



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**

ANEXO B



 GOBIERNO DE MÉXICO	GUÍA DE INTERCAMBIO DE INFORMACIÓN EN SALUD PARA UN SGSI EN SALUD – ANEXO B		
SALUD SECRETARÍA DE SALUD	CLAVE DEL DOCUMENTO: GII-A004-SGSI- ANEXO-B	VERSIÓN DEL DOCUMENTO: 01.01	FECHA DEL DOCUMENTO: 07 de junio de 2013

CONTENIDO

Contenido	2
Recomendaciones para la implementación de controles de seguridad.	4
1. POLÍTICA DE SEGURIDAD	4
1.1. Política de Seguridad de la Información	4
2. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN	6
2.1. Organización interna	6
2.2. Terceros	7
3. GESTIÓN DE ACTIVOS	8
3.1. Responsabilidad sobre los activos en salud	8
3.2. Clasificación en la información en salud	9
4. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS	10
4.1. Antes del empleo	10
4.2. Durante el empleo	11
4.3. Cese de empleo o cambio de puesto de trabajo	12
5. SEGURIDAD FÍSICA Y DEL ENTORNO	13
5.1. Áreas seguras	13
5.2. Seguridad de los equipos	14
6. GESTIÓN DE CAMBIOS	15
6.1. Responsabilidades y procedimientos de operación	15
6.2. Gestión de la provisión de servicios por terceros	16
6.3. Planificación y aceptación del sistema	16
6.4. Protección contra el código malicioso y descargable	16
6.5. Copias de seguridad	16
6.6. Gestión de la seguridad de las redes	17
6.7. Manipulación de los medios	17
6.8. Intercambio de información	18
6.9. Servicios de comercio electrónico	19
6.10. Supervisión	19
7. CONTROL DE ACCESO	21
7.1. Requisitos de control de acceso en Salud	21
7.2. Gestión de acceso de usuario	21
7.3. Responsabilidades de usuario	22
7.4. Control de acceso a la red	22
7.5. Control de acceso al sistema operativo	23
7.6. Control de acceso a las aplicaciones y a la información	23



 GOBIERNO DE MÉXICO SALUD SECRETARÍA DE SALUD	GUÍA DE INTERCAMBIO DE INFORMACIÓN EN SALUD PARA UN SGSI EN SALUD – ANEXO B		
	CLAVE DEL DOCUMENTO: GII-A004-SGSI- ANEXO-B	VERSIÓN DEL DOCUMENTO: 01.01	FECHA DEL DOCUMENTO: 07 de junio de 2013

7.7.	Equipos de cómputo portátiles y teletrabajo	23
8.	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN	24
8.1.	Requisitos de seguridad de los sistemas de información	24
8.2.	Procesamiento correcto en aplicaciones	24
8.3.	Controles criptográficos	25
8.4.	Seguridad de los archivos de sistema	25
8.5.	Seguridad en los procesos de desarrollo y soporte	26
8.6.	Gestión de la vulnerabilidad técnica	26
9.	GESTIÓN DE INCIDENTES DE LA SEGURIDAD DE LA INFORMACIÓN	26
9.1.	Notificación de eventos y puntos débiles de seguridad de la información	26
9.2.	Gestión de incidentes y mejoras de seguridad de la información	27
10.	GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	27
10.1.	Aspectos de la Seguridad de la Información en la Gestión de la Continuidad del Negocio	27
11.	CUMPLIMIENTO	29
11.1.	Cumplimiento de los requisitos legales	29
11.2.	Cumplimiento de las políticas y normas de seguridad y cumplimiento técnico	30
11.3.	Consideraciones sobre las auditorías de los sistemas de información	30



 GOBIERNO DE MÉXICO SALUD SECRETARÍA DE SALUD	GUIA DE INTERCAMBIO DE INFORMACIÓN EN SALUD PARA UN SGSI EN SALUD – ANEXO B		
	CLAVE DEL DOCUMENTO: GII-A004-SGSI- ANEXO-B	VERSIÓN DEL DOCUMENTO: 01.01	FECHA DEL DOCUMENTO: 07 de junio de 2013

RECOMENDACIONES PARA LA IMPLEMENTACIÓN DE CONTROLES DE SEGURIDAD

El presente documento contiene una serie de recomendaciones y lineamientos que los prestadores de servicios de salud opcionalmente podrán observar para la implementación de los controles establecidos en el apartado “Verificación de apego a esta Guía y Formatos”.

Existen objetivos y controles de seguridad para los cuales en el presente documento no se incluyen recomendaciones o lineamientos, esto no se exime al prestador de servicios de salud de la implementación de los controles correspondientes.

Es responsabilidad de los prestadores de servicios de salud la implementación de todos aquellos controles que le apliquen de acuerdo a la “Declaración de Aplicabilidad” (GIIS-A004-SGSI-ANEXO-A) y los términos que se definan al interior de su organización en cuanto al Sistema de Gestión de la Seguridad se refiere.

Existen Lineamientos y Recomendaciones que aplican para más de un control de seguridad, en este caso, los controles serán agrupados. Ejemplo: 5.1.2, 5.1.3, 5.1.4 y 5.1.5.

A continuación se presentan los lineamientos y recomendaciones para la implementación de los controles de seguridad.

1. POLÍTICA DE SEGURIDAD

1.1. Política de seguridad de la información

1.1.1. Documento de política de seguridad de la información

Esta política deberá contener declaraciones sobre:

- La necesidad de seguridad de la información de salud;
- Los objetivos de seguridad de la información de salud;
- Alcance de cumplimiento;
- Requisitos legales, reglamentarios y contractuales, incluidas las relativas a la protección personal de información personal de salud y las responsabilidades legales y éticas de los profesionales de salud para proteger esta información;
- Disposiciones para la notificación de incidentes de seguridad de la información, incluyendo un canal para levantar preocupaciones respecto a la confidencialidad, y sin temor a la culpa o recriminación.



 GOBIERNO DE MÉXICO SALUD SECRETARÍA DE SALUD	GUÍA DE INTERCAMBIO DE INFORMACIÓN EN SALUD PARA UN SGSI EN SALUD – ANEXO B		
	CLAVE DEL DOCUMENTO: GII-A004-SGSI-ANEXO-B	VERSIÓN DEL DOCUMENTO: 01.01	FECHA DEL DOCUMENTO: 07 de junio de 2013

En la creación del documento de política de seguridad de la información, las organizaciones de salud deberán considerar específicamente los siguientes factores, que son únicas al sector salud:

- a) La amplitud de la información de salud;
- b) Los derechos y las responsabilidades éticas del personal, según lo acordado en la ley, y aceptadas por los miembros de colegios de profesionales;
- c) Los derechos de los sujetos de atención, donde aplique, a la privacidad y el acceso a sus registros;
- d) Las obligaciones de médicos con respecto al consentimiento de obtener información de sujetos de atención y mantener la confidencialidad de la información personal de salud;
- e) Las necesidades legítimas de médicos y organizaciones de salud que sean capaces de superar los protocolos normales de seguridad cuando las prioridades de salud, a menudo involucrados a la incapacidad de ciertos temas de cuidado de expresar sus preferencias, requieren esas anulaciones, también los procedimientos a emplear para lograr esto;
- f) Las obligaciones de las respectivas organizaciones de salud, y de sus sujetos de atención, donde los servicios de salud son entregados en un “cuidado compartido” o “extensión de cuidados básicos”;
- g) Los protocolos y procedimientos a ser aplicados para compartir información para los propósitos de investigación y ensayos médicos;
- h) Las medidas adoptadas y los límites de la autoridad, empleados temporales, tales como estudiantes o personal de guardia;
- i) Las medidas adoptadas y las limitaciones impuestas al acceso a la información médica personal por los voluntarios y el personal de apoyo, como el clero y personal de caridad.

Muchas organizaciones de salud han encontrado que es ventajoso hacer el documento de la política disponible electrónicamente para el personal a través de un área de seguridad de la información en la intranet de la organización.

Cuando la organización de salud obtiene apoyo de terceros o colabora con terceros y especialmente donde recibe servicios de otras jurisdicciones, el marco de la política deberá incluir una política documentada, controles y procedimientos que cubran estas interacciones y que especifican las responsabilidades de todas las partes. En los casos en que los datos personales cruzan las fronteras nacionales o jurisdiccionales, las disposiciones del ISO 22857 deberán ser aplicadas.



 GOBIERNO DE MÉXICO SALUD SECRETARÍA DE SALUD		GUIA DE INTERCAMBIO DE INFORMACIÓN EN SALUD PARA UN SGSI EN SALUD – ANEXO B	
CLAVE DEL DOCUMENTO: GII-A004-SGSI-ANEXO-B		VERSIÓN DEL DOCUMENTO: 01.01	FECHA DEL DOCUMENTO: 07 de junio de 2013

1.1.2. Revisión de la política de seguridad de la información

Lineamientos de implementación

La revisión deberá abordar:

- La naturaleza cambiante de las operaciones de la organización de salud y los cambios concomitantes al perfil de riesgo y las necesidades de gestión de riesgo;
- Los cambios realizados en la infraestructura de TI de la organización y los cambios concomitantes traen al perfil de riesgo de la organización;
- Los cambios identificados en el entorno que afecta de manera similar el perfil de riesgo de la organización;
- Los últimos controles, los requisitos de cumplimiento, la garantía y los acuerdo por mandato jurisdiccional de los organismos de salud o por una nueva legislación o reglamento;
- Las ultimas orientaciones y las recomendaciones de las asociaciones de profesionales de la salud y de la información, comisionados de privacidad con respecto a la protección de la información personal de salud;
- Los resultados de los casos legales en los tribunales, que han estado o negado precedentes o practicas establecidas;

2. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN

2.1.Organización interna

2.1.1. Compromiso de la dirección con la seguridad de la información

Lineamientos de implementación

Es importante tener en cuenta la naturaleza esencial de la responsabilidad de gestión en las organizaciones que son custodios de la información personal de salud.

La responsabilidad y coordinación pueden ser mantenidas en un largo plazo si las organizaciones tienen una gestión de infraestructura de seguridad de la información explícita.

Cualquiera que sea la estructura organizacional que se adopte, es de suma importancia que sea diseñada y estructurada para facilitar el acceso de los sujetos de atención (por ejemplo, para hacer peticiones para obtener información personal de salud), para facilitar la presentación de informes dentro de la estructura de la organización y para garantizar la entrega oportuna de la información.

Las organizaciones de salud deberán publicar ampliamente la declaración del alcance dentro de la organización, a continuación, revisar y asegurar que está adoptada por la información de la organización, médicos y grupos de gobierno corporativo.



 GOBIERNO DE MÉXICO SALUD SECRETARÍA DE SALUD	GUÍA DE INTERCAMBIO DE INFORMACIÓN EN SALUD PARA UN SGI EN SALUD – ANEXO B		
	CLAVE DEL DOCUMENTO: GII-A004-SGI- ANEXO-B	VERSIÓN DEL DOCUMENTO: 01.01	FECHA DEL DOCUMENTO: 07 de junio de 2013

2.1.2. Coordinación de la seguridad de la información

No existen recomendaciones por parte de la DGIS para la implementación de este control.

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

No existen recomendaciones por parte de la DGIS para la implementación de este control.

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

No existen recomendaciones por parte de la DGIS para la implementación de este control.

2.1.5. Acuerdos de confidencialidad

Lineamientos de implementación

El contrato mencionado anteriormente deberá incluir referencia a las faltas que son posibles cuando una brecha en la política de seguridad de la información es identificada.

2.1.6. Contacto con las autoridades

No existen recomendaciones por parte de la DGIS para la implementación de este control.

2.1.7. Contacto con grupos de especial interés

No existen recomendaciones por parte de la DGIS para la implementación de este control.

2.1.8. Revisión independiente de la seguridad de la información

No existen recomendaciones por parte de la DGIS para la implementación de este control.

2.2. Terceros

2.2.1. Identificación de los riesgos derivados del acceso de terceros

Lineamientos de implementación

La evaluación de riesgos es esencial para la efectiva gestión de acceso de terceros a los sistemas que contengan información de salud, especialmente información personal de salud. Los derechos de los sujetos de atención deben ser protegidos, aun cuando una parte externa con posibilidad de acceso a la información de salud se encuentra localizada en una jurisdicción diferente que el que rige al sujeto de atención o de la organización de salud.

2.2.2. Tratamiento de la seguridad en relación con los clientes

No existen recomendaciones por parte de la DGIS para la implementación de este control.



 GOBIERNO DE MÉXICO SALUD SECRETARÍA DE SALUD	GUIA DE INTERCAMBIO DE INFORMACIÓN EN SALUD PARA UN SGSI EN SALUD – ANEXO B		
	CLAVE DEL DOCUMENTO: GII-A004-SGSI- ANEXO-B	VERSIÓN DEL DOCUMENTO: 01.01	FECHA DEL DOCUMENTO: 07 de junio de 2013

2.2.3. Tratamiento de la seguridad en contrato con terceros

Lineamientos de implementación

Los requisitos antes descritos son destinados para asegurar la confidencialidad, integridad y disponibilidad de la información personal de salud sea mantenida como flujo de información más allá del control, directo de una organización de salud. Donde este flujo cruce fronteras jurisdiccionales, lineamientos adicionales pueden ser encontrados en ISO 22857.

Cuando un tercero no este procesando información personal de salud, un apropiado subconjunto de características del contrato antes descrito puede ser apropiado. En todos los casos de prestación de servicios de terceros, un contrato que especifique el conjunto mínimo de controles a ser aplicados deberá ser adoptado.

3. GESTIÓN DE ACTIVOS

3.1. Responsabilidad sobre los activos en Salud

3.1.1. Inventario de activos

No existen recomendaciones por parte de la DGIS para la implementación de este control.

3.1.2. Propiedad de los activos

No existen recomendaciones por parte de la DGIS para la implementación de este control.

3.1.3. Uso aceptable de los activos de Salud

Lineamientos de implementación

Las organizaciones que procesan información de salud deberán tener reglas de mantenimiento de los activos actuales (por ejemplo, la base de datos actual de drogas) y la integridad de estos activos (por ejemplo, la integridad funcional de dispositivos médicos que graban o reportan datos).

Los dispositivos médicos que graban o reportan datos requieren consideraciones especiales de seguridad en relación con el ambiente en el cual ellos operan y las emisiones electromagnéticas que ocurran durante su operación. Estos dispositivos deben ser identificados.



 GOBIERNO DE MÉXICO SALUD SECRETARÍA DE SALUD	GUÍA DE INTERCAMBIO DE INFORMACIÓN EN SALUD PARA UN SGSI EN SALUD – ANEXO B		
	CLAVE DEL DOCUMENTO: GII-A004-SGSI- ANEXO-B	VERSIÓN DEL DOCUMENTO: 01.01	FECHA DEL DOCUMENTO: 07 de junio de 2013

3.2. Clasificación en la información en Salud

3.2.1. Lineamientos de clasificación

Lineamientos de implementación

Determinar niveles de protección para información de los activos en salud es complejo y comparado con la clasificación de datos del gobierno o la malicia puede ser engañosa. Las siguientes características son importantes para la información de activos dentro de los cuidados de salud.

- La confidencialidad de la información personal de salud es a menudo muy subjetiva, más que objetiva. En otras palabras, últimamente, solo los sujetos de datos (por ejemplo, sujetos de atención) pueden hacer una determinación apropiada de la confidencialidad relativa de varios campos o grupos de datos. Por ejemplo, una persona que escapa de una relación abusiva podría considerar su nueva dirección y número telefónico que sea mucho más confidencial que los datos clínicos sobre la configuración de su brazo roto.
- La confidencialidad de la información personal de salud es contexto-dependiente. Por ejemplo, el nombre y dirección de un sujeto de atención en una lista de admisión al departamento de urgencias de un hospital podría no ser considerada especialmente confidencial por ese individuo, aun así, el mismo nombre y dirección en una lista de admisión de una clínica de tratamiento de impotencia sexual podría ser considerada altamente confidencial por el individuo.
- La confidencialidad de la información personal de salud puede cambiar sobre el tiempo de vida del registro de salud de un individuo. Por ejemplo, el cambio de las actitudes sociales en los últimos 20 años ha dado lugar en muchos sujetos de atención, no teniendo en cuenta su orientación sexual ya que es confidencial.

Debido a que no se puede predecir la sensibilidad de un determinado elemento de información personal de salud a través de todos sus usos y todas las fases de su ciclo de vida, toda información personal de salud deberá ser objeto de adecuado cuidado en todo momento.

Identificar y (en su caso) proteger el etiquetado de activos de información confidencial puede ser una herramienta importante en la información de personal y en el cumplimiento de las políticas. Esto funciona mejor cuando la clasificación actúa como un indicador de prácticas de manejo de la información solicitada. La clasificación también puede ser un componente de acuerdos de protección de datos entre las jurisdicciones y con organizaciones de terceros y su personal. Factor de tiempo en los procesos clínicos a menudo desempeñan un papel crucial en la determinación de los requisitos de disponibilidad de la información personal de salud. Clasificación respecto a la disponibilidad, integridad y criticidad también necesita ser aplicada a los procesos, dispositivos de TI, software, ubicaciones y personal. La criticidad deberá ser identificada a través de la evaluación de riesgos.



 GOBIERNO DE MÉXICO SALUD SECRETARÍA DE SALUD	GUIA DE INTERCAMBIO DE INFORMACIÓN EN SALUD PARA UN SGSI EN SALUD – ANEXO B		
	CLAVE DEL DOCUMENTO: GII-A004-SGSI- ANEXO-B	VERSIÓN DEL DOCUMENTO: 01.01	FECHA DEL DOCUMENTO: 07 de junio de 2013

3.2.2. Etiquetado y manipulado de la información

Lineamientos de implementación

No toda la información de salud es confidencial y no todos los sistemas de información de salud proveen acceso a los usuarios a la información personal de salud. Los usuarios de los sistemas de información de salud necesitan conocer cuando los datos que están accediendo contienen información personal de salud.

4. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS

4.1. Antes del empleo

4.1.1. Funciones y responsabilidades

Lineamientos de implementación

Las organizaciones cuyo personal está involucrado en el proceso de información personal de salud deberán documentar cada participación en una descripción relevante de trabajo. Funciones y responsabilidades de seguridad, tal como se establece en la política de seguridad de la información de la organización, también deberán ser documentadas en las descripciones de trabajo relevante.

Especial atención debe ser puesta sobre las funciones y responsabilidades del personal temporal o de corto plazo, tales como estudiantes, pasantes, etc.

4.1.2. Investigación de antecedentes

Lineamientos de implementación

Es importante saber cómo y dónde ponerse en contacto con el personal profesional de la salud, aunque como algunos miembros del personal médico se mueven en una base regular, detalles de la dirección pueden tener un valor limitado. Por lo tanto, las organizaciones de salud deberán considerar la colección de un número razonable de referencias y de otras formas de comprobación, por ejemplo, por los organismos profesionales e instituciones académicas.

Siempre que sea posible, deberán llevarse a cabo verificaciones de antecedentes penales.



 GOBIERNO DE MÉXICO SALUD SECRETARÍA DE SALUD	GUÍA DE INTERCAMBIO DE INFORMACIÓN EN SALUD PARA UN SGSI EN SALUD – ANEXO B		
	CLAVE DEL DOCUMENTO: GII-A004-SGSI- ANEXO-B	VERSIÓN DEL DOCUMENTO: 01.01	FECHA DEL DOCUMENTO: 07 de junio de 2013

4.1.3. Términos y condiciones de empleo

Lineamientos de implementación

Los términos y condiciones de empleo deberán:

- Incluir una referencia a las sanciones que son posibles cuando el incumplimiento de la política de seguridad de la información sea identificada;
- Asegurar que las condiciones relativas a la confidencialidad de información personal de salud sobrevivan la terminación del empleo a perpetuidad.

Con respecto al personal clínico, los términos y condiciones de empleo deberán especificar los derechos de acceso que dicho personal tendrá a los registros de los sujetos de atención y a los sistemas de información de salud asociados en caso de reclamaciones de terceros.

Si hubo una larga brecha entre el reclutamiento y la fecha de ingreso del empleado, se deberá considerar seriamente repetir el proceso de selección, o los elementos clave del mismo.

4.2. Durante el empleo

4.2.1. Responsabilidades de la Dirección

Lineamientos de implementación

Es importante notar el énfasis especial que tiene que ser puesto sobre las preocupaciones de los sujetos de atención de que no desean que su información personal de salud sea vista por los trabajadores de la salud tales como, colegas o parientes. Tales preocupaciones a menudo constituyen un porcentaje grande de quejas de aquellos con temores sobre la confidencialidad de su información personal de salud. De la misma manera, los empleados a menudo no desean ser colocados innecesariamente en la posición de revisar la información sobre amigos, parientes o vecinos de los sujetos de atención.

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

No existen recomendaciones por parte de la DGIS para la implementación de este control.



 GOBIERNO DE MÉXICO SALUD SECRETARÍA DE SALUD	GUÍA DE INTERCAMBIO DE INFORMACIÓN EN SALUD PARA UN SGSI EN SALUD – ANEXO B		
	CLAVE DEL DOCUMENTO: GII-A004-SGSI- ANEXO-B	VERSIÓN DEL DOCUMENTO: 01.01	FECHA DEL DOCUMENTO: 07 de junio de 2013

4.2.3. Proceso disciplinario

Lineamientos de implementación

Los procesos disciplinarios de las organizaciones de salud con respecto a las violaciones de seguridad de la información deberán seguir los procedimientos que son reflejados en la política y por lo tanto conocido por el sujeto(s) del proceso disciplinario. Además de cumplir con las reglas aplicables, como procesos, deberán cumplir con los acuerdos alcanzados entre profesionales de la salud y organizaciones profesionales de salud.

4.3. Cese de empleo o cambio de puesto de trabajo

4.3.1. Responsabilidad del cese o cambio

Lineamientos de implementación

Es importante tener en cuenta que, en el cuidado de la salud, existen diferentes tipos de empleados, por ejemplo, doctores, enfermeras, y otros donde sus derechos de acceso pueden cambiar fundamentalmente. Para garantizar la terminación de los derechos anteriores que ya no están siendo requeridos para su función, tales cambios de empleo deber ser procesados inicialmente en la misma forma que para las personas que están dejando el empleo de la organización.

4.3.2. Devolución de activos

No existen recomendaciones por parte de la DGIS para la implementación de este control.

4.3.3. Retirada de los derechos de acceso

Lineamientos de implementación

Es importante tener en cuenta de los estudiantes, internos, que han conservado sus privilegios de acceso después del cese de sus prácticas, etc. especialmente en los grandes hospitales un gran número de personal temporal típicamente tendrá acceso a corto plazo a la información personal de salud. La terminación de los derechos de acceso de dicho personal debe ser cuidadosamente gestionada. Al mismo tiempo, en los cuidados de salud, muchas de las transacciones se llevan a cabo bien después de la hora de la atención (por ejemplo, al cierre de sesión de transcripciones médicas). Esto puede complicar significativamente el proceso de quitar los derechos de acceso en una manera oportuna y estas transacciones deberán ser tenidas en cuenta diseñando y poniendo en práctica procedimientos sobre el retiro de derechos de acceso.



 GOBIERNO DE MÉXICO SALUD SECRETARÍA DE SALUD	GUIA DE INTERCAMBIO DE INFORMACIÓN EN SALUD PARA UN SGSI EN SALUD – ANEXO B		
	CLAVE DEL DOCUMENTO: GII-A004-SGSI- ANEXO-B	VERSIÓN DEL DOCUMENTO: 01.01	FECHA DEL DOCUMENTO: 07 de junio de 2013

Las organizaciones de salud deberán considerar seriamente la terminación inmediata de los derechos de acceso después del suministro de un aviso de dimisión, el aviso de despido, etc. en cualquier parte donde un riesgo aumentado sea percibido de la continuación de tal acceso.

5. SEGURIDAD FÍSICA Y DEL ENTORNO

5.1. Áreas seguras

5.1.1. Perímetro de seguridad física

Lineamientos de implementación

Es importante reconocer que, en muchas instalaciones de salud, la creación de instancias de los perímetros de seguridad es especialmente difícil. Muchas áreas operacionales son permeadas por los sujetos de atención. De hecho, no hay quizás ningún otro sector industrial donde el público tiene el acceso más extenso a áreas operacionales que en la salud. Al mismo tiempo un ambiente seguro tiene que ser mantenido para preservar la seguridad física y la seguridad de los sujetos de atención, así como los datos y sistemas que pueden ser accesibles dentro del entorno. A diferencia de los clientes de otros sectores industriales, los clientes en los cuidados de la salud son a menudo incapaces de físicamente asegurar su propia seguridad personal.

Las medidas de seguridad física para la información deberán ser coordinadas con seguridad física y las medidas de seguridad para los sujetos de atención. Las organizaciones de salud tienen la obligación de proteger a ambos.

5.1.2. Controles físicos de entrada; 5.1.3. Seguridad de oficinas, despachos e instalaciones; 5.1.4. Protección contra las amenazas externas y de origen ambiental; 5.1.5. Trabajo en áreas seguras

Lineamientos de implementación

Las organizaciones que procesan información personal de salud deberán tomar acciones sensibles para asegurar que solo personal autorizado a TI (servidores, dispositivos de almacenamiento, terminales y monitores) cumplan con limitaciones físicas de entrada.



 GOBIERNO DE MÉXICO SALUD SECRETARÍA DE SALUD	GUÍA DE INTERCAMBIO DE INFORMACIÓN EN SALUD PARA UN SGSI EN SALUD – ANEXO B		
CLAVE DEL DOCUMENTO: GII-A004-SGSI-ANEXO-B	VERSIÓN DEL DOCUMENTO: 01.01	FECHA DEL DOCUMENTO: 07 de junio de 2013	

5.1.6. Áreas de acceso público y de carga y descarga

Lineamientos de implementación

Es importante tener en cuenta que la prestación de la salud incluye distintas circunstancias donde el público (los sujetos de atención y acompañantes de apoyo) físicamente son admitidos en áreas grandes con grandes cantidades de información sensible (por ejemplo, pruebas de laboratorio donde el flujo de trabajo puede dictar la creciente información de sujetos de atención en la misma área donde los datos de los sujetos de atención previos están actualmente siendo procesados; áreas de tratamiento de salas de emergencia donde los acompañantes o parientes podrían potencialmente estar expuestos a cantidades significantes de información sensible verbal o visual de otros sujetos de atención, computadoras/estaciones de trabajo de enfermería localizadas cerca de las habitaciones de pacientes). Estas áreas físicas en la salud que reúnen información de salud a través de entrevistas y que contienen sistemas donde los datos son vistos en monitores deberán por lo tanto ser sujetos de evaluación adicional.

Para asegurar que la privacidad de los sujetos de atención sea mantenida, los cuidados de la salud a menudo requieren que las noticias sean publicadas en los ascensores, en las puertas detrás de las cuales las entrevistas puedan llevarse a cabo, como en otras áreas. Dichas notificaciones sirven como recordatorio para limitar la discusión de los casos de pacientes en las zonas comunes.

5.2. Seguridad de los equipos

5.2.1. Emplazamiento y protección de equipos

Lineamientos de implementación

Las organizaciones que procesan información personal de salud deberán situar las estaciones de trabajo que permitan el acceso a la información personal de salud de una manera que evite que personas no deseadas o sujetos de atención y el público vean o accedan.

Dispositivos médicos que graben o reporten datos también requieren consideraciones especiales de seguridad en relación al ambiente en el cuál ellos operan y las emisiones electromagnéticas que ocurran durante su operación.

Organizaciones de salud, especialmente hospitales, deberán asegurar que el emplazamiento y los lineamientos de protección para equipos de TI minimicen la exposición de tales emisiones.



 GOBIERNO DE MÉXICO SALUD SECRETARÍA DE SALUD	GUÍA DE INTERCAMBIO DE INFORMACIÓN EN SALUD PARA UN SGSI EN SALUD – ANEXO B		
	CLAVE DEL DOCUMENTO: GII-A004-SGSI- ANEXO-B	VERSIÓN DEL DOCUMENTO: 01.01	FECHA DEL DOCUMENTO: 07 de junio de 2013

5.2.2. Instalaciones de suministro; 5.2.3. Seguridad del cableado; 5.2.4. Mantenimiento de los equipos

Lineamientos de implementación

Las organizaciones de salud deberán dar consideraciones serias de protección de la red y otros cableados en áreas con alta emisión de dispositivos médicos.

5.2.5. Seguridad de los equipos fuera de las instalaciones

No existen recomendaciones por parte de la DGIS para la implementación de este control.

5.2.6. Reutilización o retirada segura de los equipos

No existen recomendaciones por parte de la DGIS para la implementación de este control.

5.2.7. Retirada de materiales propiedad de la organización

No existen recomendaciones por parte de la DGIS para la implementación de este control.

6. GESTIÓN DE CAMBIOS

6.1. Responsabilidades y procedimientos de operación

6.1.1. Documentación de los procedimientos de operación

No existen recomendaciones por parte de la DGIS para la implementación de este control.

6.1.2. Gestión de cambios

Lineamientos de implementación

Es importante notar que una prueba inapropiada, inadecuada o cambios incorrectos para el procesamiento de información personal de salud puede tener consecuencias que pongan en riesgo la seguridad del paciente. El proceso de cambio deberá explícitamente registrar y evaluar el riesgo del cambio.

6.1.3. Segregación de tareas

Lineamientos de implementación

Las organizaciones que procesan información personal de salud deberán en lo posible, separar funciones y áreas de responsabilidad con el fin de reducir oportunidades para la modificación no autorizada o mal uso de información personal de salud.



 GOBIERNO DE MÉXICO SALUD SECRETARÍA DE SALUD		GUIA DE INTERCAMBIO DE INFORMACIÓN EN SALUD PARA UN SGSI EN SALUD – ANEXO B		
CLAVE DEL DOCUMENTO: GII-A004-SGSI-ANEXO-B		VERSIÓN DEL DOCUMENTO: 01.01	FECHA DEL DOCUMENTO: 07 de junio de 2013	

Las organizaciones que procesan información personal de salud deberán asegurar de que los sistemas de TI empleados contengan funcionalidades de aplicaciones que hagan cumplir la aprobación de los procesos clínicos por diferentes titulares de la función, cuando ello sea necesario.

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

No existen recomendaciones por parte de la DGIS para la implementación de este control.

6.2. Gestión de la provisión de servicios por terceros

6.2.1. Provisión de servicios; 6.2.2. Supervisión y revisión de los servicios prestados por terceros; 6.2.3. Gestión del cambio en los servicios prestados por terceros

Lineamientos de implementación

La gestión de entrega de servicios de terceros es muy simplificada cuando un contrato formal es adoptado el cual especifica el conjunto mínimo de controles a ser implementados.

6.3. Planificación y aceptación del sistema

6.3.1. Gestión de las capacidades

No existen recomendaciones por parte de la DGIS para la implementación de este control.

6.3.2. Aceptación del sistema

Lineamientos de implementación

El alcance y el rigor de las pruebas deberán ser escalados a un nivel compatible con los riesgos identificados del cambio.

6.4. Protección contra el código malicioso y descargable

No existen recomendaciones por parte de la DGIS para la implementación de este control.

6.5. Copias de seguridad

No existen recomendaciones por parte de la DGIS para la implementación de este control.



 GOBIERNO DE MÉXICO	GUIA DE INTERCAMBIO DE INFORMACIÓN EN SALUD PARA UN SGSI EN SALUD – ANEXO B		
SALUD SECRETARÍA DE SALUD	CLAVE DEL DOCUMENTO: GII-A004-SGSI- ANEXO-B	VERSIÓN DEL DOCUMENTO: 01.01	FECHA DEL DOCUMENTO: 07 de junio de 2013

6.6. Gestión de la seguridad de las redes

6.6.1. Controles de red

No existen recomendaciones por parte de la DGIS para la implementación de este control.

6.6.2. Seguridad de los servicios de red

Lineamientos de implementación

Las organizaciones que procesan información personal de salud deberán considerar cuidadosamente el impacto que la pérdida de la disponibilidad de los servicios de red tendrá sobre la práctica clínica.

6.7. Manipulación de los medios

6.7.1. Gestión de los medios extraíbles

Lineamientos de implementación

Las organizaciones que procesan información personal de salud deberán asegurar que todo el personal que almacena información de salud en medios extraíbles sea:

- Cifrada mientras la media este en tránsito o
- Protegida de ladrones mientras la media este en tránsito.

6.7.2. Retirada de medios

Lineamientos de implementación

La inadecuada eliminación de medios sigue siendo una fuente de graves violaciones de la confidencialidad del paciente. Es especialmente importante tener en cuenta que este control se debe aplicar antes de la reparación o eliminación de cualquier equipo asociado. Este requerimiento también aplica a dispositivos médicos que graban o reportan datos.

6.7.3. Procedimientos de manipulación de la información

No existen recomendaciones por parte de la DGIS para la implementación de este control.

6.7.4. Seguridad de la documentación del sistema

No existen recomendaciones por parte de la DGIS para la implementación de este control.



 GOBIERNO DE MÉXICO SALUD SECRETARÍA DE SALUD	GUIA DE INTERCAMBIO DE INFORMACIÓN EN SALUD PARA UN SGSI EN SALUD – ANEXO B		
	CLAVE DEL DOCUMENTO: GII-A004-SGSI- ANEXO-B	VERSIÓN DEL DOCUMENTO: 01.01	FECHA DEL DOCUMENTO: 07 de junio de 2013

6.8. Intercambio de información

6.8.1. Políticas y procedimientos de intercambio de información de salud; 6.8.2 Acuerdos de intercambio

Lineamientos de intercambio

Las políticas de intercambio de información de salud pueden ser encontradas en ISO 22857. Aunque este estándar explícitamente se refiere al flujo transfronterizo de información personal de salud (donde fronteras en este contexto representa jurisdicciones de salud, no necesariamente fronteras nacionales), gran parte de sus asesoramientos pueden ser adaptados, donde sea necesario, para hacer frente al intercambio de datos de una organización a otra.

Las organizaciones deberán asegurar que la seguridad de dichos intercambios de información está sujeta a políticas de desarrollo y auditorías de cumplimiento.

La seguridad de los intercambios de información puede ser en gran medida asistida por el uso de los acuerdos de intercambio de información que especifican el conjunto mínimo de controles que deben ser implementados.

6.8.3. Medios físicos en tránsito

No existen recomendaciones por parte de la DGIS para la implementación de este control.

6.8.4. Mensajería instantánea

Lineamientos de implementación

Las organizaciones que transmiten información personal de salud por mensajería electrónica deberán tomar los pasos para asegurar la confidencialidad e integridad. Es importante tener en cuenta que la seguridad del correo electrónico y la mensajería instantánea que contiene información personal de salud puede implicar procedimientos para personal de salud que no pueden imponer a los sujetos de atención y al público.

Los correos electrónicos entre profesionales de la salud los cuales contengan información personal de salud deberán ser cifrados durante su tránsito. Un enfoque a esto implica el uso de certificados digitales.

6.8.5. Sistemas de Información

No existen recomendaciones por parte de la DGIS para la implementación de este control.



 GOBIERNO DE MÉXICO SALUD SECRETARÍA DE SALUD	GUÍA DE INTERCAMBIO DE INFORMACIÓN EN SALUD PARA UN SGSI EN SALUD – ANEXO B		
	CLAVE DEL DOCUMENTO: GII-A004-SGSI- ANEXO-B	VERSIÓN DEL DOCUMENTO: 01.01	FECHA DEL DOCUMENTO: 07 de junio de 2013

6.9. Servicios de comercio electrónico

6.9.1. Comercio electrónico; 6.9.2 Transacciones en línea

Lineamientos de implementación

Es importante tener en cuenta el cuidado que hay que tener en determinar si los datos que intervienen en el comercio electrónico y las transacciones en línea contengan información personal de salud. Si es así, esta información debe ser protegida adecuadamente. De especial preocupación en la salud son los datos relacionados a la facturación, reclamaciones médicas, líneas de captura, solicitudes y otros datos de comercio electrónico de la cual información personal de salud puede ser derivada.

6.9.3. Información de Salud públicamente disponible

No existen recomendaciones por parte de la DGIS para la implementación de este control.

6.10. Supervisión

6.10.1. Registros de auditoría

Lineamientos de implementación

Los sistemas de información personal de salud que procesan información personal de salud deberán crear un registro de auditoría para cada vez que un usuario accede, crea, actualiza o guarde información personal de salud a través del sistema. Los registros de auditoría deberán identificar al usuario, identificar al sujeto de datos (por ejemplo, el sujeto de atención), identificar la función realizada por el usuario (creación del registro, acceso, actualización, etc.), y anotar la fecha y hora en la cual esta función se realizó.

Cuando la información personal de salud es actualizada, un registro del anterior contenido de los datos y la asociación con los registros de auditoría (por ejemplo, quien introdujo los datos en qué fecha) deberán ser conservados.

Sistemas de mensajería usados para transmitir mensajes que contengan información personal de salud deberán llevar un log de los mensajes transmitidos (dicho log deberá contener la hora, fecha, origen y destino del mensaje, pero no su contenido).

La organización deberá cuidadosamente evaluar y determinar el periodo de retención para estos registros de auditoría, con especial referencia a normas clínicas profesionales y obligaciones legales, con el fin de facilitar la investigación a llevarse a cabo cuando sea necesario y proporcionar evidencia del mal uso cuando sea necesario.



 GOBIERNO DE MÉXICO SALUD SECRETARÍA DE SALUD	GUÍA DE INTERCAMBIO DE INFORMACIÓN EN SALUD PARA UN SGSI EN SALUD – ANEXO B		
	CLAVE DEL DOCUMENTO: GII-A004-SGSI-ANEXO-B	VERSIÓN DEL DOCUMENTO: 01.01	FECHA DEL DOCUMENTO: 07 de junio de 2013

6.10.2. Supervisión del uso del sistema

Lineamientos de implementación

La facilidad del registro de auditoría de los sistemas de información de salud deberá ser operacional en todo momento mientras el sistema de información de salud siendo auditado esté disponible para su uso.

Sistemas de información de salud que contengan información personal de salud deberán ser provistos con facilidades para analizar registros y resultados de auditoría que:

- Permitan la identificación de todos los usuarios del sistema que han ingresado o modificado un registro(s) de un sujeto de atención sobre un periodo de tiempo dado;
- Permitir la identificación de todos los sujetos de atención cuyos registros han sido ingresados o modificados por un usuario de sistema sobre un periodo de tiempo dado.

6.10.3. Protección de la información de los registros

Lineamientos de implementación

Es importante tener en cuenta que las evidencias integrales de registro de auditoría pueden desempeñar un papel esencial en las indagaciones forenses, investigaciones dentro de la mala práctica médica, y otros procedimientos judiciales. En dichos procedimientos, las acciones de los profesionales de la salud y la sincronización de los eventos son a veces determinadas a través de un examen de los cambios y actualizaciones de la información personal de salud de un individuo.

6.10.4. Registros de administración y operación

No existen recomendaciones por parte de la DGIS para la implementación de este control.

6.10.5. Registro de fallos

No existen recomendaciones por parte de la DGIS para la implementación de este control.

6.10.6. Sincronización del reloj

Lineamientos de implementación

Es importante tener en cuenta la sincronización de los eventos registrados electrónicamente como la información personal de salud y en registros de auditoría pueden desempeñar un papel esencial en los procesos tales como indagaciones forenses, investigaciones sobre mala práctica médica, y otros procedimientos judiciales en los que es esencial determinar con precisión una secuencia clínica de eventos.



 GOBIERNO DE MÉXICO SALUD SECRETARÍA DE SALUD	GUÍA DE INTERCAMBIO DE INFORMACIÓN EN SALUD PARA UN SGSI EN SALUD – ANEXO B		
CLAVE DEL DOCUMENTO: GII-A004-SGSI-ANEXO-B	VERSIÓN DEL DOCUMENTO: 01.01	FECHA DEL DOCUMENTO: 07 de junio de 2013	

7. CONTROL DE ACCESO

7.1. Requisitos de control de acceso en Salud

7.1.1. Política de control de acceso

Lineamientos de implementación

Es importante hacer notar que en el orden en que la salud es entregada, existen requisitos más fuertes que usuales para una política clara, con autorización asociada, para anular las reglas de control de acceso “normales” en situaciones de emergencia.

Las organizaciones de salud son animadas a considerar la implementación de una solución de gestión de acceso que esto proporcionara la política de control de acceso. Además, esto apoyara los procesos de acceso de alto nivel de seguridad, como el acceso basado en tarjetas inteligentes y capacidad de “single sign-on”.

7.2. Gestión de acceso de usuario

7.2.1. Registro de usuario

Lineamientos de implementación

Es importante entender que la tarea de identificar y registrar usuarios de sistemas de información de salud incluya todas las siguientes:

- La captura precisa de la identidad de un usuario (por ejemplo, Joan March, nacido el 26 de marzo de 1982, en la actualidad reside en una dirección específica);
- La captura precisa, previa verificación de las credenciales profesionales de un usuario (por ejemplo, Dr. Joan Smith, cardiólogo) y/o título de trabajo (por ejemplo, Susan Jones, Recepcionista Medico);
- La asignación de un identificador de usuario inequívoco.

Tenga en cuenta que los sujetos de atención no son típicamente usuarios del sistema, a pesar de que son capaces de acceder a la totalidad o parte de los datos personales (por ejemplo, a través de un portal en línea) serian de hecho los usuarios del sistema (aunque estos tienen acceso limitado concedido). Tenga en cuenta también que hay aplicaciones de salud donde el usuario puede buscar información de salud general, asesoramiento e información. Si bien se puede registrar esta solicitud de información, el usuario que acceda permanece anónimo. Muchos sitios web que ofrecen información sobre el embarazo, SIDA y otros temas de salud pública operan en esta manera. Los usuarios de estos sitios de información general típicamente no requieren el registro y, por tanto son excluidos de la consideración de gestión de privilegios.



 GOBIERNO DE MÉXICO SALUD SECRETARÍA DE SALUD	GUÍA DE INTERCAMBIO DE INFORMACIÓN EN SALUD PARA UN SGSI EN SALUD – ANEXO B		
	CLAVE DEL DOCUMENTO: GII-A004-SGSI- ANEXO-B	VERSIÓN DEL DOCUMENTO: 01.01	FECHA DEL DOCUMENTO: 07 de junio de 2013

7.2.2. Gestión de privilegios

Lineamientos de implementación

Los sistemas de información de salud que contengan información personal de salud deberán soportar controles de acceso basado en roles capaces de mapear a cada usuario a uno o más roles, y cada rol para una o más funciones del sistema.

Un usuario del sistema de información de salud que contiene información personal de salud deberá acceder a sus servicios en un solo rol (por ejemplo, usuarios quienes han sido registrados con más de un rol serán designados a un solo rol durante cada inicio de sesión de acceso al sistema de información de salud).

Los sistemas de información de salud deberán asociar usuarios (incluidos profesionales de la salud, personal de soporte y otros) con los registros de los sujetos de atención y permitir el acceso futuro basado en una asociación. Lineamientos adicionales de gestión de privilegios en salud serán encontrados en ISO/TS 22600-1 y en ISO/TS 22600-2.

7.2.3. Gestión de contraseñas de usuarios

No existen recomendaciones por parte de la DGIS para la implementación de este control.

7.2.4. Revisión de los derechos de acceso de usuario

No existen recomendaciones por parte de la DGIS para la implementación de este control.

7.3. Responsabilidades de usuario

7.3.1. Uso de contraseñas, 7.3.2 Equipo de usuario desatendido; 7.3.3 Política de puesto de trabajo despejado y escritorio limpio

Lineamientos de implementación

Las organizaciones que procesan información personal de salud deberán, cuando determinen responsabilidades de los usuarios, respetar los derechos y responsabilidades éticas de profesionales de salud, como lo convenido en las leyes y aceptadas por miembros de organizaciones profesionales de la salud.

7.4. Control de acceso a la red

No existen recomendaciones por parte de la DGIS para la implementación de este control.



 GOBIERNO DE MÉXICO SALUD SECRETARÍA DE SALUD	GUÍA DE INTERCAMBIO DE INFORMACIÓN EN SALUD PARA UN SGSI EN SALUD – ANEXO B		
	CLAVE DEL DOCUMENTO: GII-A004-SGSI- ANEXO-B	VERSIÓN DEL DOCUMENTO: 01.01	FECHA DEL DOCUMENTO: 07 de junio de 2013

7.5. Control de acceso al sistema operativo

No existen recomendaciones por parte de la DGIS para la implementación de este control.

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

7.6.1. Restricción de acceso a la información

Lineamientos de implementación

Consideraciones especiales deberán ser dadas a las mediciones técnicas por las cuales un sujeto de atención esta seguramente autenticado cuando accede a toda o parte de su propia información (en los sistemas de información de salud que permiten dicho acceso). Un énfasis similar deberá también ser tomado a la facilidad de uso de dichas medidas, especialmente para sujetos de atención minusválidos, y disposiciones para acceder para los tomadores de decisiones.

7.6.2. Aislamiento de sistemas sensibles

No existen recomendaciones por parte de la DGIS para la implementación de este control.

7.7. Equipos de cómputo portátiles y teletrabajo

7.7.1. Equipos de cómputo portátiles y comunicaciones móviles

No existen recomendaciones por parte de la DGIS para la implementación de este control.

7.7.2. Teletrabajo

Lineamientos de implementación

Las organizaciones que procesan información personal de salud deberán:

- Preparar una política sobre las precauciones a ser tomadas cuando realiza teletrabajo;
- Asegurar que los usuarios de teletrabajo de sistemas de información de salud acaten esta política.

Algunas experiencias internacionales han implementado restricciones sobre teletrabajo para profesionales de la salud.

Es importante considerar que en la salud, el teletrabajo puede cruzar fronteras más allá de cualquier jurisdicción. Los médicos rutinariamente envían imágenes médicas por correo electrónico, etc. Para obtener opiniones de especialistas.



 GOBIERNO DE MÉXICO SALUD SECRETARÍA DE SALUD	GUIA DE INTERCAMBIO DE INFORMACIÓN EN SALUD PARA UN SGSI EN SALUD – ANEXO B		
	CLAVE DEL DOCUMENTO: GII-A004-SGSI- ANEXO-B	VERSIÓN DEL DOCUMENTO: 01.01	FECHA DEL DOCUMENTO: 07 de junio de 2013

8. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN

8.1. Requisitos de seguridad de los sistemas de información

No existen recomendaciones por parte de la DGIS para la implementación de este control.

8.2. Procesamiento correcto en aplicaciones

8.2.1. Identificación única de sujetos de atención

Lineamientos de implementación

La provisión de cuidados de emergencia y otras situaciones en las cuales una adecuada identificación de los sujetos de atención no habría sido posible sin inevitablemente crear instancias de múltiples registros para el mismo sujeto de atención. Algunas capacidades existirán dentro de cada sistema de información de salud para unir múltiples instancias de registros de sujetos de atención en un solo registro. Cada fusión requiere el mayor cuidado y por lo tanto no solo necesitara entrenamiento personal en cada fusión, pero también requerirá herramientas técnicas para facilitar mejor la integración de la información de registros dentro de una identificación completa.

Organizaciones que procesan información personal de salud deberán asegurar que los datos de la identificación personal puedan ser entregados si están retenidos donde sea necesario hacer esto, y las técnicas de eliminación, anonimato y pseudónimos están propiamente usadas para minimizar el riesgo de la relevación no intencionada de información personal.

8.2.2. Validación de los datos de entrada

No existen recomendaciones por parte de la DGIS para la implementación de este control.

8.2.3. Control de procesamiento interno

No existen recomendaciones por parte de la DGIS para la implementación de este control.

8.2.4. Integridad de los mensajes

No existen recomendaciones por parte de la DGIS para la implementación de este control.



 GOBIERNO DE MÉXICO SALUD SECRETARÍA DE SALUD	GUÍA DE INTERCAMBIO DE INFORMACIÓN EN SALUD PARA UN SGSI EN SALUD – ANEXO B		
	CLAVE DEL DOCUMENTO: GII-A004-SGSI-ANEXO-B	VERSIÓN DEL DOCUMENTO: 01.01	FECHA DEL DOCUMENTO: 07 de junio de 2013

8.2.5. Validación de los datos de salida

Lineamiento de implementación

Algunos factores adicionales importantes necesitan ser considerados. Antes de confiar en la información personal de salud suministrada por un sistema de información personal, a los profesionales de la salud se les necesita mostrar suficiente información para asegurar que el sujeto de atención que están tratando coincida con la información solicitada. Hacer coincidir a un sujeto de atención bajo tratamiento a un registro existente puede ser una tarea no trivial. Algunos sistemas mejoran la seguridad incluyendo fotografías de identificación con cada registro de sujetos de atención. Dichas mejoras podrían crear problemas de privacidad, como permitir potencialmente la captura implícita de características faciales tal como una prueba que no está incluida como campo de dato. Los requerimientos para la identificación de los sujetos de atención y la disponibilidad del soporte de los datos usados podrían también variar de jurisdicción a jurisdicción.

Los sistemas de información de salud deberán hacer lo posible para verificar que las impresiones de salida estén completas (por ejemplo, “pagina 3 de 5”).

8.3. Controles criptográficos

8.3.1. Política de uso de los controles criptográficos y gestión de claves; 8.3.2 Gestión de claves

Lineamientos de implementación

Los lineamientos sobre política para la emisión y uso de certificados digitales en salud y la gestión de claves pueden ser encontrados en la norma ISO 17090-3.

8.4. Seguridad de los archivos de sistema

8.4.1. Control del software en explotación

No existen recomendaciones por parte de la DGIS para la implementación de este control.

8.4.2. Protección de los datos de prueba del sistema

Lineamientos de implementación

Las organizaciones que procesan información personal de salud no deberán usar información personal actual como datos de prueba.



 GOBIERNO DE MÉXICO SALUD SECRETARÍA DE SALUD	GUÍA DE INTERCAMBIO DE INFORMACIÓN EN SALUD PARA UN SGSI EN SALUD – ANEXO B		
	CLAVE DEL DOCUMENTO: GII-A004-SGSI- ANEXO-B	VERSIÓN DEL DOCUMENTO: 01.01	FECHA DEL DOCUMENTO: 07 de junio de 2013

8.4.3. Control de acceso al código fuente de los programas

No existen recomendaciones por parte de la DGIS para la implementación de este control.

8.5. Seguridad en los procesos de desarrollo y soporte

No existen recomendaciones por parte de la DGIS para la implementación de este control.

8.6. Gestión de la vulnerabilidad técnica

No existen recomendaciones por parte de la DGIS para la implementación de este control.

9. GESTIÓN DE INCIDENTES DE LA SEGURIDAD DE LA INFORMACIÓN

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

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

No existen recomendaciones por parte de la DGIS para la implementación de este control.

9.1.2. Notificación de puntos débiles de seguridad

Lineamientos de implementación

Las organizaciones que procesan información personal de salud deberán establecer gestión de responsabilidades de incidentes de seguridad y procedimientos en orden de:

- Asegurar de manera rápida, efectiva y ordenadamente responder a incidentes de seguridad;
- Asegurar que exista un proceso de escalamiento efectivo para incidentes como la gestión de riesgos y planes gestión de la continuidad del negocio pueden ser invocados en circunstancias correctas y en el tiempo correcto;
- Colectar y preservar datos relacionados a incidentes tales como pistas de auditoría, registros y otra evidencia.



 GOBIERNO DE MÉXICO SALUD SECRETARÍA DE SALUD	GUÍA DE INTERCAMBIO DE INFORMACIÓN EN SALUD PARA UN SGSI EN SALUD – ANEXO B		
	CLAVE DEL DOCUMENTO: GII-A004-SGSI- ANEXO-B	VERSIÓN DEL DOCUMENTO: 01.01	FECHA DEL DOCUMENTO: 07 de junio de 2013

Incidentes de seguridad de la información que incluyen corrupción o revelaciones no intencionadas de información personal de salud o pérdida de disponibilidad de sistemas de información de salud, donde cada pérdida negativamente afecta al cuidado del paciente o contribuye a eventos clínicos adversos.

Las organizaciones deberán informar al sujeto de atención siempre que la información personal de salud ha sido revelada de manera no intencional.

Las organizaciones deberán informar al sujeto de atención siempre que la falta de disponibilidad de los sistemas de información de salud podría negativamente afectar sus cuidados.

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

9.2.1. Responsabilidades y procedimientos

No existen recomendaciones por parte de la DGIS para la implementación de este control.

9.2.2. Aprendizaje de los incidentes

No existen recomendaciones por parte de la DGIS para la implementación de este control.

9.2.3. Recopilación de evidencias

Lineamientos de implementación

Las organizaciones que procesan información personal de salud necesitarán considerar las implicaciones de recopilar evidencia para propósitos de establecer malas prácticas médicas, y necesitarán considerar requisitos inter jurisdiccionales cuando los sistemas de información de salud son accedidos a través de fronteras jurisdiccionales.

10. GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

10.1. Aspectos de la seguridad de la información en la gestión de la continuidad del negocio

No existen recomendaciones por parte de la DGIS para la implementación de este control.

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

No existen recomendaciones por parte de la DGIS para la implementación de este control.



 GOBIERNO DE MÉXICO SALUD SECRETARÍA DE SALUD	GUÍA DE INTERCAMBIO DE INFORMACIÓN EN SALUD PARA UN SGSI EN SALUD – ANEXO B		
	CLAVE DEL DOCUMENTO: GII-A004-SGSI- ANEXO-B	VERSIÓN DEL DOCUMENTO: 01.01	FECHA DEL DOCUMENTO: 07 de junio de 2013

10.1.2. Continuidad del negocio y evaluación de riesgos

No existen recomendaciones por parte de la DGIS para la implementación de este control.

10.1.3. Desarrollo e implementación de planes de continuidad que incluyan la seguridad de la información

No existen recomendaciones por parte de la DGIS para la implementación de este control.

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

No existen recomendaciones por parte de la DGIS para la implementación de este control.

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

Lineamientos de implementación

Las siguientes consideraciones son importantes en los ambientes de salud. Gestión de la continuidad del negocio, que incluye recuperación de desastres, se reconoce cada vez más como requisito para las organizaciones de salud y de la prioridad que se concede sigue creciendo. Como reflejo de la rigurosa disponibilidad de los requisitos en salud, un gran esfuerzo debe ser invertido en la capacidad de recuperación de acuerdos de entrega, no solo para la propia tecnología sino también para el entrenamiento cruzado de personal de salud.

Planificación de la continuidad en salud es especialmente difícil para los profesionales de seguridad de la información, que tendrán que ser adecuadamente integrados con los planes de la organización para el manejo de fallas de energía, implementación de control de infecciones y el tratamiento de otras emergencias clínicas. En efecto, la invocación de cualquiera de estos es probable que conduzca directamente a la invocación del plan de gestión de la continuidad del negocio, aunque solo sea para dar apoyo adicional a la normalmente disponible. Sin embargo, los incidentes han mostrado que los principales incidentes pueden causar una escasez de personal, que a su vez puede limitar severamente la capacidad de operar con éxito los planes de gestión de continuidad del negocio.

Las organizaciones de salud deben asegurarse de que sus planes de gestión de continuidad del negocio incluyan la gestión de planeación de las crisis de salud. Las organizaciones de salud también deben asegurarse de que los planes que se desarrollan son evaluados regularmente en una base “programática”. Las evaluaciones incluidas en ese programa deberán basarse sobre otros, procedentes de pruebas de escritorio para pruebas modulares para la síntesis de los tiempos de recuperación probables y finalmente a los ensayos completos. Dicho programa es por lo tanto un riesgo bajo y ofrece una mejora real en el nivel general de conocimiento de su usuario.



 GOBIERNO DE MÉXICO SALUD SECRETARÍA DE SALUD		GUIA DE INTERCAMBIO DE INFORMACIÓN EN SALUD PARA UN SGSI EN SALUD – ANEXO B		
CLAVE DEL DOCUMENTO: GII-A004-SGSI-ANEXO-B		VERSIÓN DEL DOCUMENTO: 01.01	FECHA DEL DOCUMENTO: 07 de junio de 2013	

11. CUMPLIMIENTO

Lineamientos de implementación

Las organizaciones de salud deberán poner un programa de auditoría de cumplimiento en el lugar que dirige el ciclo de vida de operaciones, por ejemplo, no solamente de aquellos procesos que identifican publicaciones, pero también de aquellos que identifican los problemas, sino también de aquellos que revisan resultados y que deciden sobre actualizaciones del SGSI.

11.1. Cumplimiento de los requisitos legales

11.1.1. Identificación de la legislación aplicable

No existen recomendaciones por parte de la DGIS para la implementación de este control.

11.1.2. Derechos de propiedad intelectual

No existen recomendaciones por parte de la DGIS para la implementación de este control.

11.1.3. Protección de los documentos de la organización

No existen recomendaciones por parte de la DGIS para la implementación de este control.

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

Lineamientos de implementación

Un ejemplo de legislación o regulación que requiere el consentimiento informal de los sujetos de atención es el Consejo Europeo y Recomendación, R (97)5 sobre la Protección de los Datos Médicos, Consejo de Europa, Estrasburgo, 12 de febrero de 1997.

Antes de que se lleve a cabo un análisis genético, el interesado debe ser informado acerca de los objetivos del análisis y la posibilidad de hallazgos inesperados.

Se les debe informar de los hallazgos inesperados si:

- a) Que no esté prohibido por la legislación nacional;
- b) La persona misma ha perdido esta información
- c) No es probable que la información cause un daño grave
 - I. A su salud
 - II. A su consanguíneo o uterino, a un miembro de su familia o a una persona que tenga una relación directa con su línea genética
- d) Esta información es de importancia directa para su tratamiento o prevención.



 GOBIERNO DE MÉXICO SALUD SECRETARÍA DE SALUD	GUIA DE INTERCAMBIO DE INFORMACIÓN EN SALUD PARA UN SGSI EN SALUD – ANEXO B		
	CLAVE DEL DOCUMENTO: GII-A004-SGSI- ANEXO-B	VERSIÓN DEL DOCUMENTO: 01.01	FECHA DEL DOCUMENTO: 07 de junio de 2013

11.1.5. Prevención del uso indebido de recursos de tratamiento de la información

No existen recomendaciones por parte de la DGIS para la implementación de este control.

11.1.6. Regulación de los controles criptográfico

No existen recomendaciones por parte de la DGIS para la implementación de este control.

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

11.2.1. Cumplimiento de las políticas y normas de seguridad

No existen recomendaciones por parte de la DGIS para la implementación de este control.

11.2.2. Comprobación del cumplimiento técnico

Lineamientos de implementación

Se presta especial atención al cumplimiento de los fines de la interoperabilidad técnica, como sistemas de información de salud a gran escala suelen consistir en muchos sistemas inter operando.

11.3. Consideraciones sobre las auditorías de los sistemas de información

11.3.1. Controles de auditoría de los sistemas de información

No existen recomendaciones por parte de la DGIS para la implementación de este control.

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

No existen recomendaciones por parte de la DGIS para la implementación de este control.

