiles a seguir esta política.

### 7.7.2. Teletrabajo

Se deberán redactar e implantar, una política de actividades de teletrabajo, así como los planes y procedimientos de operación correspondientes.

## 8. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN

### 8.1. Requisitos de seguridad de los sistemas de información

**Objetivo:** Garantizar que la seguridad está integrada en los sistemas de información.

Los sistemas de información abarcan los sistemas operativos, la infraestructura, las aplicaciones de la organización, los productos disponibles en el mercado, los servicios y las aplicaciones desarrolladas por el usuario. Las fases de diseño y de implantación del SIRES que da soporte a los procesos de negocios pueden resultar cruciales para la seguridad. Los requisitos de seguridad deberán ser identificados y acordados antes de desarrollar o implantar los SIRES.

Durante la fase de requisitos de un proyecto, todos los requisitos de seguridad deberán identificarse, justificarse, acordarse y documentarse como parte de las necesidades globales del negocio dentro de un sistema de información.

#### 8.1.1. Análisis y especificación de los requisitos de seguridad

En las declaraciones de los requisitos de negocio para los nuevos sistemas de información, o para mejoras de los sistemas de información ya existentes, se deberán especificar los requisitos de los controles de seguridad.

### 8.2. Procesamiento correcto en aplicaciones

**Objetivo:** Evitar errores, pérdidas, modificaciones no autorizadas o usos indebidos de la información en las aplicaciones.

Deberán diseñarse controles adecuados en las aplicaciones, incluyendo las desarrolladas por el usuario, para garantizar un correcto tratamiento. Estos controles deberán incluir la validación de los datos introducidos, el procesamiento interno y los datos resultantes.



|                                                                                                                                                                  |                                                                          |                                        |                                                    |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------|----------------------------------------|----------------------------------------------------|
|  <b>GOBIERNO DE MÉXICO</b>   <b>SALUD</b><br><small>SECRETARÍA DE SALUD</small> | <b>GUIA DE INTERCAMBIO DE INFORMACIÓN EN SALUD PARA UN SGSI EN SALUD</b> |                                        |                                                    |
|                                                                                                                                                                  | <b>CLAVE DEL DOCUMENTO:</b><br>GIIIS-A004-01-07                          | <b>VERSIÓN DEL DOCUMENTO:</b><br>01.07 | <b>FECHA DEL DOCUMENTO:</b><br>07 de junio de 2013 |

En los sistemas que procesen o afecten a información sensible, valiosa o crítica, puede ser necesario implantar controles adicionales. Dichos controles deberán determinarse en función de los requisitos de seguridad y de la evaluación de riesgos.

### 8.2.1. Identificación única de sujetos de atención

#### Control

Sistemas que procesan información personal de salud deberán:

- Asegurar que cada sujeto de atención sea identificado de manera única en el sistema;
- Ser capaz de fusionar información duplicada o registros duplicados si es determinado que múltiples registros de un mismo sujeto de atención han sido creados de manera no intencional o durante una emergencia médica.

### 8.2.2. Validación de los datos de entrada

La introducción de datos en las aplicaciones deberá validarse para garantizar que dichos datos son correctos y adecuados.

### 8.2.3. Control de procesamiento interno

Para detectar cualquier corrupción de la información debida a errores de procesamiento o actos intencionados, se deberán incorporar comprobaciones de validación en las aplicaciones.

### 8.2.4. Integridad de los mensajes

Se deberán identificar los requisitos para garantizar la autenticidad y para proteger la integridad de los mensajes en las aplicaciones y se deberán identificar e implantar los controles adecuados.

### 8.2.5. Validación de los datos de salida

#### Control

Los datos de salida de una aplicación se deberán validar para garantizar que el tratamiento de la información almacenada es correcto y adecuado a las circunstancias.

Los sistemas que procesan información personal de salud deberán proveer información de identificación que asista a profesionales de salud en confirmar que el registro electrónico de salud coincida con el sujeto de atención bajo tratamiento.



|                                                                                                                                                                   |                                                                      |                                 |                                             |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------|---------------------------------|---------------------------------------------|
|  <b>GOBIERNO DE MÉXICO</b><br><b>SALUD</b><br><small>SECRETARÍA DE SALUD</small> | GUIA DE INTERCAMBIO DE INFORMACIÓN EN SALUD PARA UN<br>SGSI EN SALUD |                                 |                                             |
|                                                                                                                                                                   | CLAVE DEL DOCUMENTO:<br>GIIS-A004-01-07                              | VERSIÓN DEL DOCUMENTO:<br>01.07 | FECHA DEL DOCUMENTO:<br>07 de junio de 2013 |

### 8.3. Controles criptográficos

**Objetivo:** Proteger la confidencialidad, la autenticidad o la integridad de la información por medios criptográficos.

Deberá desarrollarse una política acerca del uso de controles criptográficos. Deberá existir una gestión de las claves que de soporte al uso de técnicas criptográficas.

#### 8.3.1. Política de uso de los controles criptográficos y gestión de claves

Se deberán formular e implantar una política para el uso de controles criptográficos para proteger la información.

#### 8.3.2. Gestión de claves

Deberá implantarse un sistema de gestión de llaves para dar soporte al uso de técnicas criptográficas por parte de la organización.

### 8.4. Seguridad de los archivos de sistema

**Objetivo:** Garantizar la seguridad de los archivos de sistema.

Deberá controlarse el acceso a los archivos de sistema y al código fuente de los programas, y los proyectos de TI y sus actividades de apoyo deberán llevarse a cabo de forma segura. Deberá tenerse cuidado para evitar la exposición de datos sensibles en entornos de prueba.

#### 8.4.1. Control del software en explotación

Deberán estar implantados procedimientos para controlar la instalación de software en los sistemas en producción.

#### 8.4.2. Protección de los datos de prueba del sistema

Los datos de prueba se deberán seleccionar cuidadosamente y deberán estar protegidos y controlados.

#### 8.4.3. Control de acceso al código fuente de los programas

Se deberá restringir el acceso al código fuente de los programas.



|                                                                                                                                                                   |                                                                      |                                 |                                             |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------|---------------------------------|---------------------------------------------|
|  <b>GOBIERNO DE MÉXICO</b><br><b>SALUD</b><br><small>SECRETARÍA DE SALUD</small> | GUÍA DE INTERCAMBIO DE INFORMACIÓN EN SALUD PARA UN<br>SGSI EN SALUD |                                 |                                             |
|                                                                                                                                                                   | CLAVE DEL DOCUMENTO:<br>GIIS-A004-01-07                              | VERSIÓN DEL DOCUMENTO:<br>01.07 | FECHA DEL DOCUMENTO:<br>07 de junio de 2013 |

## 8.5. Seguridad en los procesos de desarrollo y soporte

**Objetivo:** Mantener la seguridad del software y de la información de las aplicaciones.

Los entornos de proyecto y de asistencia técnica deberán estar estrictamente controlados.

Los directores responsables de los sistemas de aplicación también deberán responsabilizarse de la seguridad del entorno del proyecto o de asistencia técnica. Deberán asegurarse de que todas las modificaciones del sistema propuestas se revisan para comprobar que no ponen en peligro la seguridad del sistema o del entorno operativo.

### 8.5.1. Procedimiento de control de cambios

La implementación de cambios deberá controlarse mediante el uso de procedimientos formales de control de cambios.

### 8.5.2. Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo

Cuando se modifiquen los sistemas operativos, las aplicaciones críticas de la organización deberán ser revisadas y probadas para garantizar que no existen efectos adversos en las operaciones o en la seguridad de la organización.

### 8.5.3. Restricciones a los cambios en los paquetes de software

Se deberán evitar las modificaciones en los paquetes de software, limitándose a los cambios necesarios, y todos los cambios deberán ser objeto de un control riguroso.

### 8.5.4. Fugas de información

Deberán evitarse las situaciones que permitan que se produzcan fugas de información.

### 8.5.5. Externalización del desarrollo de software

La externalización del desarrollo de software deberá ser supervisada y controlada por la organización.

## 8.6. Gestión de las vulnerabilidades técnicas

**Objetivo:** Reducir los riesgos resultantes de la explotación de las vulnerabilidades técnicas publicadas.

La gestión de la vulnerabilidad técnica deberá implantarse de forma efectiva, sistemática y repetitiva y deberán adoptarse medidas que confirmen su efectividad. Estas consideraciones deberán incluir los sistemas operativos y cualquier otra aplicación que se esté usando.





|                                                                                                                                                                   |                                                                   |                                 |                                             |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------|---------------------------------|---------------------------------------------|
|  <b>GOBIERNO DE MÉXICO</b><br><b>SALUD</b><br><small>SECRETARÍA DE SALUD</small> | GUÍA DE INTERCAMBIO DE INFORMACIÓN EN SALUD PARA UN SGSI EN SALUD |                                 |                                             |
|                                                                                                                                                                   | CLAVE DEL DOCUMENTO:<br>GIIS-A004-01-07                           | VERSIÓN DEL DOCUMENTO:<br>01.07 | FECHA DEL DOCUMENTO:<br>07 de junio de 2013 |

### 8.6.1. Control de las vulnerabilidades técnicas

Se deberá obtener la información adecuada acerca de las vulnerabilidades técnicas de los sistemas de información que están siendo utilizados, evaluar la exposición de la organización a dichas vulnerabilidades y adoptar las medidas adecuadas para afrontar el riesgo asociado.

## 9. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN

### 9.1. Notificación de eventos y puntos débiles de seguridad de la información

**Objetivo:** Asegurarse de que los eventos de seguridad de la información y las debilidades asociadas con los sistemas de información, se comunican de manera que sea posible emprender las acciones correctivas oportunas.

Deberán existir procedimientos formales de comunicación de eventos en forma escalada. Todos los trabajadores, contratistas y terceros deberán conocer los procedimientos de comunicación de los diferentes tipos de eventos y puntos débiles que pueden afectar a la seguridad de los activos de la organización. Se les deberá requerir que comunicaran al contacto designado cualquier evento o punto débil de seguridad de la información lo antes posible.

#### 9.1.1. Notificación de eventos de seguridad de la información

Los eventos de seguridad de la información se deberán notificar a través de los canales adecuados de gestión lo antes posible.

#### 9.1.2. Notificación de puntos débiles de seguridad

Todos los empleados, contratistas y terceros que sean usuarios de los sistemas y servicios de información deberán estar obligados a anotar y notificar cualquier punto débil que observen o que sospechen exista, en dichos sistemas o servicios.

### 9.2. Gestión de incidentes y mejoras de seguridad de la información

**Objetivo:** Garantizar que se aplica un enfoque coherente y efectivo a la gestión de los incidentes de seguridad de la información.

Deberán existir responsabilidades y procedimientos para tratar los incidentes y los puntos débiles de seguridad de la información de forma efectiva una vez que se hayan comunicado.



|                                                                                                                                                                  |                                                                      |                                 |                                             |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------|---------------------------------|---------------------------------------------|
|  <b>GOBIERNO DE MÉXICO</b>   <b>SALUD</b><br><small>SECRETARÍA DE SALUD</small> | GUIA DE INTERCAMBIO DE INFORMACIÓN EN SALUD PARA UN<br>SGSI EN SALUD |                                 |                                             |
|                                                                                                                                                                  | CLAVE DEL DOCUMENTO:<br>GIIIS-A004-01-07                             | VERSIÓN DEL DOCUMENTO:<br>01.07 | FECHA DEL DOCUMENTO:<br>07 de junio de 2013 |

Deberá aplicarse un proceso de mejora continua a la reacción, la supervisión, la evaluación y la gestión general de los incidentes de seguridad de la información.

Cuando sean necesarias pruebas, éstas deberán recopilarse para garantizar el cumplimiento de los requisitos legales.

### 9.2.1. Responsabilidades y procedimientos

Se deberán establecer las responsabilidades y procedimientos de gestión para garantizar una respuesta rápida, efectiva y ordenada a los incidentes de seguridad de la información.

### 9.2.2. Aprendizaje de los incidentes

Deberán existir mecanismos que permitan cuantificar y supervisar los tipos, volúmenes y costos de los incidentes de seguridad de la información.

### 9.2.3. Recopilación de evidencias

Cuando se emprenda una acción contra una persona u organización, después de un incidente de seguridad de la información, que implique acciones legales (tanto civiles como penales), deberán recopilarse las evidencias, conservarse y presentarse conforme a las normas y regulaciones establecidas en la jurisdicción correspondiente.

## 10. GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

### 10.1. Aspectos de la Seguridad de la Información en la Gestión de la Continuidad del Negocio

**Objetivo:** Contrarrestar las interrupciones de las actividades de la organización y proteger los procesos críticos de negocio de los efectos derivados de fallos importantes o catastróficos de los sistemas de información, así como garantizar su oportuna reanudación.

Deberá implantarse un proceso de gestión de la continuidad del negocio para minimizar los efectos sobre la organización y poder recuperarse de pérdidas de activos de información (como resultado, por ejemplo, de desastres naturales, accidentes, fallos de los equipos y acciones intencionadas), hasta un nivel aceptable mediante una combinación de controles preventivos y de recuperación. Este proceso deberá identificar los procesos críticos de negocio e integrar los requisitos de gestión de la seguridad de la información para la continuidad de negocio con otros requisitos de continuidad relacionados con aspectos tales como las actividades, el personal, los materiales, el transporte y las instalaciones.



|                                                                                                                                                                   |                                                                          |                                        |                                                    |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------|----------------------------------------|----------------------------------------------------|
|  <b>GOBIERNO DE MÉXICO</b><br><b>SALUD</b><br><small>SECRETARÍA DE SALUD</small> | <b>GUIA DE INTERCAMBIO DE INFORMACIÓN EN SALUD PARA UN SGSI EN SALUD</b> |                                        |                                                    |
|                                                                                                                                                                   | <b>CLAVE DEL DOCUMENTO:</b><br>GIIIS-A004-01-07                          | <b>VERSIÓN DEL DOCUMENTO:</b><br>01.07 | <b>FECHA DEL DOCUMENTO:</b><br>07 de junio de 2013 |

Las consecuencias de los desastres, fallos de seguridad, pérdidas del servicio y disponibilidad del servicio deberán estar sometidas a un análisis de efectos sobre el negocio. Deberán desarrollarse e implantarse planes de continuidad de negocio para garantizar una reanudación adecuada de las actividades fundamentales. La seguridad de la información deberá ser una parte integrada en el proceso general de continuidad del negocio y de otros procesos de gestión dentro de la organización.

La gestión de la continuidad del negocio deberá incluir controles para identificar y reducir los riesgos, además del proceso general de evaluación de riesgos, limitar las consecuencias de incidentes dañinos y garantizar que la información necesaria para los procesos del negocio está disponible.

### **10.1.1. Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio**

Deberán desarrollarse y mantenerse un proceso para la continuidad del negocio en toda la organización, que gestione los requisitos de seguridad de la información necesarios para la continuidad del negocio.

### **10.1.2. Continuidad del negocio y evaluación de riesgos**

Deberán identificarse los eventos que pueden causar interrupciones en los procesos de negocio, así como la probabilidad de que se produzcan tales interrupciones, sus efectos y sus consecuencias para la seguridad de la información.

### **10.1.3. Desarrollo e implantación de planes de continuidad que incluyan la seguridad de la información**

Deberán desarrollarse e implantarse planes para mantener o restaurar las operaciones y garantizar la disponibilidad de la información en el nivel y en el tiempo requerido, después de una interrupción o una falla de los procesos críticos de negocio.

### **10.1.4. Marco de referencia para la planificación de la continuidad del negocio**

Deberá mantenerse un único marco de referencia para los planes de continuidad del negocio, para asegurar que todos los planes sean coherentes, para cumplir los requisitos de seguridad de la información de manera consistente y para identificar las prioridades de realización de pruebas y mantenimiento.

### **10.1.5. Pruebas, mantenimiento y reevaluación de los planes de continuidad del negocio**

Los planes de continuidad del negocio deberán probarse y actualizarse periódicamente para asegurar que están al día y que son efectivos.



|                                                                                                                                                                   |                                                                      |                                 |                                             |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------|---------------------------------|---------------------------------------------|
|  <b>GOBIERNO DE MÉXICO</b><br><b>SALUD</b><br><small>SECRETARÍA DE SALUD</small> | GUIA DE INTERCAMBIO DE INFORMACIÓN EN SALUD PARA UN<br>SGSI EN SALUD |                                 |                                             |
|                                                                                                                                                                   | CLAVE DEL DOCUMENTO:<br>GIIIS-A004-01-07                             | VERSIÓN DEL DOCUMENTO:<br>01.07 | FECHA DEL DOCUMENTO:<br>07 de junio de 2013 |

## 11. CUMPLIMIENTO

### 11.1. Cumplimiento de los requisitos legales

**Objetivo:** Evitar incumplimientos de las leyes o de las obligaciones legales, reglamentarias o contractuales y de los requisitos de seguridad.

El diseño, funcionamiento, uso y la gestión de los SIREs pueden estar sujetos a requisitos legales, reglamentarios y contractuales de seguridad. Deberá consultarse a los asesores legales de la organización o a abogados adecuadamente cualificados acerca de los requisitos legales específicos. Los requisitos legales pueden ser diferentes en cada país e incluso por Entidad Federativa, y puede ser diferente para la información creada en una determinada ubicación y que se transmite a otra (es decir, transfronterizo de datos).

#### 11.1.1. Identificación de la legislación aplicable

Todos los requisitos pertinentes, tanto legales como reglamentarios o contractuales, y el enfoque de la organización para cumplir dichos requisitos, deben estar definidos, documentados y mantenerse actualizados de forma explícita para cada sistema de información de la organización.

#### 11.1.2. Derechos de propiedad intelectual (IPR)

Deberán implementarse procedimientos adecuados para garantizar el cumplimiento de los requisitos legales, reglamentarios y contractuales sobre el uso de material, con respecto al cual pueden existir derechos de propiedad intelectual y sobre el uso de productos de software propietario.

#### 11.1.3. Protección de los documentos de organización

Los documentos importantes deberán estar protegidos contra la pérdida, destrucción y clasificación de acuerdo con los requisitos legales, reglamentarios, contractuales de la organización.

#### 11.1.4. Protección de datos y privacidad de la información de carácter personal

##### Control

Debe garantizarse la protección y la privacidad de los datos según se requiera en la legislación y la reglamentación aplicables y, en su caso, en las cláusulas contractuales pertinentes.

Las organizaciones que procesan información personal de salud deberán gestionar consentimientos informados por parte de los sujetos propietarios.



|                                                                                                                                                                  |                                                                      |                                 |                                             |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------|---------------------------------|---------------------------------------------|
|  <b>GOBIERNO DE MÉXICO</b>   <b>SALUD</b><br><small>SECRETARÍA DE SALUD</small> | GUIA DE INTERCAMBIO DE INFORMACIÓN EN SALUD PARA UN<br>SGSI EN SALUD |                                 |                                             |
|                                                                                                                                                                  | CLAVE DEL DOCUMENTO:<br>GIIIS-A004-01-07                             | VERSIÓN DEL DOCUMENTO:<br>01.07 | FECHA DEL DOCUMENTO:<br>07 de junio de 2013 |

Donde sea posible, los consentimientos informados de los sujetos propietarios y objetos de la atención médica, deberá ser obtenida antes de que la información personal de salud sea enviada por correo electrónico, enviada por fax o comunicada por conversación telefónica o divulgada de otra manera por partes externas a la organización de salud.

### **11.1.5. Prevención del uso indebido de recursos de tratamiento de la información y regulación de los controles criptográficos**

Se deberá disuadir a los usuarios de utilizar los recursos de tratamiento de la información para fines no autorizados.

### **11.1.6. Regulación de los controles criptográficos**

Los controles criptográficos se deben utilizar de acuerdo con todos los contratos, lineamientos, leyes y reglamentaciones pertinentes.

## **11.2. Cumplimiento de las políticas y normas de seguridad y cumplimiento técnico**

**Objetivo:** Asegurar que los SIRES cumplen las políticas y normas de seguridad de la organización.

La seguridad de los SIRES deberá revisarse periódicamente.

Dichas revisiones deberán realizarse mediante una comparación con políticas de seguridad adecuadas y deberá auditarse que las plataformas técnicas y los SIRES cumplan las normas de implantación de seguridad y los controles de seguridad documentados que resulten aplicables.

### **11.2.1. Cumplimiento de las políticas y normas de seguridad**

Los directores deberán asegurarse de que todos los procedimientos de seguridad dentro de su área de responsabilidad se cumplan.

### **11.2.2. Comprobación del cumplimiento técnico**

Deberá comprobarse periódicamente que los SIRES cumplen las normas de aplicación para la implantación.



|                                                                                                                                                                  |                                                                      |                                 |                                             |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------|---------------------------------|---------------------------------------------|
|  <b>GOBIERNO DE MÉXICO</b>   <b>SALUD</b><br><small>SECRETARÍA DE SALUD</small> | GUÍA DE INTERCAMBIO DE INFORMACIÓN EN SALUD PARA UN<br>SGSI EN SALUD |                                 |                                             |
|                                                                                                                                                                  | CLAVE DEL DOCUMENTO:<br>GIIS-A004-01-07                              | VERSIÓN DEL DOCUMENTO:<br>01.07 | FECHA DEL DOCUMENTO:<br>07 de junio de 2013 |

### 11.3. Consideraciones sobre las auditorías de los sistemas de información de salud

**Objetivo:** Maximizar la eficacia y reducir al mínimo la interferencia hacia o desde los sistemas en los procesos de auditoría.

#### 11.3.1. Controles de auditoría de los sistemas de información

Requisitos de auditoría y actividades que implican comprobaciones sobre sistemas en operación deberán ser planeadas para minimizar el riesgo a los procesos de Salud.

#### 11.3.2. Protección de las herramientas de auditoría de los sistemas de información

El acceso a las herramientas de auditoría de sistemas de información deberá estar protegido para evitar cualquier posible mal uso o compromiso.

