Universidad Nacional Autónoma de México
Programa de Posgrado en Ciencias de la Administración

La gestión de riesgos de seguridad del Sector Salud en México

T e s i s

Que para optar por el grado de:

Maestra en Administración

Presenta:
Miriam Josefina Padilla Espinosa

Tutor:
M.A. Uriel Calvo Palmerín
Facultad de Contaduría y Administración

México, D. F. 2014

AGRADECIMIENTOS

A mi tutor Dr. Carlos Eduardo Puga Murguía:

Gracias por creer en mi trabajo por todo lo que compartió conmigo, una gran tristeza dejo en mi corazón su partida porque teníamos muchas cosas por hacer juntos, pero agradezco tanto a Dios la gran oportunidad de haber conocido a un gran ser humano, un maestro ejemplar y un tutor maravilloso, he cumplido mi promesa y por fin este trabajo que juntos comenzamos esta terminado.

Son tantas las personas que han estado cerca de mí y que han sido parte fundamental para hacer que este sueño sea hoy una realidad, gracias a todos por su apoyo, su cariño y amistad. El fruto de todo este tiempo se refleja en este trabajo que hoy con gran amor dedico a todos ustedes.

A mis padres:

Gracias por darme la vida, por siempre preocuparse y darme lo mejor, las cosas más valiosas que ustedes me han dado y que llevaré por siempre conmigo es su inmenso amor, su preocupación por mi educación y la fuerza para siempre luchar por lograr mis metas, hoy hemos alcanzado la cima de esta montaña que en ocasiones los obstáculos la hacían ver muy alta, sé que tu papi me miras desde el cielo y estás compartiendo conmigo y con mi mami este momento, el camino para llegar fue arduo pero la satisfacción de la vista al llegar a lo más alto es espléndida, gracias por estar ahí para alentarme siempre y por su apoyo incondicional.

A mi novio Óscar:

Porque tu amor ha iluminado e inspirado cada día, hemos compartido tantos momentos especiales y hemos crecido juntos como amigos, como pareja y como profesionales, gracias por todo tu apoyo en este proyecto que hoy llega a su fin y del cual has sido una parte muy especial. *"…That when you have it, you trust it... you believe in it.. take a chance on it.. and you're willing to sacrifice anything to keep it, no matter what the cost*".

A mi familia:

A mis hermanos Gerardo, Alejandro y Perla, a mis tías Rosy y Vero gracias por su apoyo en momentos que fueron muy difíciles para mi familia, por su amor desde que era pequeña.

A mi tutor de generación Mtro. Scott Da Gama

Gracias por todos tus consejos, tu guía, eres un gran amigo ha sido un gran placer para mi conocerte eres un ser humano extraordinario, te admiro y te estimo mucho.

A mi tutores y guías Mtro. Uriel Calvo y Mtra Celia Luz González Fernández:

Profundamente agradecida con ustedes, no sólo por ser mis profesores durante mi estancia en el posgrado, además de ello por el gran apoyo que me han brindado para concluir mi trabajo, por su guía y constante preocupación, no hay palabras que puedan expresar mi agradecimiento.

A todos mis profesores del posgrado:

Gracias por todo el conocimiento y consejos que compartieron tanto dentro como fuera del aula, porque ello no solo me ha permitido crecer profesionalmente sino además ha hecho de mí una mejor persona.

A mis amigos:

Por todas aquellas ocasiones en que no había tiempo para poder verlos, gracias por su comprensión y su apoyo incondicional. Los quiero.

A mi Alma mater:

Mi querida y amada Universidad orgullosa siempre de llevar muy en alto tu nombre, cuantos momentos he compartido en tus aulas, como estudiante de licenciatura, después como estudiante de posgrado y agradecida ahora por tener la dicha de ser catedrática de la Facultad de Ingeniería, donde he tenido la oportunidad de compartir mucho de lo que he recibido como universitaria.

Se cierra un ciclo que me ha enriquecido como persona, que me ha dejado mucho aprendizaje en todos los aspectos académico, personal y espiritual, que si he logrado esto es gracias también a todos ustedes, ahora si es el momento para que en lo más alto de esta montaña extienda los brazos y orgullosamente pueda decir …

¡LO HE LOGRADO!

ÍNDICE

Introducción 1
Capítulo 1: La seguridad de la información en los datos clínicos 3
1.1 Los datos, la información y la informática. 3
1.1.1 Datos 4
1.1.2 Información 4
1.1.3 Informática 5
1.2 Seguridad de la información 5
1.2.1 Seguridad 6
1.2.2 Servicios de seguridad 7
1.2.3 Amenazas 9
1.2.4 Vulnerabilidades 10
1.2.5 Ataques 10
1.2.6 Normativa de seguridad de la información 10
1.2.6.1 Normatividad y regulaciones 11
1.2.6.2 Estándares 11
1.3 Datos clínicos 22
1.4 Tratamiento jurídico de los datos clínicos 24
1.4.1 Panorama nacional 24
1.4.2 Panorama internacional 27
1.5 Importancia de la seguridad de los datos clínicos 29
Capítulo 2: Gestión de Riesgos de seguridad 33
2.1 Evolución histórica de la gestión de riesgos 33
2.2 Conceptos fundamentales sobre la gestión de riesgos de seguridad 36
2.2.1 Riesgo 38
2.2.2 Riesgos de seguridad de la información 39
2.2.3 Valoración de riesgos 39
2.2.4 Tratamiento del riesgo 41
2.3 Proceso General de Gestión de Riesgos 43

2.4 Modelos para la gestión / valoración de riesgos 45
2.4.1 ISO 31000 46
2.4.2 NIST 48
2.4.3 OCTAVE 49
2.4.4 FRAP 50
2.4.5 COSO 51
2.4.6 MAGERIT 52
2.4.7 ISO 27005 53
2.4.8 COBRA 54
2.5 La gestión de riesgos de seguridad de la información en el Sector Salud de México 55
Capítulo 3: Sistema de Salud en México 59
3.1 Panorama general del Sistema de Salud en México 59
3.1.1 IMSS 66
3.1.2 ISSSTE 67
3.2 Principales amenazas en los datos clínicos 69
Capítulo 4: Diseño de la investigación 77
4.1 Planteamiento del problema de investigación 77
4.1.1 Justificación de la investigación 78
4.2 Preguntas de investigación 79
4.2.1 Pregunta general 79
4.2.2 Preguntas específicas 79
4.3 Objetivos 80
4.3.1 Objetivo general 80
4.3.2 Objetivos específicos 80
4.4 Formulación de hipótesis 80
4.5 Variables 81
4.6 Metodología empleada 83
4.7 Selección de la muestra 84
4.8 Elaboración del instrumento 85
4.8.1 Redefiniciones fundamentales 85
4.8.2 Revisión enfocada de la literatura 86
4.8.3 Identificación del dominio de las variables a medir y sus indicadores 87

4.8.4 Toma de decisiones clave ... 98
4.8.5 Construcción del instrumento ... 98
4.8.6 Prueba piloto ... 103
4.8.7 Elaboración de la versión final del instrumento y su procedimiento de aplicación ... 103
4.8.8 Entrenamiento del personal que va administrar el instrumento ... 104
4.8.9 Autorización para aplicar el instrumento ... 104
4.8.10 Administración del instrumento ... 104
4.9 Confiabilidad y validez ... 104
Capítulo 5: Análisis de los resultados ... 106
5.1 Descripción institucional ... 107
5.2 Gestión de riesgos de seguridad ... 113
5.3 Seguridad de la información ... 116
5.4 Conclusiones ... 122
Capítulo 6: Metodología para la gestión de riesgos de seguridad del sector de salud en México ... 124
6.1 Objetivo ... 125
6.2 Roles y responsabilidades ... 126
6.3 Definiciones ... 128
6.4 Enfoque ... 129
6.5 Metodología ... 130
6.5.1 Capacitar ... 134
6.5.2 Descubrir ... 137
6.5.3 Reaccionar ... 146
6.5.4 Vigilar ... 151
6.5.5 Mejorar ... 151
6.6 Calidad ... 152
Conclusiones ... 154
Glosario ... 156
Anexos ... 158
A. Instrumento de medición ... 159
B. Oficio de presentación del estudio ... 164
C. Estudio informacional ... 165
1. Introducción ... 166

2. Justificación 166
3. Objetivos 167
4. Conceptos básicos 167
5. Desarrollo 169
6. Hallazgos y conclusiones 194
D. Formatos Metodología CADERVIM 196
E. Oficio de nombramiento de jurado de tesis 201
Bibliografía: 202

INTRODUCCIÓN

La incorporación de las tecnologías de información y comunicaciones en el Sector Salud en México pretenden transformar la prestación de los servicios, para mejorar los tiempos, la calidad y satisfacer la demanda cada vez mayor, como resultado del crecimiento de la población y el comportamiento de las enfermedades. Si bien la incorporación de tecnología ha contribuido a mejorar la situación del sector salud público, éste enfrenta aún grandes retos en materia de innovación tecnológica y seguridad de la información, siendo este último, el objeto de análisis de la presente investigación.

La seguridad de la información para la protección de los datos personales es un tema que en los últimos años ha cobrado gran importancia, iniciativas a nivel legal y normativo han logrado avances significativos en el tema, no obstante en el sector salud aún hay grandes áreas de oportunidad con relación a la protección de los datos personales, incluidos en éstos los datos clínicos, es por ello que el enfoque ante incidentes de seguridad de información es de tipo reactivo, de ahí que instituciones como el Instituto Mexicano del Seguro Social (IMSS) y el Instituto de Seguridad y Servicios Sociales de los Trabajadores del Estado (ISSSTE) sean víctimas del mal uso de sus activos, generando con ello problemas de tipo financiero y en su reputación, además a la par del crecimiento tecnológico surgen nuevas amenazas que atentan contra la seguridad de los datos clínicos y es por ello que las instituciones de salud requieren definir estrategias que consideren estos escenarios bajo un enfoque de gestión de riesgos, para que puedan enfrentar los retos que en materia de seguridad de la información surgen a la par de la incorporación de la tecnología.

Por este motivo nace la inquietud de investigar la situación actual sobre la seguridad de la información en los datos clínicos, si cuentan o no con alguna metodología para gestionar los riesgos de seguridad y su conocimiento sobre estándares internacionales, normatividad y leyes en la materia, con base en los resultados obtenidos se propondrá una metodología para la gestión de riesgos de seguridad de la información que contribuya a mejorar la protección de los datos clínicos y fortalezca la cultura de seguridad de la información.

El presente trabajo de investigación está integrado por seis capítulos que se presentan y describen a continuación:

En el *Capítulo 1 La seguridad de la información en los datos clínicos:* presenta las definiciones sobre los conceptos fundamentales relacionados con la seguridad de la información y los datos clínicos, además del marco normativo tanto nacional como internacional, una breve descripción del panorama actual sobre los datos clínicos y la importancia de su protección.

El *Capítulo 2 Gestión de riesgos de seguridad*: describe la evolución histórica de la gestión de riesgos, los conceptos fundamentales, los principales estándares relacionados, el enfoque para evaluar los riesgos de seguridad, las diferentes opciones para dar tratamiento a los riesgos identificados, además presenta a detalle el proceso general para la gestión de riesgos de seguridad y los diferentes modelos que existen, por último el capítulo concluye con una descripción sobre el panorama actual de la gestión de riesgos de seguridad de la información en el sector salud en México.

En el *Capítulo 3 Sistema de salud en México:* se muestra la estructura del estado actual del sistema de salud en México, su marco jurídico y se describen a detalle las instituciones que serán sujetas de análisis (IMSS e ISSSTE), una vez entendiendo el contexto se dan a conocer las principales amenazas que atentan contra la seguridad de la información de los datos clínicos para mostrar la importancia que el personal de las instituciones tenga conocimientos que les permitan estar protegidos ante eventos inesperados.

El *Capítulo 4 Diseño de la investigación:* detalla el planteamiento del problema que da origen a la investigación, se plantean las preguntas de investigación, la hipótesis, las variables de estudio que serán consideradas, se define la muestra y se construye el instrumento que será aplicado en las instituciones incluidas en el alcance.

En el *Capítulo 5 Análisis de los resultados:* se observa el comportamiento de las variables de estudio, se da respuesta con esta información a las preguntas de investigación y se verifica si se cumple o no la hipótesis planteada en el capítulo anterior.

Para concluir y una vez que se han identificado las áreas de oportunidad en materia de gestión de riesgos de seguridad de la información, el *Capítulo 6 Metodología para la gestión de riesgos de seguridad del sector salud en México*, se propone una metodología que pueda apoyar a las instituciones de salud para mejorar la protección de los datos clínicos. En este apartado se describe cada etapa y actividades necesarias que conforman la propuesta, así como los roles y responsabilidades involucradas.

Finalmente en el apartado de conclusiones se analizan los resultados obtenidos como resultado de la investigación esperando que este estudio sea una puerta para futuras investigaciones sobre la seguridad de la información en el sector salud.

CAPÍTULO 1

LA SEGURIDAD DE LA INFORMACIÓN EN LOS DATOS CLÍNICOS

El propósito de este capítulo es, abordar los conceptos fundamentales relacionados con la seguridad de la información y los datos clínicos, se presenta la definición de dato, información, informática, seguridad de la información, la clasificación de los servicios de seguridad, el tipo de amenazas, vulnerabilidades y ataques, así como el significado de datos clínicos y su tratamiento jurídico a nivel nacional e internacional. Para concluir se presenta una reflexión, que muestra los grandes retos que en la actualidad enfrentan las tecnologías de la información y comunicaciones en el sector salud en México, así como el panorama actual sobre iniciativas como la implantación del expediente clínico electrónico.

1.1 LOS DATOS, LA INFORMACIÓN Y LA INFORMÁTICA.

Es común que las palabras, datos e información sean utilizadas de forma indistinta, esto es, debido al desconocimiento sobre la diferencia existente en ambos términos, hecho que fue identificado durante la lectura de las fuentes consultadas, en las cuales, se hace referencia a los datos clínicos como información, registro, expediente adicionando la palabra clínica o médica, según sean el caso. En el caso de la informática, ha adoptado un papel fundamental para llevar a cabo el manejo de la información, que en tiempos actuales, es de vital importancia, considerando las demandas tanto de usuarios como de consumidores, hacia las empresas e instituciones sobre la necesidad de innovar en los servicios. De tal forma que en la actualidad las tecnologías de la información y comunicaciones, han fungido como uno de los actores principales en el proceso de innovación, hecho que también ha sido adoptado en instituciones del sector salud y sus diversas iniciativas para modernizar el servicio, tal como la implementación de sistemas web para la atención de los derechohabientes, mejora y automatización en su proceso para la obtención de citas mediante el uso de Internet, la incorporación de expedientes clínicos electrónicos, así como de sistemas de información para los médicos y la

integración tanto de equipos de cómputo como de alta tecnología en los hospitales y clínicas de especialidades.

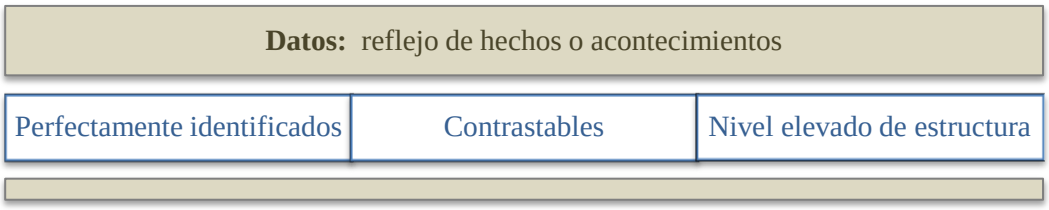
A continuación se presentan los siguientes conceptos:

1.1.1 DATOS

Los datos son resultados de observaciones obtenidas a partir, de mediciones aplicadas a hechos concretos o valores asignados de forma explícita a un objeto o acontecimiento. *(Cornella, 2000)* De tal forma que los datos son un reflejo de hechos que ocurren en la realidad y cuentan con las siguientes características que permiten su distinción (Figura 1.1 Características de los datos).

- ***a)*** *Perfectamente identificados:* dado que están integrados por conjuntos de símbolos (letras, números) no hay posibilidad de confusión.
- ***b)*** *Contrastables:* de manera indiscutible es posible determinar si son ciertos o no.
- ***c)*** *Nivel elevado de estructura:* al darse a conocer entre emisor y receptor, la posibilidad de confusión es mínima, ya que no brindan la alternativa para ser interpretados. En caso de presentarse un mala interpretación de los datos, esto puede deberse más a un problema de comunicación en el medio utilizado que por los datos en sí mismos.

Figura 1. 1 Características de los datos.



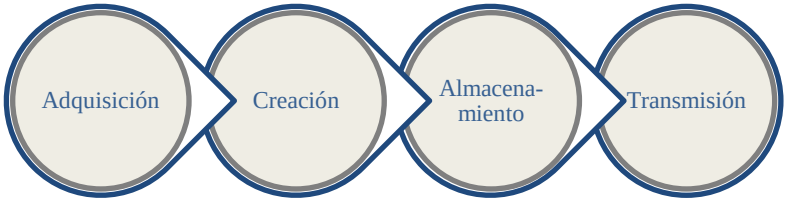
Fuente: Elaboración propia con información de Cornella, Alfons. (2000). La información no es necesariamente conocimiento. Infonomia.com: la empresa es información.

1.1.2 INFORMACIÓN

Una vez que los datos seleccionados, han sido analizados, bajo un contexto personal o colectivo, en un momento determinado, adquieren un sentido que los convierte en información. A diferencia de las máquinas cuya actividad es el manejo de datos, los seres humanos tienen la capacidad de crear información, dado que pueden interpretar los datos, brindándoles un sentido, el cual dependerá de factores como, el contexto en el cual se encuentra la persona responsable de la interpretación así como de sus capacidades para realizar el análisis *(Cornella, 2000).*

La información puede estar en cuatros estados (Figura 1.2 Estados de la información), la adquisición que se da a través de los sentidos vista, el olfato, el tacto, el gusto y el oído, la creación es posible gracias a las habilidades que los seres humanos poseen, el almacenamiento se logra mediante el uso de la memoria y en muchas ocasiones en medios externos y la transmisión, se da del sujeto, que mediante alguna tecnología transfiere la información a un dispositivo de almacenamiento temporal. *(Daltabuit, Hernández, Mallen, & Vázquez, 2007)*

Figura 1. 2 Estados de la información.



Fuente: Elaboración propia con información de Daltabuit, Enrique, Hernández, Leobardo, Mallen, Guillermo, & Vázquez, J. (2007). La seguridad de la información. México: Noriega Editores.

1.1.3 INFORMÁTICA

El término "informática" hace referencia al manejo de la información, que incluye desde su computación, sistematización, creación, almacenamiento y transmisión *(Daltabuit et al., 2007)*. El concepto de informática fue definido en 1983 por *(Gorn)* como la ciencia de la computación más la ciencia de la información.

La informática es de gran relevancia para las profesiones modernas ya que abarca desde disciplinas de información tradicional como los sistemas, la computación y las ciencias de la información y da firmeza a otras como la comunicación, los negocios, el diseño, entre otras *(Gammack, Hobbs, & Pigott, 2011)*.

1.2 SEGURIDAD DE LA INFORMACIÓN

Los avances en las tecnologías de la información han revolucionado considerablemente la forma en que se crea, se almacena y se transfiere la información, lo cual ha generado a su vez el surgimiento de nuevas amenazas, cuya finalidad es afectar la seguridad de los activos.

Las principales amenazas pronosticadas para el año 2013, con base en la información de un estudio del año 2012, de la empresa McAfee, indica que los dispositivos móviles y la nube, serán uno de los blancos de preferencia por los atacantes, seguido del malware que afecta a los equipos móviles y de cómputo, los ataques a gran escala y la insistencia de grupos como Anonymous sin duda representan una gran reto para las organizaciones e instituciones tanto nacionales como internacionales.

Considerando éstos pronósticos aunados a la falta de cultura de seguridad de la información y la importancia que en la actualidad han adquirido recursos como las redes sociales, donde 6 de cada 10 internautas en México accede a alguna red social y en los cuales el 90% hace uso de ellas como medio de comunicación con familiares y amigos *(AMIPCI, 2011)*, los dispositivos inteligentes y los servicios en la nube, que forman parte fundamental de la vida diaria tanto laboral como personal, muestra, que el tema de la privacidad de los datos personales, así como la importancia de la información que se transfiere, almacena y crea en estos medios es un asunto de gran preocupación.

En un estudio sobre la protección de datos personales entre usuarios y empresas realizado en 2012 por la Asociación Mexicana de Internet (AMIPCI), se identifican datos interesantes relacionados con el grado de importancia que los usuarios le otorgan a los datos personales, resultados que muestran que 31% de los evaluados en el estudio no pudieron definir el concepto de datos personales, siendo las redes sociales, la banca en línea y los portales de compras, los sitios donde con mayor frecuencia los usuarios dejan sus datos tanto de identificación, sensibles, patrimoniales y de salud principalmente.

Ante estas amenazas potenciales es fundamental que tanto las organizaciones como instituciones en México definan mecanismos para protección de la seguridad, no sólo de sus activos físicos, sino además de la información, los datos personales y la privacidad, la cual está definida en el artículo 6 de la Constitución Política de los Estados Unidos Mexicanos de 1917 como un derecho constitucional.

A continuación se presentan los principales conceptos relacionados con la seguridad de la información.

1.2.1 SEGURIDAD

El término seguridad se refiere a los resultados obtenidos al implementar y mantener medidas de protección, que permitan a una entidad cumplir con su misión y funciones críticas, no obstante los riesgos existentes en el uso de los sistemas de información. Las medidas de protección pueden incluir una combinación de estrategias cuyo objetivo es disuadir, prevenir, evitar, detectar, recuperar y corregir, para lo cual es fundamental que las estrategias estén integradas en un enfoque de gestión de riesgos *(CNSS, 2010)*.

La seguridad de la información se define como la protección de la información y de los sistemas de información, de acciones no autorizadas como, el acceso, el uso, la divulgación, la alteración y la modificación, con la finalidad de brindar servicios de seguridad como son la integridad (que la información no sea alterada sin autorización), la confidencialidad (que la información sólo sea conocida por quienes tienen derecho a ello) y la disponibilidad (que los usuarios autorizados puedan hacer uso de ésta cuando lo requieran) *(NIST, 2011)*. Vista como una disciplina, la seguridad de la información busca el cumplimiento de los servicios de seguridad, que previamente se hayan identificado como importantes o deseables, apoyándose en cinco pilares fundamentales (Figura1.3 Pilares de la seguridad de la información):

a) *Proceso:* es fundamental comprender como es procesada la información, para definir el conjunto de medidas que deben ser implementadas.

b) *Criptología:* disciplina que basada en técnicas variadas de matemáticas para proteger la confidencialidad, autenticidad e integridad de la información.

c) *Control de acceso:* metodologías implementadas para garantizar que sólo pueda acceder a la información o recursos el personal que cuente con la autorización debida.

d) *Buenas prácticas:* están integradas por políticas y normas específicas, las cuales deben estar alineadas con los objetivos de la organización.

e) *Mecanismos:* definidos como los medios específicos que serán utilizados para cumplir con los objetivos establecidos en aspectos relacionados con la seguridad de la información.

Figura 1. 3 Pilares de la seguridad de la información.

Fuente: Elaboración propia con información de Daltabuit, Enrique, Hernández, Leobardo, Mallen, Guillermo, & Vázquez, J. (2007). La seguridad de la información. México: Noriega Editores

1.2.2 SERVICIOS DE SEGURIDAD

El estándar *ISO 7498-2 Information processing systems -- Open Systems Interconnection -- Basic Reference Model -- Part 2: Security Architecture*, establece la diferencia entre los conceptos servicio y mecanismo de seguridad, el primero se refiere a una característica que debe tener un sistema, para satisfacer una política de seguridad, el servicio de seguridad identifica lo que es requerido, mientras que un mecanismo es un procedimiento concreto utilizado para implementar el servicio de seguridad, ya que describe cómo lograrlo *(Bertolín, 2008)*.

Los servicios de seguridad se clasifican en (Figura 1.4 Tabla clasificación de servicios de seguridad):

Figura 1. 4 Tabla clasificación de servicios de seguridad.

Servicio de seguridad	Descripción
Confidencialidad	Se refiere a la capacidad de asegurar que sólo las personas autorizadas puedan tener acceso al recurso, este servicio es responsable de preservar las restricciones autorizadas sobre el acceso y la divulgación de la información, así como incluir mecanismos como los métodos de criptografía, para proteger la privacidad personal y la propiedad de la información.
Autenticación	Servicio responsable de verificar la identidad de un usuario, proceso o dispositivo, a menudo como un requisito para permitir el acceso a determinado recurso. Se realiza principalmente a través de: - Algo que se sabe (contraseña). - Algo que se tiene (tarjeta de identificación). - Algo que se es (voz, retina, iris).
Integridad	Servicio encargado de la protección contra la modificación o destrucción de la información, asegurando que el contenido no haya sufrido cambio alguno.
Control de acceso	Servicio que tiene la habilidad para conceder, denegar o limitar el acceso a recursos específicos. El control de acceso es ejecutado para permitir el acceso al recurso solicitado, una vez que el usuario haya sido identificado y autenticado de forma exitosa.
No repudio	Servicio que garantiza al remitente que la información fue entregada al destinatario a quien a su vez le brinda pruebas de la identidad del remitente, esta protección se efectúa mediante una colección de pruebas irrefutables que servirán como prueba ante cualquier disputa.
Disponibilidad	Servicio que se cumple cuando el personal autorizado puede acceder al recurso cuando lo requiere y el número de veces que sea necesario.

Fuente: Elaboración propia con información de López B., Jaquelina, & Quezada R., Cintia. (2006). Fundamentos de Seguridad Informática (F. d. I. UNAM Ed.). México.
NIST, *National Institute of Standards and Technology*. (2011). *Glossary of Key Information Security Terms*. Consultado 22/02/2013, Obtenido de http://csrc.nist.gov/publications/nistir/ir7298-rev1/nistir-7298-revision1.pdf

1.2.3 AMENAZAS

Una amenaza es cualquier evento o circunstancia con el potencial de impactar negativamente en las operaciones, los activos de una organización, los individuos, otras organizaciones, o de un país, mediante el acceso no autorizado a un sistema de información o la destrucción, la divulgación o modificación de la información, así como la denegación de servicio *(NIST, 2012)*. Las amenazas en sí mismas no son acciones, para ser consideradas peligrosas deben ser generadas por una fuente de amenaza, definida como la intención y el método dirigido de forma intencional para la explotación de una vulnerabilidad específica o como situaciones que accidentalmente provoque una vulnerabilidad (*SANS, 2012)*.

Las fuentes de amenaza más comunes pueden ser de tres tipos:

Figura 1. 5 Fuentes de amenaza más comunes.

Naturales	Humanas	Ambientales
•Inundaciones, terremotos, tornados, deslaves, avalanchas, tormentas eléctricas y otros eventos similares.	•Eventos causados por los seres humanos,que pueden ser intencionales (ataques de red, software malicioso o acceso no autorizado a información confindencial) o accidentales (entrada de datos involuntaria o descuidos).	•Fallo en el suministro por largo plazo, contaminación, derrames de productos químicos, etcétera.

Fuente: Elaboración propia con información de NIST, *National Institute of Standards and Technology*. (2002). *Risk Management Guide for Information Technology Systems Special Publication 800-30*. Consultado 23/02/2013, Obtenido de http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

A continuación se presenta un listado parcial de amenazas que podrían afectar los activos de una organización.

- Revelación accidental.
- Actos de la naturaleza.
- Modificaciones intencionales en el software o en sistemas de información.
- Uso del ancho de banda.
- Interrupción o interferencia del suministro eléctrico.
- Modificación intencional de los datos.
- Error en la configuración de un sistema (accidental).
- Mal funcionamiento o interrupción de las telecomunicaciones.

1.2.4 VULNERABILIDADES

Una vulnerabilidad se define como una debilidad en un sistema de información, procedimiento de seguridad, controles internos o implementación, que podría ser explotada por una fuente de amenaza, ya sea de forma intencional o accidental, dando como resultado una brecha de seguridad o una violación a una política de seguridad.

Las vulnerabilidades no sólo se encuentran dentro de los sistemas de información o aspectos relacionados con tecnologías de la información, pueden presentarse debido a problemas en la estructura organizacional, lo cual se verá reflejado en estrategias débiles para la gestión de riesgo, decisiones inconsistentes y desviadas de la misión y visión de la organización, así como en la cultura de seguridad percibida en el entorno. *(NIST, 2012).*

1.2.5 ATAQUES

El término ataque se refiere a cualquier tipo de actividad que mediante la explotación de una vulnerabilidad pretende recolectar, interrumpir, denegar, degradar o destruir los recursos de los sistemas de información o la información en sí misma *(Daltabuit et al., 2007).*

Una clasificación general de los ataques es dividirlos en:

a) *Ataque pasivo:* consiste en la observación del comportamiento, sin alterar ni el estado del sistema ni la información, sólo afecta el servicio de seguridad de la confidencialidad, afectando la privacidad del sistema o de la información.

Ejemplo: monitoreo, espionaje de mensajes y análisis de tráfico.

b) *Ataque activo:* este tipo de ataque modifica o afecta la información o el estado del sistema o ambos, altera los servicios de confidencialidad, integridad, autenticidad.

Ejemplo: engaño, suplantación, réplica o modificación de mensajes y la negación de servicio.

1.2.6 NORMATIVA DE SEGURIDAD DE LA INFORMACIÓN

Dado el gran crecimiento y auge que en la actualidad han cobrado las tecnologías de la información y comunicaciones en diversos sectores, para el procesamiento, almacenamiento, manipulación y transmisión de la información, aunado a la evolución de nuevas amenazas y la sofisticación en las técnicas de ataques, ha sido necesario que tanto a nivel nacional como

internacional se establezcan mecanismos normativos para regular las estrategias, los controles y los procedimientos que las entidades implementan para mejorar la seguridad de sus activos.

El contar con un conjunto de normas y regulaciones nacionales e internacionales, ha generado una preocupación tanto en las instituciones, como en las empresas por implementar mecanismos de seguridad adecuados para lograr su cumplimiento, lo cual se verá reflejado en una ventaja competitiva, ya que aumentará tanto la confianza de los clientes o usuarios del servicio, como el reconocimiento e imagen de la entidad.

La figura 1.6 Normatividad de seguridad de la información, presenta un diagrama que integra las normativas, las regulaciones y los estándares nacionales e internacionales relacionados con la seguridad de la información, la privacidad, los datos personales, los delitos informáticos y los derechos de propiedad, los cuáles se mencionarán posteriormente.

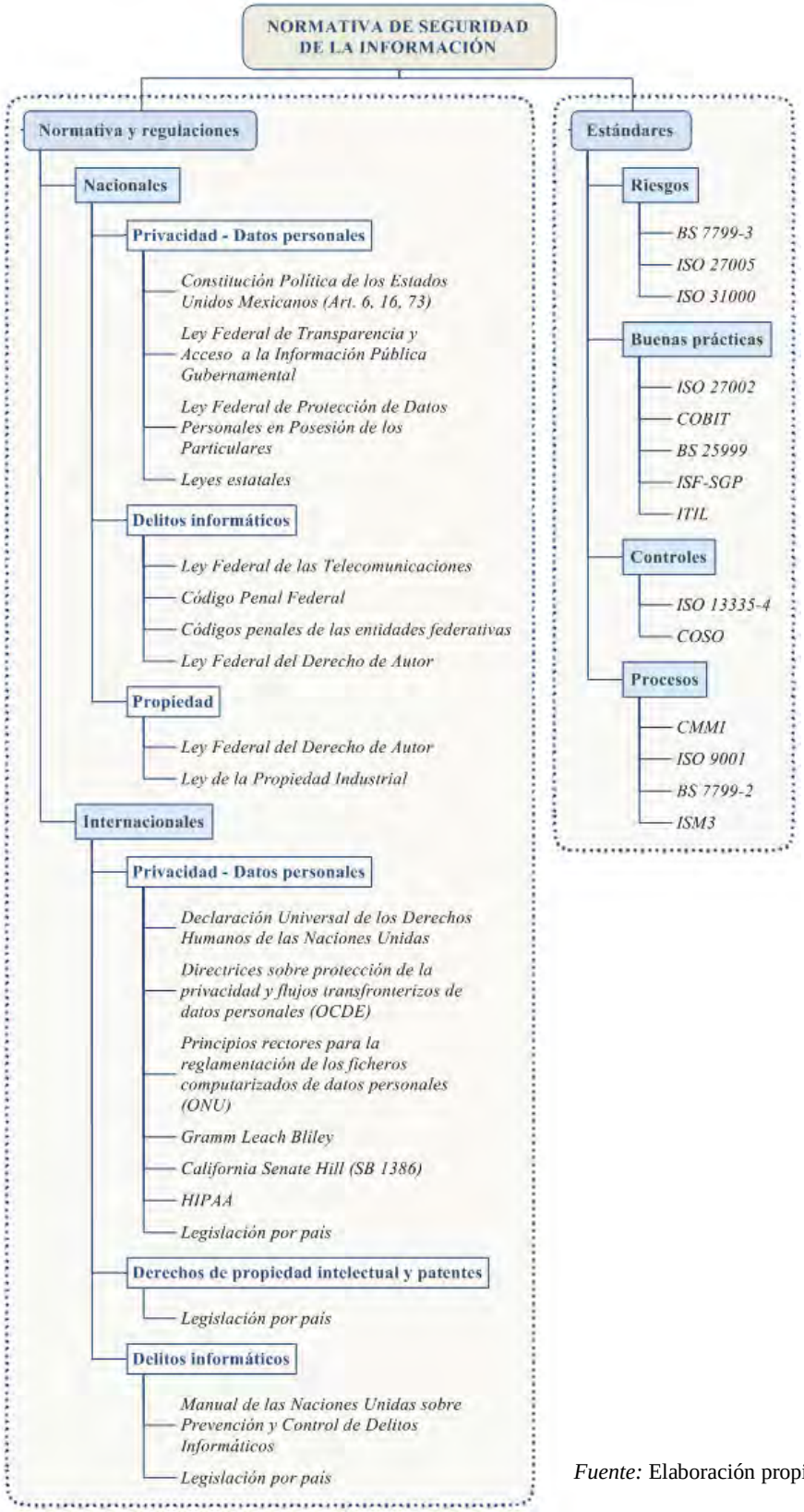
1.2.6.1 NORMATIVIDAD Y REGULACIONES

Para abordar el tema de las normas y regulaciones actuales en materia de seguridad de la información fueron clasificados considerando su alcance en nacionales e internacionales, incluyendo en el primer ámbito la legislación en materia de privacidad y datos personales, seguido de las leyes y códigos aplicables en materia de delitos informáticos, dicha clasificación fue incluida considerando las amenazas que atentan contra la información, por último se incluye un apartado relacionado con los derechos de propiedad. (Véase figura 1.7 Tabla de normatividad y regulaciones nacionales sobre seguridad de la información y figura1.8 Tabla de normatividad y regulaciones internacionales sobre seguridad de la información)

1.2.6.2 ESTÁNDARES

Los estándares sobre seguridad de la información han sido clasificados considerando su objetivo principal, identificando así, los estándares para la gestión de riesgos, seguidos de los estándares de buenas prácticas, los orientados a controles y finalmente los de procesos.
(Véase figura 1.9 Estándares sobre seguridad de la información)

Figura 1. 6 Normatividad de seguridad de la información



Fuente: Elaboración propia.

Figura 1. 7 Tabla de normatividad y regulaciones nacionales sobre seguridad de la información.

Normatividad y regulaciones NACIONALES	
Privacidad –Datos Personales	Constitución Política de los Estados Unidos Mexicanos • *Artículo 6* como resultado de una reforma del 2007 la protección de los datos fue reconocida como un derecho constitucional. Fracción II y III. • *Artículo 16* establece en su primer párrafo una cláusula general sobre privacidad, en 2009 se incluye como segundo párrafo de este artículo, el derecho de protección de los datos personales, así como las acciones (acceso, rectificación y cancelación), que el propietario puede realizar sobre éstos, además menciona la privacidad en las comunicaciones. • *Artículo 73* fue reformado en el 2009 para incluir como facultad del Congreso de la Unión la protección de los datos personales en poder de particulares. Fracción XXIX-O. *(CPEUM, 1917)*
	Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental. Legislación de ámbito federal, su objetivo es proveer lo necesario para garantizar el acceso de toda persona a la información en posesión de los Poderes de la Unión, los órganos constitucionales autónomos o con autonomía legal y cualquier otra entidad federal *(LFTAIPG, 2002)*.
	Ley Federal de Protección de Datos Personales en Posesión de los Particulares. Publicada en el año 2010, su objetivo es proteger los datos personales en posesión particulares, así como regular su tratamiento legítimo, controlado e informado para garantizar la privacidad y el derecho a la autodeterminación informativa de las personas *(LFPDPPP, 2010).*

Figura 1.7 Tabla de normatividad y regulaciones nacionales sobre seguridad de la información. (Continuación)

Privacidad y Datos Personales	Leyes Estatales • *Aguascalientes:* Ley de Transparencia e Información Pública del Estado. Artículos 23 y 27. • *Baja California:* Ley de Acceso a la Información Pública para el Estado. Artículos 25 y 28. • *Baja California Sur:* Ley de Transparencia y Acceso a la Información Pública para el Estado. Artículos 26 y 27. • *Campeche:* Ley de Transparencia y Acceso a la Información Pública del Estado. Artículos 31, 35 y 38. • *Chiapas:* Ley que garantiza la transparencia y el derecho a la información pública para el Estado. Artículo 43. • *Chihuahua:* Constitución Política del Estado. Artículo 4, Ley de Transparencia y Acceso a la Información Pública del Estado. Artículo 3, 38 y 39. • *Coahuila:* Ley de Acceso a la Información Pública y Protección de Datos Personales para el Estado. Artículos 62 y 69. • *Colima:* Ley de Transparencia y Acceso a la Información Pública del Estado. Artículo 17, Ley de Protección de Datos Personales del Estado. Artículo 7. • *Distrito Federal:* Ley de Transparencia y Acceso a la Información Pública del Distrito Federal. Artículo 12, Ley de Protección de Datos Personales para el Distrito Federal. Artículo 26 y 30. • *Durango:* Ley de Acceso a la información Pública del Estado. Artículos 44 y 48. • *Estado de México:* Ley de Transparencia y Acceso a la Información Pública. Artículos 5, 50 y 53. • *Guanajuato:* Ley de Protección de Datos Personales para el Estado. Artículos 9 y 10. • *Guerrero:* Ley de Acceso a la Información Pública del Estado. Artículo 19 y 20. • *Hidalgo:* Ley de Transparencia y Acceso a la Información Pública Gubernamental del Estado. Artículos 15 y 40. • *Jalisco:* Ley de Transparencia e Información Pública del Estado. Artículo 30, Código Civil del Estado. Artículos 40 bis 10, bis 11 y bis 24. • *Michoacán de Ocampo:* Ley de Transparencia e Información Pública del Estado. Artículos 65 y 66. • *Morelos:* Ley de Información Pública, Estadística y Protección de Datos Personales del Estado. Artículos 21 y 61. • *Nayarit:* Ley de Transparencia y Acceso a la Información Pública del Estado. Artículo 25. • *Nuevo León:* Ley de Transparencia y Acceso a la Información del Estado. Artículos 55 y 56. • *Oaxaca:* Ley de Transparencia y Acceso a la Información Pública del Estado. Artículo 40, Ley de Protección de Datos Personales del Estado. Artículos 6, 18 y 20. • *Puebla:* Ley de Transparencia y Acceso a la Información Pública del Estado. Artículo 19. • *Quintana Roo:* Ley de Transparencia y Acceso a la Información Pública del Estado. Artículos 32 y 33.

Figura 1.7 Tabla de normatividad y regulaciones nacionales sobre seguridad de la información. (Continuación)

Privacidad y Datos Personales	• *San Luis Potosí:* Ley de Transparencia Administrativa y Acceso a la Información Pública del Estado. Artículos 12, 51 y 57. • *Sinaloa*: Ley de Acceso a la Información Pública del Estado. Artículo 35. • *Sonora:* Ley de Acceso a la Información Pública del Estado. Artículo 32. • *Tabasco:* Ley de Transparencia y Acceso a la Información Pública del Estado. Artículo 57. • *Tamaulipas*: Ley de Transparencia y acceso a la Información Pública del Estado. Artículos 6 y 36. • *Tlaxcala:* Ley de Acceso a la Información Pública y Protección de Datos Personales para el Estado. Artículos 43 y 47. • *Veracruz:* Ley de Transparencia y Acceso a la Información Pública para el Estado. Artículos 19, 22 y 23. • *Yucatán:* Ley de Acceso a la Información Pública del Estado y los municipios. Artículos 21 y 26. • *Zacatecas:* Ley de Acceso a la Información Pública del Estado. Artículo 34. *(ITEI, 2010)*
Delitos Informáticos	Ley Federal de las Telecomunicaciones Creada en 1995, con el objeto de regular el uso, aprovechamiento y explotación del espectro radioeléctrico, de las redes de telecomunicaciones y de la comunicación vía satélite. Como parte de las últimas reformas se añadió la obligación de cuidar los datos personales a las empresas particulares que son concesionarias de redes públicas de telecomunicaciones. *(LFT, 1995)*
	Ley Federal del Derecho de Autor Ley creada en 1996, que en su capítulo IV titulado "De los programas de computación y las bases de datos" incluye en los artículos 101 a 114, regulaciones para la protección de los programas y las bases de datos, mediante la obtención de un certificado autoral expedido por el Instituto Nacional del Derecho de Autor (INDA). El título VIII "De los registros de derechos" capítulo I artículo 164 y el capítulo II " De las infracciones en materia de comercio" artículo 231 fracción V, los cuales se refieren a la protección de los programas de computación, así como de las bases de datos, además de incluir las infracciones en las que se incurran por uso indebido con fines lucrativos directa o indirectamente *(LFDA, 1996)*.
	Código Penal Federal Regula los delitos informáticos en su título noveno, capítulo II, referido a la revelación de secretos y acceso ilícito a equipos y sistemas informáticos. Artículos 211 bis 1 a 211 bis 7 *(CPF, 1931*).

Figura 1.7 Tabla de normatividad y regulaciones nacionales sobre seguridad de la información. (Continuación)

Delitos Informáticos	Códigos penales de las entidades federativas • *Distrito Federal:* Código Penal del Distrito Federal. Artículos 336 y 355. • *Estado de México:* Código Penal del Estado de México. Artículo 174. • *Jalisco:* Código Penal para el Estado Libre y Soberano de Jalisco. Artículo170 bis. • *Nuevo León:* Código Penal para el Estado de Nuevo León. Artículos 242 bis, 365, 427,428 y 429. • *Quintana Roo:* Código Penal para el Estado Libre y Soberano de Quintana Roo. Artículo 189 bis. • *Sinaloa:* Código Penal para el Estado de Sinaloa. Artículo 217. *(Piña Libien, 2006)*
Propiedad	Ley Federal del Derecho de Autor Creada en 1996, el artículo 11 establece el reconocimiento del Estado al creador de obras literarias o artísticas, entre las que se incluyen los programas de cómputo. La reproducción queda protegida a favor del autor y se prohíbe la fabricación o uso de sistemas o productos destinados a eliminar la protección de los programas *(LFDA, 1996).*
	Ley de la Propiedad Industrial Creada en 1991 con el objetivo de proteger la propiedad industrial, mediante la regulación y otorgamiento de patentes de invención registros de modelos de utilidad, diseños industriales, marcas, y avisos comerciales; publicación de nombres comerciales; declaración de protección de denominaciones de origen, y regulación de secretos industriales *(LPI, 1991).*

Fuente: Elaboración propia.

Figura 1. 8 Tabla de normatividad y regulaciones internacionales sobre seguridad de la información.

Normatividad y regulaciones INTERNACIONALES	
Privacidad –Datos Personales	Declaración Universal de los Derechos Humanos de las Naciones Unidas. Desde el año de 1948 en su artículo 19 incluye el derecho a investigar y recibir información, así como difundirla por cualquier medio de expresión *(ITEI, 2010)*.
	Directrices sobre protección de la privacidad y flujos transfronterizos de datos personales. Creadas en 1980 por la Organización para la Cooperación y el Desarrollo Económico (OCDE), en dicho documento se establecen los principios de aplicación tanto nacional como internacional, para el sector público y privado, considerándose como los estándares mínimos para completar medidas de protección de la privacidad y de las libertades individuales, la participación individual que incluye el derecho de controlar los datos personales, el derecho de comunicación sobre éstos y el derecho de reclamación, para en caso de ser procedente decidir si se eliminan, rectifican, completan o corrigen *(OCDE, 1980)*.
	Principios rectores para la reglamentación de los ficheros computarizados de datos personales. Adoptado por las Naciones Unidas en 1990, incluyendo en "Principios relativos a las garantías mínimas que deberán preverse en la legislación Nacional", el derecho de toda persona, para conocer sin restricción alguna el fin que tienen sus datos y el destinatario de éstos, siempre y cuando manifieste su interés y que demuestre su identidad como propietario de los datos *(ONU, 1990)*.
	Gramm Leach Bliley Ley federal sobre la privacidad aprobada en 1999 regula el tratamiento de la información personal y confidencial que las empresas estadounidenses de servicios financieros recopilan como parte de sus actividades, contiene elementos de privacidad y gestión de seguridad de tecnologías de la información *(United States Congress, 1999)*.
	California Senate Hill (SB1386) Ley aprobada en el estado de California en Estado Unidos en el año 2003, cuyo objetivo es obligar a cualquier entidad o persona que almacena o transmite datos personales de los residentes del estado de California a notificar a los propietarios de los datos, cuando éstos hayan sido comprometidos por algún problema de seguridad, lo cual impulsa a las organizaciones a implementar tecnologías de cifrado, así como estrategias para mejorar la respuesta a incidentes de seguridad *(California Senate, 2003)*.

Figura 1.8 Tabla de normatividad y regulaciones internacionales sobre seguridad de la información. (Continuación)

Privacidad y Datos Personales	HIPAA *Health Insurance Portability and Accountability (HIPAA)*, Ley de Portabilidad y Responsabilidad del Seguro Médico, aprobada en 1996 por el Congreso de Estados Unidos, su objetivo es establecer la regulación para la protección de los datos de los pacientes, considerando los tres puntos del triángulo CID (Confidencialidad, Disponibilidad e Integridad). Se divide en cinco títulos o secciones: I. Portabilidad. II. Simplificación administrativa. III. Disposiciones de salud relacionadas a impuestos. IV. Aplicación y cumplimiento de los requisitos de planes grupales de salud. V. Retención de ingresos. (USA Congress, 1996)
Delitos Informáticos	Manual de las Naciones Unidas sobre Prevención y Control de Delitos Informáticos. En este documento se hace referencia a la definición de delitos informáticos y se presenta una clasificación que incluye: fraudes cometidos mediante manipulación de computadoras, falsificaciones informáticas, daño o modificaciones de programas o daños computarizados *(Tellez, 2004)*.
	Legislación por país. • Estados Unidos: Acta Federal de Abuso Computacional (18 U.S.C. Sec. 1030) 1994. • Alemania: Ley contra la Criminalidad Económica 1986. • Austria: Ley de reforma del Código Penal, 1987, artículo 148. • Gran Bretaña: *Computer Misuse Act*, Ley de Abusos Informáticos, 1991. • Holanda: Ley de Delitos Informáticos, 1993. • Francia: Ley relativa al fraude informático, 1988, • España: Nuevo Código Penal de España, artículos 264-2 y 248. *(Tellez, 2004)*

Fuente: Elaboración del autor.

Figura 1. 9 Estándares sobre seguridad de la información. (Continuación)

Estándares	
Riesgos	BS 7799-3 *Information security management systems – Part 3: Guidelines for information security risk management* Publicado en 2006 por *British Standards Institution* (BSI), corresponde a la tercera parte de BS 7799, dedicado a la gestión de riesgos de seguridad de la información, brinda directrices sobre la forma de evaluar, tratar, re-evaluar y monitorizar los riesgos, así como el proceso de toma de decisiones por parte de la dirección *(BSI, 2006a)*.
	ISO 27005 *Information technology - Security techniques - Information security risk management.* Estándar que proporciona las directrices relacionadas con la gestión de riesgos de seguridad de la información en una organización, apoyado en los requisitos establecidos por la norma ISO 27001 *Information technology – Security techniques – Information security management systems – Requirements*. Es aplicable a todo tipo de organización, no recomienda una metodología específica, ya que eso dependerá del alcance y del tipo de sector al que pertenezca la organización *(ISO/IEC, 2008)* .
	ISO 31000 *Risk management — Principles and guidelines* Norma internacional que brinda principios y directrices genéricas sobre la gestión del riesgo, puede utilizarse por cualquier organización, no es específica de una industria o sector concreto. El enfoque está estructurado en tres elementos claves, para una efectiva gestión de riesgos *(ISO, 2009)*: • Principios de gestión del riesgo. • Marco de trabajo para la gestión de riesgos. • El proceso de gestión de riesgos.
Buenas prácticas	ISO 27002 *Information technology — Security techniques — Code of practice for information security management* Tuvo su origen en el estándar ISO 17799 *Information technology -- Security techniques -- Code of practice for information security management*, que a su vez es descendiente del BS 7799. ISO 27002 incluye un conjunto de prácticas recomendadas (buenas prácticas) a nivel mundial para garantizar la seguridad de la información a nivel institucional, su cumplimiento no es obligatorio, sin embargo proporciona una base sólida para un programa de seguridad de la información, orientada a la preservación de los atributos de confidencialidad, integridad y disponibilidad de la información. Contiene 39 objetivos de control y 133 controles aplicables, agrupados en 11 dominios: 1. Políticas de seguridad. 2. Organización de la seguridad de la información. 3. Gestión de activos. 4. Seguridad de los recursos humanos.

Figura 1. 9 Estándares sobre seguridad de la información. (Continuación)

Buenas prácticas	5. Seguridad física y ambiental. 6. Gestión de comunicaciones y operaciones. 7. Control de acceso. 8. Sistemas de información; adquisición, desarrollo y mantenimiento. 9. Gestión de incidentes de seguridad de la información. 10. Gestión de la continuidad del negocio. 11. Conformidad. *(ISO/IEC, 2005)*
	COBIT *Control Objectives for Information and related Technology* *Control Objectives for Information and related Technology* (COBIT), modelo que proporciona buenas prácticas mediante un marco referencial de dominios y procesos. Provee guías detalladas sobre objetivos de control para los procesos de gestión de tecnología de información, sus objetivos principales son investigar, desarrollar, publicar y promover un conjunto de objetivos de control de TI internacionales, actualizados para ser una herramienta para gerentes de negocio y auditores, se divide en 34 procesos pertenecientes a cuatro dominios o recursos de TI, los cuáles dan una visión completa de cómo controlar, gestionar y medir un proceso. 1. Planeación y Organización (PO) 2. Adquisición e Implementación (AI) 3. Entrega y soporte (ES) *4.* Monitoreo (M) *(ISACA, 2005)*
	BS 25999 *Business Continuity Management (BCM)* Creado en el año de 2006 por el *British Standards Institution (*BSI). El BSI 25999-1 define un conjunto de buenas prácticas dedicadas a la gestión de la continuidad de negocio, puede ser utilizado por cualquier organización, sin importar su tamaño o el sector al cual pertenezca. Establece el proceso para que una organización pueda desarrollar e implementar la continuidad de negocio, incluyendo una lista completa de controles basadas en las mejores prácticas de *Business Continuity Management (BCM).* *(BSI, 2006b).*
	ISF-SGP *Information Security Forum: The Standard of Good Practice for Information Security* Estándar de buenas prácticas para la seguridad de la información, *Standard of Good Practice for Information Security*, creado con el objetivo de ayudar a las organizaciones con los riesgos asociados a los sistemas de información, sin importar su estructura o tamaño. ISF-SGP es una herramienta de gran importancia para mejorar la calidad y la eficiencia de los controles aplicados a la organización *(ISF, 2003).*
	ITIL *Information Technology Infraestructure Library* *Information Technology Infraestructure Library* (ITIL) surge durante los años 80 en el Reino Unido, como un modelo dedicado a la gestión de las operaciones y servicios de los sistemas y tecnologías de la información y comunicaciones, nace de un conjunto de publicaciones de las mejores prácticas para la gestión de servicios de tecnologías de la

Figura 1. 9 Estándares sobre seguridad de la información. (Continuación)

	información integradas bajo el enfoque de procesos, provee una terminología estándar, interdependencia entre los procesos, lineamientos para la implementación, para la definición de roles y responsabilidades de los procesos, lista de chequeo de madurez, así como lo que se debe hacer y lo que no *(Addy, 2007)*.
Controles	ISO 13335-4 *Information technology — Guidelines for the management of IT Security — Part 4:Selection of safeguards* Estándar que proporciona un conjunto de guías para la administración de la seguridad de las TI, está dirigido a los responsables de administrar la seguridad, ya que pueden aplicar ésta guía en las diferentes áreas de trabajo. Los objetivos principales de ISO 13335 son la definición y descripción de los conceptos asociados con seguridad de tecnologías de la información (TI), identificación de las relaciones existentes entre la administración de seguridad en TI con la administración general de TI, presentación de modelos definidos para el análisis e implementación de una estructura adecuada de seguridad en TI, además de proveer una guía general de referencia para la evaluación e implementación de seguridad de TI. El ISO 13335-4 provee guías para la selección de controles que puedan ser implementados para llevar a cabo la administración de la seguridad *(ISO/IEC, 2000)*.
	COSO *Committee of Sponsoring Organizations* de la *Treadway Commision* *Committee of Sponsoring Organizations* de la *Treadway Commision* (COSO) fue creado en 1985 con la finalidad de identificar los factores que ocasionan informes financieros fraudulentos y emitir un conjunto de recomendaciones que garanticen la máxima transferencia informativa. COSO establece una definición común de controles internos, normas y criterios, los cuales permiten a las empresas y organizaciones evaluar sus sistemas de control *(COSO, 2009)*.
Procesos	CMMI *Capability Maturity Model Integration* *Capability Maturity Model Integration (*CMMI), fusiona los modelos de mejora de procesos para ingeniería de sistemas, de software, desarrollo de productos integrados y adquisición del software, su primera versión fue publicada en enero del 2002. Es un modelo descriptivo que detalla los atributos esenciales que deberían caracterizar a una organización en un determinado nivel de madurez, al ser un modelo de calidad del software, clasifica a las organizaciones en niveles de madurez, que permite conocer la madurez de los procesos que se realizan para producir software *(SEI, 2010)*.
	ISO 9001 Sistemas de gestión de la calidad — Requisitos Norma internacional, genérica e independiente de cualquier industria o sector económico, aplicable a todos los tipos y tamaños de empresas, que específica los requisitos para implantar un sistema de gestión de calidad, utilizado por las organizaciones para demostrar su capacidad de satisfacer los requisitos del cliente. ISO 9001 establece principios para mejorar la calidad final de producto o servicio mediante la adopción de sencillas mejoras en la organización de la empresa. El estándar está basado en un modelo de proceso y desarrolla los ocho principios de la

Figura 1. 9 Estándares sobre seguridad de la información. (Continuación)

Procesos	gestión de calidad, que actúan como base y fundamento de las normativas *(ISO, 2008a).*
	BS 7799-2 *Information security management systems- specification with guidance for use.* Estándar que se encarga de auditar y certificar a aquellas empresas solicitantes, que hayan desarrollado un Sistema de Gestión de Seguridad de la Información (SGSI), el cuál es un enfoque sistémico para gestionar, información sensible en la organización, con el objetivo de reforzar la seguridad de la misma. BS 7799-2 es una guía de auditoría del SGSI basada en los requisitos que deben ser cubiertos por la organización *(BSI, 2002).*
	ISM3 *Information Security Management Maturity Model* *Information Security Management Maturity Model (ISM3),* es un estándar abierto creado por Vicente Aceituno, el objetivo de los sistemas de gestión de seguridad (ISM) es prevenir o mitigar los ataques, errores y accidentes que representen una amenaza a la seguridad de los sistemas de información y los procesos organizativos soportados por éstos. ISM3 cuenta con cinco niveles de madurez los cuales se adaptan a los objetivos de seguridad de la organización y a los recursos que están disponibles *(ISM3 Consortium, 2007).*

Fuente: Elaboración propia.

1.3 DATOS CLÍNICOS

En la actualidad no hay un término estandarizado para referirse a los datos clínicos, que en algunas ocasiones son mencionados mediante palabras como expediente clínico, datos o historial médico, e información o ficha clínica, en México para hacer referencia a los datos clínicos, se emplea con mayor frecuencia el término expediente clínico y recientemente en el artículo 3, fracción VI, de la LFPDPPP[1] se incluye dentro de la definición de datos personales sensibles, elementos que forman parte de los datos clínicos, como son, el estado de salud presente y futuro, la información genética, y la preferencia sexual, dada esta situación es de suma importancia que la legislación en México, considere la incorporación y definición puntual de los datos clínicos y los datos genéticos, con el objeto de estandarizar términos y evitar posibles confusiones.

Para el presente estudio se considerará el término dato clínico para hacer referencia a todos aquellos resultados obtenidos a partir de observaciones, mediciones y evaluaciones que permitan determinar el estado de salud de un paciente y con ello definir las acciones a seguir para su tratamiento.

De forma que el expediente clínico estará conformado por el conjunto de datos clínicos y datos personales, que mediante un orden y una estructura determinada, recopilara cronológicamente todos los aspectos relacionados con la salud de un paciente. El expediente clínico representa una base para

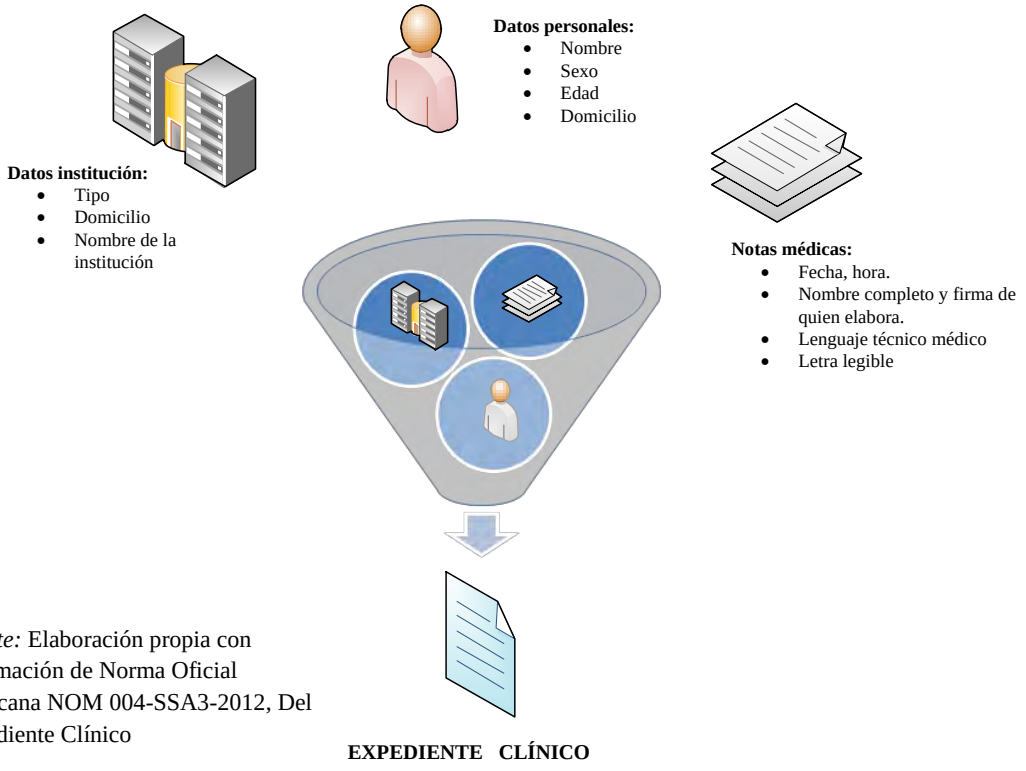
[1] Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

conocer las condiciones de salud, los actos médicos y los diferentes procedimientos ejecutados por el equipo médico para brindar el servicio *(DGIS, 2011)*.

El expediente clínico es definido formalmente en 1998 en la Norma Oficial Mexicana NOM-168-SSA1-1998, Del Expediente Clínico, como el conjunto de documentos escritos, gráficos e imagenológicos o de cualquier otra índole, en los cuales el personal de salud, deberá hacer registros, anotaciones y certificaciones correspondientes a su intervención, con arreglo a las disposiciones sanitarias. La norma fue actualizada en el año 2012 quedado actualmente con el nombre de NOM-004-SSA3-2012 Del expediente clínico.

El apartado 5 de la NOM-004-SSA3-2012, Del Expediente Clínico, indica los datos generales que debe incluir el expediente clínico (Figura 1.10 Datos generales que integran el expediente clínico), los cuáles son: el tipo, domicilio y nombre de la institución a la que pertenece el paciente, de éste último se incluirán sus datos personales como nombre, sexo, edad y domicilio, las notas médicas que sean adicionadas en el expediente deberán tener la fecha, hora, así como el nombre completo y firma de quién la elabora, deberán ser expresadas en lenguaje técnico médico, sin incluir abreviaturas, con letra legible sin tachaduras y ser conservadas en buen estado *(SSA, 1998)*.

Figura 1. 10 Datos generales que integran el expediente clínico.



Fuente: Elaboración propia con información de Norma Oficial Mexicana NOM 004-SSA3-2012, Del Expediente Clínico

1.4 TRATAMIENTO JURÍDICO DE LOS DATOS CLÍNICOS

1.4.1 PANORAMA NACIONAL

Para explicar el panorama actual en materia jurídica sobre los datos clínicos, se hará mención de la situación actual del expediente clínico en México y de los datos personales que se encuentran integrados en éste, considerando que en la actualidad México no cuenta con alguna definición formal que establezca el término datos clínicos.

Los datos clínicos en México han generado una gran polémica, que surge a partir de la promulgación de nuevas leyes creadas para la protección de los datos personales, tanto para el sector público como el privado, además de la exigencia por parte de los pacientes en su derecho a estar informados, en acceder a su información y solicitar la confidencialidad de la misma y la postura sobre la propiedad de los expedientes clínicos, considerando por un lado que los datos que integran el expediente clínico son tanto objetivos como subjetivos, que si bien son del paciente y sobre él, también incluye una interpretación por la parte médica que surge como resultado de aplicar al paciente interrogatorios, exploraciones físicas y estudios clínicos, que permitirán definir las acciones a seguir para el tratamiento de la enfermedad, estas directrices serán establecidas con base al conocimiento del médico tratante.

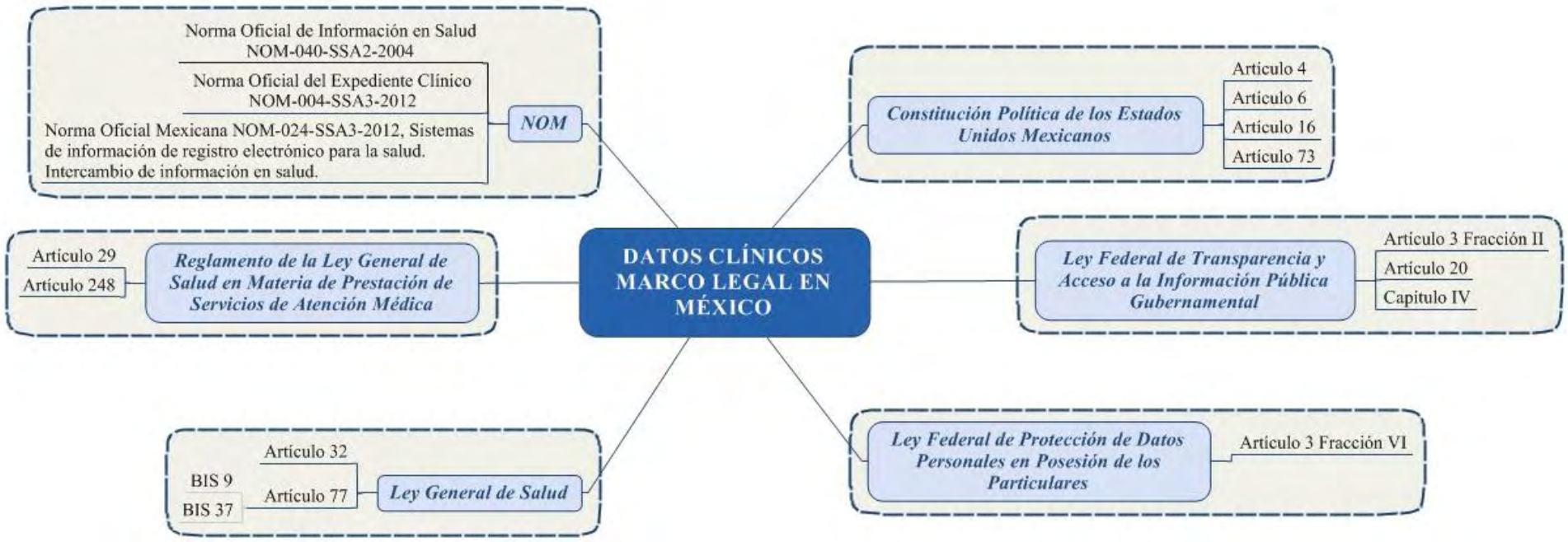
Dado este problema sobre la propiedad del expediente clínico, la Norma Oficial Mexicana NOM-004-SSA3-2012, Del Expediente Clínico en su apartado 5.4 establece que el expediente clínico es propiedad de la institución y del prestador de servicios médicos y considerando por un lado el derecho del paciente en acceder a la información y por otro lado desde la perspectiva médica el resguardo del secreto médico y del proceso previo a establecer un diagnóstico, se determinó en esta misma norma, la obligación del médico en plasmar en un resumen clínico, los aspectos relevantes de la atención médica brindada al paciente y que se encuentran ya incluidos en su expediente clínico, el resumen deberá incluir como mínimo: el padecimiento actual, diagnósticos tratamientos, evolución, pronóstico, estudios de laboratorio y de gabinete.

Sin embargo al considerarse al expediente clínico como un instrumento legal de evidencia sobre la actuación del profesional de la salud, que si bien es propiedad de la institución y del prestador de servicios médicos, éstos últimos están en la obligación de entregarlo a las autoridades competentes (autoridad judicial, órganos de procuración de justicia, autoridades sanitarias y comisiones de arbitraje médico) en caso de ser requerido.

Por otro lado considerando la definición previamente establecida para los datos clínicos, como objeto de estudio de este documento, es necesario establecer el marco legal en México relacionado con éstos, dado que las leyes actuales en materia de datos personales incluyen a los datos clínicos dentro de la definición de datos personales sensibles.

Las figuras 1.11 Marco legal en México en materia de datos clínicos y 1.12 Tabla sobre el Marco legal en México sobre datos clínicos, brindan un panorama general sobre el marco legal existente en México relacionado con los datos clínicos:

Figura 1. 11 Marco legal en México en materia de datos clínicos.



Fuente: Elaboración propia con información *de*

Gabuardi, Carlos A. El Marco Jurídico de la Información en Materia de Salud en México.
Leal, Héctor Vázquez, Campos, Raúl Martínez, Domínguez, Carlos Blázquez, & Sheissa, Roberto Castañeda. Un expediente clínico electrónico universal para México: características, retos y beneficios.
Salvador Rosas, Griselda. (2007). La protección de los datos personales en expedientes clínicos, un derecho fundamental de todo individuo. (Licenciado en Derecho Licenciatura), UNAM. Consultado en http://132.248.9.195/pd2007/0618485/Index.html
Sánchez-González, JM, & Ramírez-Barba, EJ. El expediente clínico en México

Figura 1. 12 Tabla sobre el Marco legal en México sobre datos clínicos.

DATOS CLÍNICOS Y EL MARCO LEGAL EN MÉXICO
Constitución Política de los Estados Unidos Mexicanos
• *Artículo 4* sobre el derecho de la protección a la salud. • *Artículo 6* reforma para incluir la protección de los datos personales. • *Artículo 16* garantizar la intimidad y privacidad sobre la protección de datos. • *Artículo 73* fracción XXIX-O incluido para considerar la protección de los datos personales en posesión de los particulares.
Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental
Interpreta que el expediente clínico se integra bajo el concepto de datos personales y obliga a las instituciones de gobierno a entregar copia completa del expediente a solicitud del paciente. • *Artículo 3 Fracción II* presenta la definición de datos personales que incluye los datos sobre el estado de salud físico o mental, preferencias sexuales u otros que afecten la intimidad del propietario. • *Capítulo IV* establece un marco general que regula la obtención, transmisión, uso y manejo de los datos personales en posesión de dependencias y entidades federales. • *Artículo 20* establece las responsabilidades sobre los datos personales por parte de los sujetos obligados.
Ley Federal de Protección de Datos Personales en Posesión de los Particulares
• *Artículo 3 Fracción VI* establece la definición de los datos personales sensibles que incluye aspectos como el estado de salud presente y futuro así como la información genética.
Ley General de Salud
Establece las primeras referencias al expediente clínico. • *Artículo 32* fundamentos de la Norma Oficial Mexicana NOM-168-SSA1-1998, Del Expediente Clínico y el uso de medios electrónicos. • *Artículo 77 bis 9* sobre integración de expedientes clínicos • *Artículo 77 bis 37* establece que los beneficiarios de sistema de protección social en salud tiene derecho a un expediente clínico.
Reglamento de la Ley General de Salud en materia de prestaciones de servicios de atención médica
• *Artículo 29* establece el deber de todo profesional de salud en proporcionar al usuario, familia, tutor o representante legal información completa sobre el diagnostico, pronostico y tratamiento correspondiente. • *Artículo 248* protege los expedientes clínicos del área de salud mental contra la divulgación cuando esta sea sin fines científicos o terapéuticos.
Norma Oficial Mexicana NOM-004-SSA3-2012, Del Expediente Clínico
Dirigida a sistematizar, homogeneizar y actualizar el manejo del expediente clínico.
Norma Oficial Mexicana NOM-024-SSA3-2012, Sistemas de información de registro electrónico para la salud. Intercambio de información en salud.
Regular los Sistemas de Información de Registro Electrónico para la Salud, así como establecer los mecanismos para que los Prestadores de Servicios de Salud del Sistema Nacional de Salud registren, intercambien y consoliden información.
Norma Oficial Mexicana NOM-040-SSA2-2004, En materia de información en salud.
Norma mexicana que establece los criterios para obtener, integrar, organizar, procesar, analizar y difundir la información en salud.
Programa Sectorial de Salud 2013-2018
Documento que fue creado para el sexenio del presidente Enrique Peña Nieto y considera dentro de las estrategias a seguir la implantación del expediente clínico electrónico.

Fuente: Elaboración propia con información *de Gabuardi, Carlos A. El Marco Jurídico de la Información en Materia de Salud en México.*

1.4.2 PANORAMA INTERNACIONAL

El tema de los datos clínicos a nivel internacional también ha generado preocupación tanto en temas relacionados con la seguridad de la información, la propiedad, la privacidad, la protección de los datos personales y la incorporación de un expediente clínico electrónico, que sin duda requiere la integración de las tecnologías de la información y comunicaciones, representando así un grande reto para los países que lo han incorporado y los que desean hacerlo.

Las figuras 1.13 Datos clínicos y el marco legal internacional y 1.14 Marco legal internacional sobre los datos clínicos, muestran un panorama general en materia de datos clínicos de diferentes organismos internacionales y países, así como los principales estándares utilizados en la actualidad.

Figura 1. 13 Datos clínicos y el marco legal internacional.

Fuente: Elaboración propia con información *de*
Leal, Héctor Vázquez, Campos, Raúl Martínez, Domínguez, Carlos Blázquez, & Sheissa, Roberto Castañeda. Un expediente clínico electrónico universal para México: características, retos y beneficios.
DGIS, Dirección General de Información en Salud. (2011). Manual del Expediente Clínico Electrónico.

Figura 1. 14 Marco legal internacional sobre los datos clínicos.

DATOS CLÍNICOS MARCO LEGAL INTERNACIONAL
OMS Organización Mundial de la Salud
Establece la importancia de los expedientes clínicos como un medio para la recolección de la información relativa a la salud.
Consejo de Europa Recomendación (97) 5
Define a los datos médicos como aquellos referidos a todos los datos personales relativos a la salud de un individuo.
Unión Europea directiva 95/46/CE
Define los datos de salud como una categoría especial de datos.
Declaración Ibero- Latinoamérica sobre derecho, bioética y genoma humano de 2001
Dentro de sus funciones es promover la legislación que regule el almacenamiento y difusión de la información genética individual de tal forma que se respete la privacidad y la intimidad de cada persona.
Normativa Española
Reconoce la propiedad tanto del paciente en cuanto a datos personales como al médico en el caso de las anotaciones, de forma que el paciente tiene derecho a obtener copia del expediente clínico y el médico puede elegir si incluye o no todos los comentarios. Ley 41/2002 de España establece la definición de información clínica.
República de Chile
El Código Sanitario establece que la ficha clínica pertenece al establecimiento de salud, quien tiene la obligación de entregar un resumen cuando se solicite.
República de Argentina
Obliga a los médicos y establecimientos de salud a entregar los datos que integran la historia clínica, al menos cada seis meses para que el paciente pueda verificarlos y actualizarlos.
Venezuela
Código de Deontología Médica Establece que el médico tiene derecho a la propiedad intelectual de la historia médica, pero la información contenida en la historia clínica es del paciente.
Estándares
• **HL7:** *Health Level Seven International*, Estándar de mensajería para el intercambio electrónico de información clínica basada en el *Reference Information Model* (RIM). • **CIE-10:** Corresponde a la clasificación internacional de enfermedades, por sus siglas en inglés: *International Statistical Classification of Diseases and Related Health Problems*. En México y en países como Estados Unidos se sigue usando dicha versión de clasificación en los sistemas de gestión hospitalaria. • **DICOM:** *Digital Imaging and Communication in Medicine* es un estándar reconocido internacionalmente para el intercambio de imágenes médicas, pensado para el manejo, almacenamiento, impresión y transmisión de imágenes médicas. • **LOINC:** *Logical Observation Identifiers Names and Codes* contiene un conjunto de códigos universales para identificar observaciones clínicas y laboratorio. • **SNOMED CT:** *Systematized Nomenclature of Medicine Clinical Terms*, esta nomenclatura de términos médicos y clínicos fue desarrollada en Estados Unidos, con el objeto de contar con un lenguaje universal.

Fuente: Elaboración propia con información *de Leal, Héctor Vázquez, Campos, Raúl Martínez, Domínguez, Carlos Blázquez, & Sheissa, Roberto Castañeda. Un expediente clínico electrónico universal para México: características, retos y beneficios. DGIS, Dirección General de Información en Salud. (2011). Manual del Expediente Clínico Electrónico*

1.5 IMPORTANCIA DE LA SEGURIDAD DE LOS DATOS CLÍNICOS

Los avances en el campo de la ciencia y la tecnología han transformado la dinámica social, las formas actuales de comunicación, creando a su vez la necesidad de incorporar las tecnologías de la información y comunicaciones en diversos sectores de México, el sector salud, no se ha quedado atrás, incorporando tecnologías que van más allá de la infraestructura, ésta situación aunada a la creciente demanda de los servicios médicos requiere métodos y recursos tecnológicos que permitan agilizar el proceso de atención a los pacientes, para brindar un servicio de calidad, reducir errores, estandarizar procedimientos e implementar mecanismos para proteger los datos clínicos y personales de los pacientes.

Los principales retos que actualmente enfrenta el sector público de salud en México se presentan a continuación:

- *Información dispersa:* no se cuenta con un expediente clínico único centralizado, dado que se generan expedientes dependiendo del nivel de atención que sea requerido por el paciente, lo que afecta la continuidad, integridad y disponibilidad de la información.

- *Cultura organizacional:* existe una separación entre los recursos administrativos y médicos que complican la adopción y mejora continua de los sistemas y procedimientos.

- *Incorporación de tecnología:* se han adoptado sistemas de cómputo para agilizar los procesos de atención a los derechohabientes, así como para la recolección, tratamiento y uso de la información, los inconvenientes que en algunos casos se presentan al incorporar nuevas tecnologías es la resistencia al cambio por parte de los recursos humanos, aunados a desarrollos de sistemas de cómputo deficientes, con interfaces poco amigables que complican el proceso de adopción.

- *Estandarización de procedimientos:* es fundamental establecer estándares para la recolección, el tratamiento y la seguridad de los datos clínicos y personales, logrando con ello el cumplimiento con la normatividad aplicable y mejorando así la prestación de servicios.

- *Mecanismos de seguridad:* necesario establecer medidas para el control de acceso a los expedientes clínicos, el cual deberá ser considerando los roles y los permisos asociados a cada rol. En la actualidad una gran problemática es contar con expedientes clínicos en formato físico, que son resguardados en grandes estantes y custodiados en un área "restringida" denominada generalmente archivo clínico.

- *Riesgos:* los expedientes clínicos están conformados tanto por datos clínicos sobre el estado de salud del paciente, como por datos personales que lo identifican, es indispensable tener presente las amenazas, como son los fraudes, el robo de identidad entre otros, que atentan contra la intimidad, la integridad y la privacidad de los derechohabientes. Es importante enfatizar que la incorporación de las tecnologías de la información y

comunicaciones dentro del sector salud, trae consigo nuevas amenazas que utilizan estos medios para obtener acceso a los expedientes clínicos, de ahí la importancia de contar con medidas para identificar, evaluar y dar tratamiento a los riesgos de seguridad de la información.

- *Amenazas:* el estándar *ISO 27799:2008 Health informatics -- Information security management in health using ISO/IEC 27002* presenta en su Anexo A algunas de las amenazas que atentan contra la seguridad de los datos clínicos, algunas de ellas son: la suplantación de algún profesional de la salud o proveedor del servicio para violar la confidencialidad de la información, ataques a los sistemas de información mediante cualquier clase de programa que interrumpan o afecten el servicio, infiltración e intercepción de comunicaciones, fallas provocadas que alteren el correcto funcionamiento de la infraestructura, la red, los sistemas, errores en el mantenimiento, robo por parte de personal interno o externo, entre otras *(ISO, 2008b)*.

El sector salud en México ha identificado en las tecnologías de la información y las comunicaciones un aliado, que le permitirá mejorar la eficiencia y la calidad en la prestación del servicio, generando con ello un mayor bienestar de la población. Ante este escenario surge la iniciativa de implantar el expediente clínico electrónico, como un instrumento que brinde información más completa al personal médico tratante y que permita la comunicación al instante entre las diferentes unidades médicas, el cual deberá utilizar estándares internacionales, interactuar con diversos sistemas como los existentes en laboratorios, banco de sangre, imagenología, hemodiálisis entre otros, así mismo adoptar medidas de seguridad para protección de los datos clínicos y personales que incluyan el control de acceso basado en roles.

De forma tal que el expediente clínico electrónico va más allá de sólo digitalizar la información física o la integración de los datos generados por otros sistemas en un formato digital, la propuesta establecida por la Secretaria de Salud, en el Manual del Expediente Clínico Electrónico del año 2011, pretende implantar un sistema de expediente clínico electrónico, que se integre y comunique con las demás áreas, la figura 1.15 Diagrama de contexto Sistema de Expediente Clínico Electrónico, muestra la interacción deseada.

El expediente clínico electrónico presenta grandes ventajas como son:

- Al mejorar la disponibilidad de la información permite diagnósticos médicos más precisos y oportunos, reduciendo con ello la probabilidad de cometer errores que impacten en la salud del paciente.

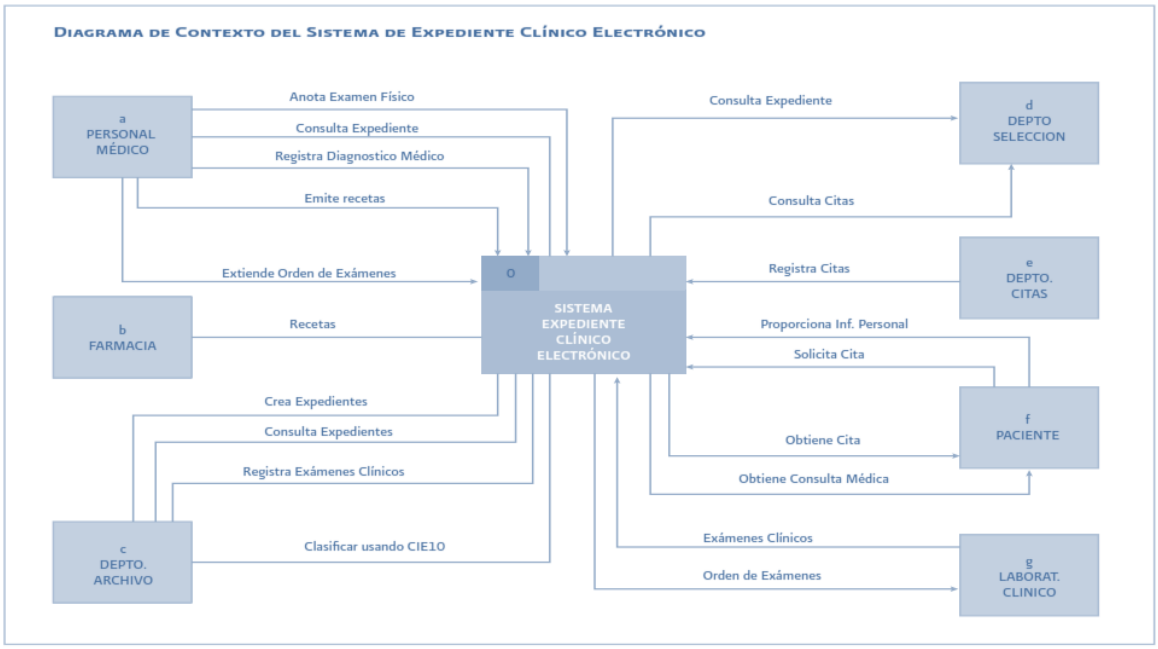
- Monitoreo con mayor precisión sobre datos que puedan ser relevantes para investigaciones en materia de salud.

- Reducción de fraudes médicos dado que se contarán con mecanismos que identifiquen las actividades realizadas por los usuarios del sistema.

- Medidas de seguridad más robustas para los accesos a los datos clínicos.

- Mejora en la calidad de los servicios, reduciendo los tiempos de espera que en algunas ocasiones generan procedimientos burocráticos innecesarios.

Figura 1. 15 Diagrama de contexto Sistema de Expediente Clínico Electrónico.



Fuente: Imagen obtenida de la DGIS, Dirección General de Información en Salud. (2011). Manual del Expediente Clínico Electrónico.

En la actualidad algunas clínicas y hospitales tanto de instituciones de salud públicas como privadas han realizado esfuerzos para incorporar el uso de expedientes clínicos electrónicos, identificando ciertas limitantes y problemas que han afectado el crecimiento del alcance inicial.

Las barreras identificadas son:

- *Aspectos financieros*, considerando la cantidad de datos que requieren ser procesados, transmitidos, almacenados y la infraestructura tecnológica requerida.

- *Aspectos organizaciones*, la falta de capacitación o la resistencia al cambio son factores fundamentales para el éxito o fracaso de cualquier tecnología, reflejado en el gran reto que implica la migración de expedientes clínicos en papel hacia formatos digitales, así como la carencia de métodos efectivos para evaluar la calidad de los programas o sistemas.

- *Nuevos retos en materia de seguridad informática*, considerando que el uso de nuevas tecnologías trae consigo nuevas amenazas, pero a su vez una gama de alternativas para la protección de los datos, como el uso de la criptografía, la firma electrónica, el uso de certificados digitales, así como un campo de acción para especialistas y expertos en temas de seguridad de la información y tecnología.

- *Legislación:* es indispensable establecer reformas en la legislación actual para incluir explícitamente las regulaciones requeridas en materia de datos clínicos y datos genéticos, más allá de lo que en la actualidad se ha definido dentro de la legislación de datos personales. Dado que los datos clínicos requieren un tratamiento y regulación especial que permita tanto a la institución la protección de la propiedad como al paciente ejercer su derecho de acceso a la información y a su vez es indispensable estandarizar los procesos y formatos utilizados para el registro de los datos clínicos, que evitará que cada institución de salud gestione y elabore expedientes clínicos con formatos diversos, creando así un formato único para el registro de datos en materia de salud.

Que las instituciones cuenten con estrategias y mecanismos que protejan la seguridad de la información de los datos clínicos es una prioridad, considerando la gran participación que en los últimos años han tenido las tecnologías de la información y comunicaciones en el sector salud, así como las leyes que establecen la obligación de instituciones públicas y privadas en proteger los datos personales sensibles, definición que incluye a los datos clínicos.

Ante este panorama es necesario que las instituciones de salud fomenten en su personal la cultura en materia de seguridad de la información y establezcan mecanismos para identificar y dar tratamiento a los riesgos, reduciendo los daños en sus activos principales y logrando con ello una forma proactiva de actuación, lo cual disminuirá el impacto de posibles incidentes que afecten la imagen y credibilidad de las instituciones de salud, además la posibilidad de incorporar más recursos especializados en temas de seguridad de la información, tecnología e informática que vean en el sector salud un gran reto y una oportunidad para aplicar sus conocimientos en beneficio de la sociedad.

Una vez que se han definido los conceptos básicos sobre la seguridad de la información y los datos clínicos y se ha presentado cual es la situación actual en México y en el mundo sobre estos temas, se identifican los grandes retos que representa la integración de las tecnologías de información y comunicaciones en el sector salud en México, así como las limitantes que han frenado la implementación a nivel país, de un expediente clínico electrónico, que van desde cuestiones tecnológicas hasta organizacionales y la necesidad en materia jurídica por llevar a cabo reformas que incluyan tanto la definición de los datos clínicos, más allá de lo que actualmente se tiene definido, así como establecer medidas rigurosas para su protección y tratamiento, que garanticen los derechos tanto del paciente, como del personal médico y de las instituciones de salud.

Para establecer mecanismos que permitan la protección de los datos clínicos, las instituciones de salud deben redefinir sus estrategias, basándolas en un enfoque orientado hacia la gestión de riesgos, tema que será abordado con mayor profundidad en el Capítulo 2 Gestión de riesgos, dicho enfoque les permitirá generar proyecciones sobre lo que está ocurriendo y lo que podría ocurrir en el futuro en materia de amenazas, vulnerabilidades, técnicas de ataque, que atenten contra la confidencialidad, integridad y disponibilidad de los datos clínicos. Todo esto dará como resultado que los riesgos de seguridad de la información identificados se puedan, evaluar, conocer su impacto y en base a esta información establecer las prioridades y los controles para reducir la probabilidad de ocurrencia y los daños generados.

CAPÍTULO 2

GESTIÓN DE RIESGOS DE SEGURIDAD

Una vez que en el capítulo 1 fueron abordados los conceptos sobre la seguridad de la información y la importancia de ésta, para protección de la confidencialidad, integridad y disponibilidad de los datos clínicos, en este capítulo se presenta la gestión de riesgo como una estrategia que permita a las instituciones de salud administrar de forma segura los procesos, los sistema de salud y los datos clínicos de los pacientes, considerando que actualmente las tecnologías de la información y comunicaciones han tomado un papel de gran importancia para la prestación de los servicios de salud, aunado a la diversidad de amenazas que aprovechan un sinfín de vulnerabilidades mediante ataques cada vez más sofisticados. En la actualidad existe una gran variedad de modelos sobre la gestión de riesgos de seguridad, dada la gran oferta existente es fundamental que las instituciones de salud consideren la adopción de una metodología para la gestión de riesgos personalizada, basada en los modelos actuales, con el objeto de dar solución a los problemas y necesidades que en materia de seguridad de la información las instituciones de salud enfrentan. Es importante mencionar que contar con una metodología para la gestión de riesgos no garantiza la seguridad de la información en un cien por ciento, dado que no existe dicho nivel de seguridad, la forma en que una metodología contribuirá, será para reducir los riesgos identificados a un nivel aceptable.

2.1 EVOLUCIÓN HISTÓRICA DE LA GESTIÓN DE RIESGOS

La idea de la gestión de riesgos y la necesidad del hombre de no ser sometido a los caprichos del destino, establece la separación entre los tiempos modernos y la antigüedad, esta idea revolucionaria de que el futuro es más que un deseo de los dioses, aunado a la forma activa de ser del hombre ante la naturaleza dio como resultado el descubrimiento que el futuro era más que una vista hacia el pasado o un oráculo oscuro que monopolizaba los acontecimientos. Y es así como surge la idea de ir más allá, en conocer el futuro, de forma que el hombre pudiera cuantificar y racionalizar la toma de decisiones en función del riesgo.

El término riesgo proviene del italiano *risico* o *rischio* cuyo significado, según lo establecido en la Real Academia Española es aquella contingencia o proximidad de un daño.

De forma que el riesgo es una opción, no es el destino como tal, lo cual brinda la libertad para definir y elegir las mejores estrategias que permitan lograr los resultados deseados y el cumplimiento con los objetivos establecidos.

La siguiente tabla presenta la evolución de la gestión de riesgos, considerando etapas donde los riesgos son determinados mediante fundamentos relacionados con la probabilidad, así como el uso de gráficos como la curva de campana y la importancia que adquiere el tema de gestión de riesgos relacionado con aspectos financieros y de seguros, antecedentes que han permitido vincular la gestión de riesgos en ámbitos como la seguridad de la información, lo que en la actualidad representa una estrategia fundamental para las organizaciones.

Figura 2. 1 Tabla evolución de la gestión de riesgos.

Etapa / Año	Descripción
Siglo XV-XVI Renacimiento	Durante este periodo la gente comenzó una era de liberación de la opresión generada durante la Edad Media, etapa donde la religión impuso una gran cantidad de restricciones. En el *Renacimiento* se comienzo a ver otras opciones para operar el mundo, se desarrolló la ciencia, el capitalismo, siendo éstos siglos XV y XVI uno de los momentos en la historia más favorables para la invención.
1654	En este año el famoso matemático, físico, escritor e inventor *Blaise Pascal* en su inquietud por descubrir la forma de predecir el resultado de un juego, antes de que éste terminara, descubrió la Teoría de la Probabilidad, la cual es el núcleo matemático de la gestión de riesgos.
A partir de esta etapa las personas fueron capaces de tomar decisiones y predecir el futuro fundamentándolo sobre una base numérica.	
Siglo XVII	
1711	*Jacob Bernoulli* estableció una ley donde demostró que una muestra aleatoria de artículos podía aproximarse a una población.
1738	En este año surge la curva de campana que funcionó como una herramienta crítica para vincular las técnicas de muestreo estadístico con la probabilidad.
1763	Año que representa el comienzo del desarrollo de la estadística bayesiana.
1800´s	Se desarrolla el negocio de los seguros y con ello las medidas actuariales del riesgo a partir de datos históricos.

Figura 2. 1 Tabla evolución de la gestión de riesgos. (Continuación)

1900	*Bachelier* examina los valores y precios de intercambio en París y defiende su tesis con relación a que los precios siguen un camino aleatorio.
1909-19015	La Oficina de Estadística Estándar, Moody'sy Fitch comienzan la calificación de bonos corporativos mediante la información contable.
1940´s	*John von Neuman, Stanislaw Ulam* y *Nicholas Metropolis* desarrollan el método Monte Carlo, el cuál es un método no determinístico, usado para aproximar expresiones matemáticas complejas y costosas de evaluar con exactitud.
1952	*Harry Markowitz* establece una base estadística para la diversificación y genera portafolios eficientes para los diferentes niveles de riesgo. La teoría moderna de portafolios explica las ventajas que tiene el empresario al diversificar sus inversiones para reducir el riesgo.
1956	Se publica el artículo de *Russell Gallagher* titulado "Gestión de Riesgos: Una nueva etapa del control de costos". Philadelphia se convierte en el punto central del pensamiento orientado a la gestión de riesgos. *Snider* argumenta que el gerente de seguros debe ser un gestor de riesgos. *Herbert Denenberg* retoma los escritos de Henri Fayol para su posible integración con la gestión de riesgo.
1962	*Massey Ferguson* desarrolla la idea del costo del riesgo, comparación entre las pérdidas con fondos propios, las primas de seguros, los costos de control de pérdidas y los costos para la administración de ingresos.
1966	El Instituto de Seguros de América expide el primer reconocimiento "Socio en Gestión de Riesgo".
1974	*Gustav Hamilton* crea el círculo de la gestión de riesgos, el cual describe gráficamente la interacción entre todos los elementos del proceso, desde la evaluación y control hasta los recursos financieros y las comunicaciones.
1975	La Sociedad Americana de Gestión de Seguros cambia su nombre a Sociedad de Gestión de Seguros y Riesgos, lo que marca un cambio sobre la importancia que adquiere con el tiempo el término gestión de riesgos.

Figura 2. 1 Tabla evolución de la gestión de riesgos. (Continuación)

1976	La revista Fortune publica "La revolución de la Gestión de Riesgos", artículo que sugiere la coordinación de las funciones de la gestión de riesgos dentro de la organización y la responsabilidad de las políticas de la organización y su supervisión.
1983	El discurso de *William Ruckelshaus* "Ciencia, Riesgo y Políticas Públicas" lleva la gestión del riesgo a la agenda de la política nacional.
1995	*AS/NZS 4360:1995* es publicada por primera vez la primera norma de gestión de riesgos. Revive el interés en la gestión de riesgos operacionales.
1996	Se pone en marcha la *Asociación Global de Profesionales de Riesgo*, la cual opera a través de Internet y se ha convertido en la asociación más grande en el mundo, enfocada en el riesgo financiero.

Fuente: Elaboración propia con información *de Bernstein, Peter L. (1996). Against the gods: The remarkable story of risk: Wiley New York.*

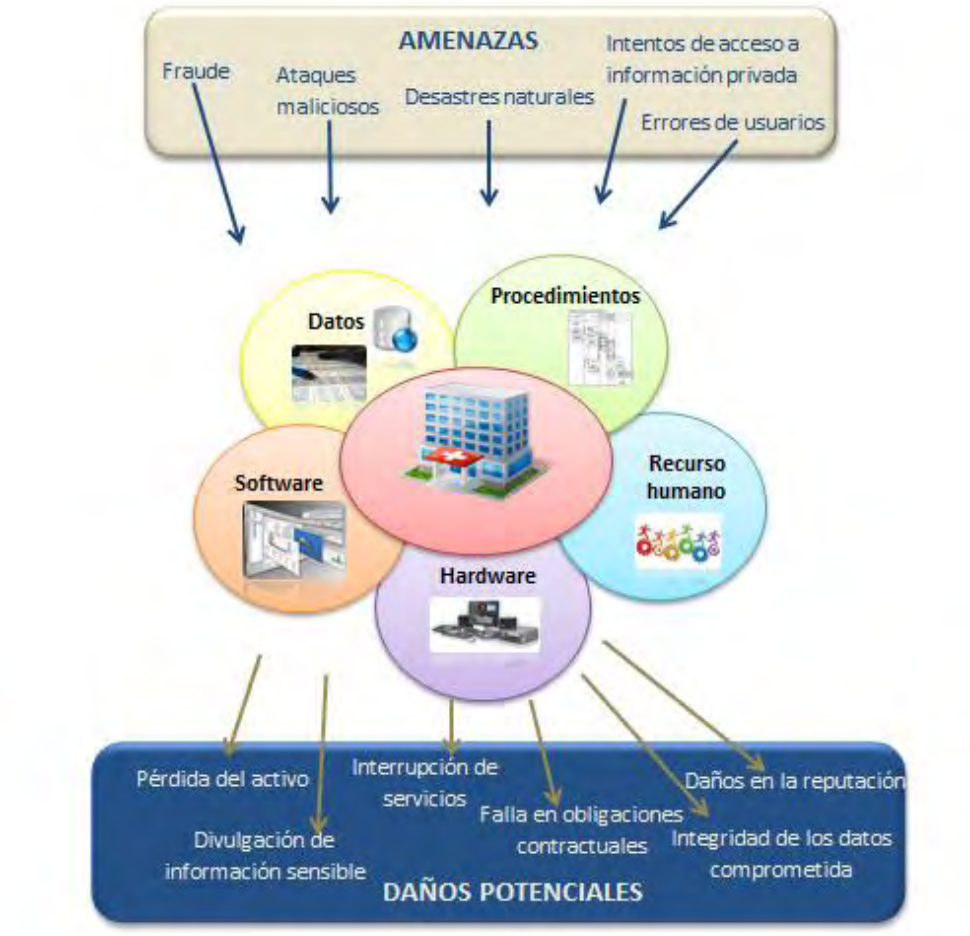
2.2 CONCEPTOS FUNDAMENTALES SOBRE LA GESTIÓN DE RIESGOS DE SEGURIDAD

La incorporación de las tecnologías de la información (TI) en el sector público han transformado la forma de prestar los servicios a los ciudadanos, hecho que se ve reflejado en los resultados obtenidos por México según el Informe Global de Tecnologías de Información del año 2013 del Foro Económico Mundial, donde México alcanza el lugar 63 en el ranking de 144 países, logrando un avance de 13 posiciones con respecto al lugar 76 que ocupaba en el año 2012, hecho que fundamentalmente se debe a los esfuerzos realizados por el gobierno para desarrollar su oferta de servicios en línea, así como mejoras generales en el entorno empresarial y de innovación. De igual forma el sector privado se ha beneficiado del uso de las TI al adoptar sistemas de información en sus procesos y operaciones, resultados que se encuentran reflejados en términos económicos, de productividad, cumplimiento y competitividad.

Los sistemas de información están integrados por entidades diversas desde supercomputadoras, estaciones de trabajo, computadoras personales, teléfonos celulares hasta sistemas altamente especializados, los cuáles se encuentran en exposición constante a una gran cantidad de amenazas que al ser materializadas, mediante la explotación de vulnerabilidades conocidas o desconocidas pudieran afectar la continuidad de las operaciones de la organización y comprometer la confidencialidad, integridad y disponibilidad de la información (Véase figura 2.2 Panorama actual en materia de amenazas en las TI).

Ante estas condiciones es fundamental que los líderes de las entidades públicas y privadas comprendan la importancia de la gestión de riesgos de seguridad de la información, su responsabilidad dentro de éste proceso y la forma en que deben alinearlo con la misión, las funciones de la entidad, los recursos humanos y los procesos que influyen en el diseño, desarrollo e implementación de los sistemas de información.

Figura 2. 2 Panorama actual en materia de amenazas en las TI.



Fuente: Elaboración propia

Una gestión de riesgos de seguridad de la información efectiva requiere en gran parte de la comunicación y la cultura en materia de seguridad informática, para gestionar los riesgos en una organización es necesario realizar actividades que involucren a todo el personal de la misma, desde los directivos que proveen la visión estratégica de las metas y objetivos de la organización, los mandos medios que coordinan las actividades de planeación, ejecución y administración de los proyectos hasta el personal operativo que hace uso de los sistemas de información para el desarrollo de sus actividades en cumplimiento con las funciones y misión de la organización.

Figura 2. 3 Recursos humanos y la gestión de riesgos.

Fuente: Elaboración propia.

Una vez analizado el contexto actual y el papel de la gestión de riesgos, como una estrategia de mejora, que dinamiza y protege la red de procesos y recursos de una organización, mediante la implementación de acciones para garantizar la continuidad de las operaciones y la seguridad de la información, se presentan a continuación los siguientes conceptos fundamentales relacionados con la gestión de riesgos de seguridad de la información.

2.2.1 RIESGO

El estándar ISO 31000 *Risk management – Principles and guidelines*, define el riesgo como el efecto de la incertidumbre en la consecución de los objetivos, donde un efecto es considerado como una desviación de lo esperado que puede ser positiva o negativa, la incertidumbre es el estado generado cuando no se cuenta con la información y el conocimiento necesario sobre un cierto evento, su probabilidad de ocurrencia o el impacto que éste conlleva. Frecuentemente el riesgo es expresado en términos de la combinación de la probabilidad de ocurrencia y las consecuencias del evento.

a) *Probabilidad de ocurrencia:* definida por el ISO 31000 como la posibilidad de que algo suceda, ésta puede ser medida o determinada de forma tanto objetiva en el caso de un método de análisis de riesgos cuantitativo, como subjetiva para un método de análisis de riesgos cualitativo. El *National Institute of Standards* and Technology (NIST) en su *Special Publication 800-30 Guide for Conducting Risk Assessments* define la probabilidad de ocurrencia como un factor ponderado basado en la posibilidad de que una amenaza determinada tenga la capacidad de explotar una vulnerabilidad o conjunto de vulnerabilidades.

b) *Consecuencia:* ISO 31000 la define como el resultado de un evento que afecta los objetivos establecidos, las consecuencias pueden ser inciertas, de igual forma sus efectos pueden ser tanto positivos como negativos. El NIST en su SP 800-30 define el término impacto para referirse a la magnitud del daño esperado como consecuencia de una divulgación no autorizada, modificación, destrucción o pérdida de información o de los sistemas de información. En términos generales considera la magnitud de los daños generados cuando se materializa una amenaza.

2.2.2 RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Son aquellos riesgos que surgen de la pérdida de la confidencialidad, integridad y disponibilidad de la información o de los sistemas de información y que representa un impacto potencial adverso para la operación de la organización y sus recursos. *(NIST, 2012)*

2.2.3 VALORACIÓN DE RIESGOS

Definido según ISO 31000 como el proceso general de identificación, análisis y evaluación del riesgo. El objetivo de la valoración de riesgo es proveer información basada en evidencia que sea analizada para la toma de decisiones, sobre como un riesgo en particular atenta contra la organización y con base en ello determinar las medidas preventivas correspondientes *(IEC/ISO, 2009)*.

A continuación se presentan algunos de los beneficios de realizar una valoración de riesgos:

- Entender los riesgos y los impactos potenciales asociados a éstos, conocer esta información permitirá seleccionar los medios para el tratamiento de los riesgos identificados.
- Proporcionar mayor información para la toma de decisiones.
- Identificar las vulnerabilidades en la organización.
- Evaluar y establecer prioridades.
- Conocer sobre los requerimientos regulatorios.
- Determinar estrategias y controles para el tratamiento de los riesgos y evaluar su efectividad.

Los riesgos pueden ser evaluados considerando dos enfoques (véase figura 2.4 Enfoques para la valoración del riesgo):

Figura 2. 4 Enfoques para la evaluación del riesgo.

Enfoque	Descripción
Cuantitativo	Este enfoque utiliza una serie de métodos, principios o reglas de evaluación del riesgo, basadas en el uso de números, es más efectiva para respaldar un análisis de costo-beneficio de las alternativas seleccionadas para dar respuesta a los riesgos, sin embargo los resultados de una evaluación de riesgos cuantitativa pueden ser poco claros y requerir de una explicación o interpretación. Los costos de una evaluación cuantitativa, en términos de tiempo esperado, el esfuerzo, los recursos involucrados y la inversión en el uso o desarrollo de herramientas para la evaluación, son en la mayoría de los casos compensados por los beneficios obtenidos en términos de rigor, repetibilidad y reproducibilidad de la evaluación. Para asignar valores de la información, los sistemas, los procesos de negocio, el costo de recuperación, el impacto y los riesgos, pueden ser considerados los costos directos e indirectos. Además de la siguiente ecuación. $R_{Riesgo} = P_{Probabilidad} \ X \ C_{Costo}$
Cualitativo	La evaluación cualitativa emplea métodos, principios o reglas para evaluar el riesgo basados en categorías o niveles (alto, moderado, bajo). El rango de valores para la evaluación es pequeño en algunos casos, complicando relativamente la comparación y priorización de los riesgos. Al ser un análisis subjetivo los resultados podrían estar influenciados por la experiencia individual lo que ocasionaría resultados de evaluación diferentes. Es importante que la organización defina claramente sus criterios para evaluar el impacto y la probabilidad, siendo una opción los términos de alto, medio o bajo, el significado de estas opciones y los parámetros que deben ser considerados para las mismas, deberán ser previamente indicados. Se debe integrar un listado con los riesgos que serán evaluados por los involucrados, considerando los criterios previamente definidos. Con la información resultante se integrará una matriz cuyo eje horizontal es la probabilidad de ocurrencia y el impacto el eje vertical.

Fuente: Elaboración propia con información de *Special Publication 800-30 Guide for Conducting Risk Assessment y SANS, SysAdmin Audit Networking and Security Institute (2012). An Introduction to Information System Risk Management* .

Es importante destacar que la selección del enfoque de evaluación utilizado, dependerá de la cultura organizacional, los objetivos en materia de seguridad de la información, los recursos destinados para el análisis y el entorno.

2.2.4 TRATAMIENTO DEL RIESGO

El estándar ISO 27005 *Information technology- Security techniques- Information security risk management* establece cuatro opciones para el tratamiento de los riesgos, la figura 2.5 Tabla opciones para el tratamiento de riesgos presenta a detalle esta información.

Las cuatro opciones para el tratamiento del riesgo no son mutuamente exclusivas, lo cual indica que pueden ser combinadas considerando las necesidades de cada organización, con el objeto de reducir la probabilidad del riesgo, sus posibles consecuencias, así como transferirlo o conservar cualquier riesgo residual, definido en el estándar ISO 31000, como el riesgo resultante después de aplicar medidas para el tratamiento del riesgo.

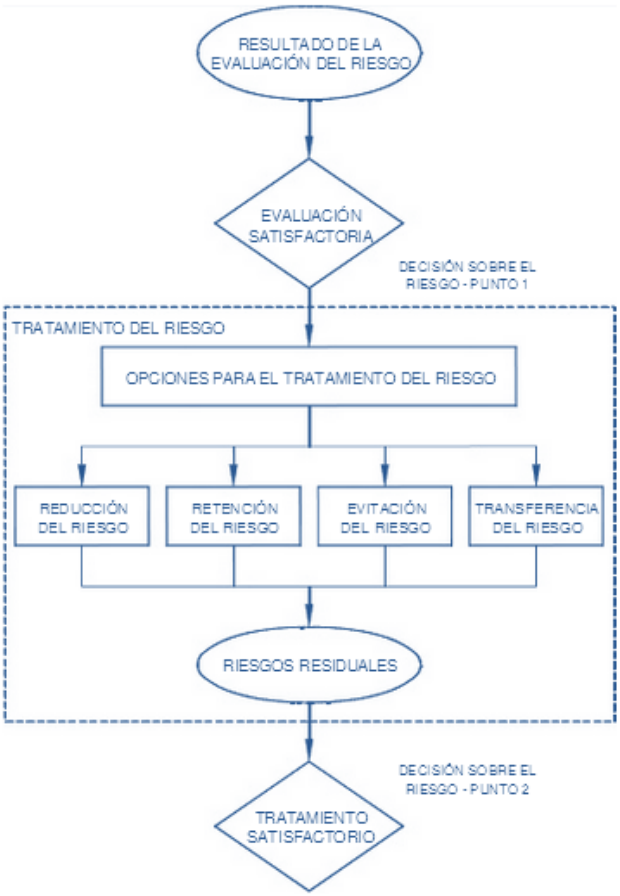
Figura 2. 5 Tabla opciones para el tratamiento de riesgos.

Opción	Descripción
Reducción/ Mitigar	Esta opción de tratamiento considera la selección de controles para reducir el nivel de riesgo, lo cual permitirá que el riesgo residual sea llevado a un nivel aceptable por la organización. La selección de controles debe considerar el criterio de aceptación de riesgos, el costo, el tiempo de implementación, así como las leyes y los requerimientos contractuales.
Retención/Aceptar	Esta opción consiste en la decisión de mantener el riesgo en el nivel que se encuentra, considerando que el riesgo está dentro de los niveles de aceptación definidos por la organización y que a su vez satisface sus políticas.
Evitación/ Eliminar	Esta opción consiste en evitar la actividad o la acción que da origen a un riesgo en particular. Cuando un riesgo es considerado como alto y el costo de implementar otras opciones de tratamiento excede los beneficios, se debe tomar una decisión para evitar por completo el riesgo, ya sea retirando una actividad o cambiando las condiciones bajo las cuales se efectúa.
Transferencia	Esta opción considera transferir el riesgo a otra entidad que sea más eficiente en manejarlo. Es importante destacar que la transferencia de riesgos puede crear nuevos riesgos o modificar los previamente identificados, por lo que es necesario un tratamiento de riesgo adicional.

Fuente: Elaboración propia con información *ISO/IEC. (2005). ISO 27002:2005-Information technology — Security techniques — Code of practice for information security management.*

La figura 2.6 Actividades para el tratamiento del riesgo muestra el procedimiento a seguir una vez que se han identificado los riesgos y se han determinado las opciones que serán implementadas para su tratamiento, ya acordadas las acciones es necesario verificar que los riesgos residuales se encuentren dentro de los niveles aceptables, previamente definidos por la organización. Una vez que se han implementado las medidas de tratamiento es necesario evaluar si han contribuido a reducir el riesgo, en caso de no haberse logrado se deberá evaluar nuevamente la opción de tratamiento seleccionada y la posibilidad de elegir otras alternativas.

Figura 2. 6 Actividades para el tratamiento del riesgo.



Fuente: Imagen obtenida de *ISO/IEC. (2005). ISO 27002:2005-Information technology — Security techniques — Code of practice for information security management.*

2.3 PROCESO GENERAL DE GESTIÓN DE RIESGOS

El proceso general para la gestión de riesgos de seguridad en una organización definido por el NIST en su *Special Publication 800-39 Managing Information Security Risk – Organization, Mission, and Information System View* está integrado por las siguientes etapas (Véase figura 2.7 Proceso General para la Gestión de Riesgos):

Figura 2. 7 Proceso General para la Gestión de Riesgos.

Fuente: Elaboración propia con información de *Special Publication 800-39 Managing Information Security Risk – Organization, Mission, and Information System.*

1. *Estructurar:* en esta etapa se definirán los criterios para evaluar y aceptar el riesgo, así como la especificación de las directrices para la toma de decisiones relacionadas con los riesgos identificados.

   Los directivos de la organización deberán definir la estrategia para la gestión de riesgos de seguridad, hacerla de conocimiento a todo el personal, con el objetivo de crear una cultura en materia de gestión de riesgos y seguridad de la información, de tal forma que los

directivos asuman los riesgos a los que se enfrenta la organización, conozcan las vulnerabilidades y posibles amenazas, así como su impacto y la probabilidad de ocurrencia, toda esta información les permitirá establecer de forma adecuada la estrategia para la evaluación, respuesta y monitoreo de los riesgos.

Para definir la estrategia es necesario previamente especificar el criterio de evaluación de los riesgos, sus niveles, la tolerancia, las prioridades y los grados de aceptación, estos criterios deben estar alineados a la misión de la organización, sus objetivos, su entorno, sus clientes y su cumplimiento con acuerdos contractuales y regulaciones.

2. *Evaluar:* dentro de esta fase se identificaran los riesgos mediante el uso de un modelo para la evaluación y serán considerandos los criterios para valorar el riesgo previamente definidos por la organización.

   El propósito de la evaluación de riesgo es definir los activos críticos para la operación, se identifican las posibles amenazas que atenten contra la seguridad de la información y la continuidad de la operación, así como las vulnerabilidades internas y externas a la organización. Además se evalúa el posible daño y el impacto adverso generado cuando una amenaza explota una vulnerabilidad y la probabilidad de que esto suceda.

   Para llevar a cabo las actividades de evaluación del riesgo es necesario que la organización identifique las herramientas, las técnicas y las metodologías que utilizarán durante el proceso, debe contar con la información sobre las amenazas y las vulnerabilidades que puedan afectar los activos, además especificar las limitantes con posibilidad de influir en la evaluación del riesgo. Es de gran importancia que los roles y responsabilidades estén claramente definidas, así como la forma en que la información es recolectada, creada, almacenada y transferida en la organización. El personal estratégico y táctico debe considerar la forma en que el riesgo se presenta en la organización y especificar la frecuencia con la cual se realizará la evaluación del mismo.

   Al final de esta etapa se determina el valor del riesgo, en función de impacto y la probabilidad de ocurrencia.

3. *Responder:* una vez evaluados los riesgos, en esta etapa se determinan las opciones para su tratamiento y los controles que serán implementados.

   El plan de tratamiento del riesgo debe estar alineado con las directrices definidas en la estrategia para la gestión de riesgos de seguridad. En esta fase se definen las acciones para dar tratamiento a los riesgos resultantes (reducción, retención, evitación y transferencia). Se deben evaluar las alternativas, considerando el criterio de evaluación, la tolerancia al riesgo y los lineamientos previamente definidos por la organización en la etapa 1 Evaluar, antes de llevar a cabo la implementación de controles se deberá realizar un análisis.

Para la elaboración y evaluación de un plan para el tratamiento de los riesgos de seguridad, la organización podrá apoyarse en herramientas, técnicas o metodologías, que contribuyan con información sobre los resultados obtenidos una vez implementados los controles. La organización podrá compartir esta información con el personal de la organización como parte de las actividades de comunicación y retroalimentación.

4. *Monitorizar:* esta fase forma parte de las acciones de mejora continua, indispensable para llegar a una madurez en el proceso de gestión de riesgos, esta etapa es la responsable de dar seguimiento a los controles implementados, así como de las actividades de comunicación, necesarias para que la organización participe y retroalimente el proceso de gestión de riesgos.

   Las actividades que se llevan a cabo en esta etapa consisten en verificar que las medidas implementadas como parte de las actividades del plan de tratamiento de riesgo, cumplan con los requerimientos de seguridad y a la vez se encuentren alineadas a la misión, la función, las políticas y las responsabilidades en materia de cumplimiento de la organización.

2.4 MODELOS PARA LA GESTIÓN / VALORACIÓN DE RIESGOS

Para llevar a cabo la gestión de riesgos de seguridad de la información, las organizaciones adoptan y toman como referencia diversos modelos para gestionar o valuar adecuadamente sus riesgos.

Cabe señalar que si bien existe una gran variedad de modelos, es importante que la organización cuente con una metodología personalizada que se encuentre alineada a su misión, su cultura organizacional y sus necesidades en materia de seguridad de la información.

Los factores clave que deben ser considerados por la metodología para la gestión de riesgos de seguridad creada o adaptada por la organización son:

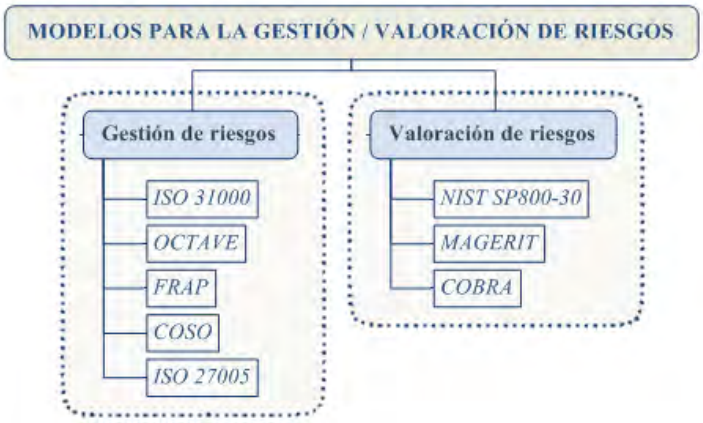
a) *Flexibilidad:* es un factor fundamental, la metodología debe ser capaz de modificarse para ser adoptada por la organización, además con el paso del tiempo y en respuesta a futuros cambios, debe permitir la incorporación de mejoras en su estructura e implementación.

b) *Repetibilidad:* la metodología debe llevarse a cabo regularmente, para generar una cultura en materia de gestión de riesgos de seguridad, de tal forma que se cuente con datos que permitan la comparación de los diferentes resultados obtenidos en el tiempo.

c) *Regulaciones:* la organización debe crear, personalizar o adaptar la metodología considerando su alineación con la misión, la visión, las políticas y los procesos.

La figura 2.8 Modelos para la gestión/valoración de riesgos presenta los modelos principales considerados por las organizaciones para llevar a cabo la gestión y evaluación de sus riesgos, la descripción de cada uno se presenta a continuación.

Figura 2. 8 Modelos para la gestión/valoración de riesgos



Fuente: Elaboración propia.

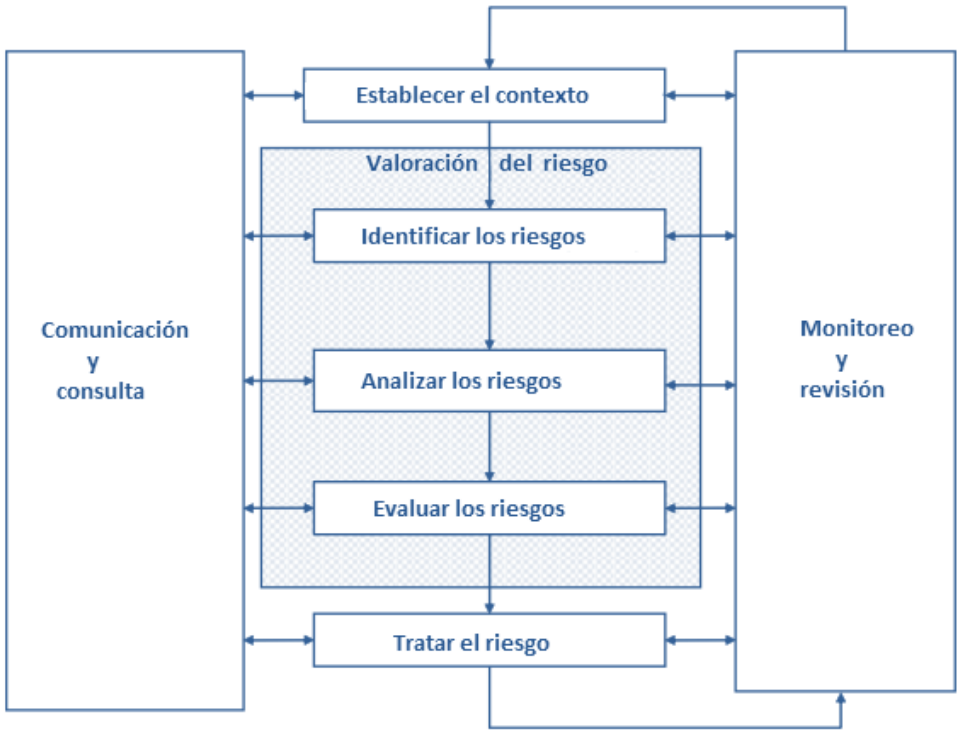
2.4.1 ISO 31000

El estándar *ISO 31000 Risk Management Principles and Guidelines* es una norma internacional que proporciona los principios y directrices genéricas sobre la gestión de riesgo, puede ser adoptada por cualquier organización pública o privada, por lo tanto, no es específica de una industria o sector en particular.

El documento proporciona los términos básicos en materia de gestión de riesgos y sus definiciones, así como el marco que la organización debe considerar para la adopción de esta norma y el proceso a seguir para su implementación.

El proceso para la gestión de riesgos definido por el ISO 31000 presenta la siguiente estructura (Véase figura 2.9 Proceso para gestión de riesgos ISO 31000):

Figura 2. 9 Proceso para la gestión de riesgos ISO 31000.



Fuente: Imagen obtenida de *ISO. (2009). ISO 31000 Risk management — Principles and guidelines.*

1. *Establecer el contexto:* en esta etapa la organización identifica, los procesos, los activos críticos, define el alcance incluido en el proceso de gestión y el criterio de evaluación que será considerado.

2. *Identificación de los riesgos:* mediante sesiones con los interesados se identifican las amenazas y vulnerabilidades que pueden afectar los activos previamente identificados.

3. *Análisis de los riesgos:* los responsables definen el enfoque para evaluar el riesgo (cuantitativo, cualitativo), determinan la probabilidad de ocurrencia y el impacto para cada riesgo crítico definido.

4. *Evaluación del riesgo*: facilita la toma de decisiones, basada en los resultados del análisis de riesgos.

5. *Tratamiento del riesgo:* define el conjunto de medidas que serán implementadas para tratar los riesgos identificados.

La etapa comunicación y consulta al igual que monitoreo y revisión se presentan durante todo el proceso de gestión.

2.4.2 NIST

El *National Institute of Standards and Technology* (NIST) en su *Special Publication 800-30 Guide for Conducting Risk Assessments* es un estándar del gobierno federal de los Estados Unidos de América, diseñado principalmente con un enfoque cualitativo, para ser utilizado por analistas de seguridad, expertos técnicos y propietarios de sistemas con el objetivo de evaluar y gestionar los riesgos en sistemas de información.

La metodología ofrecida por el NIST en su nueva versión, se integra de cuatro etapas (Véase figura 2.10 Proceso para la valoración de riesgos NIST SP800-30):

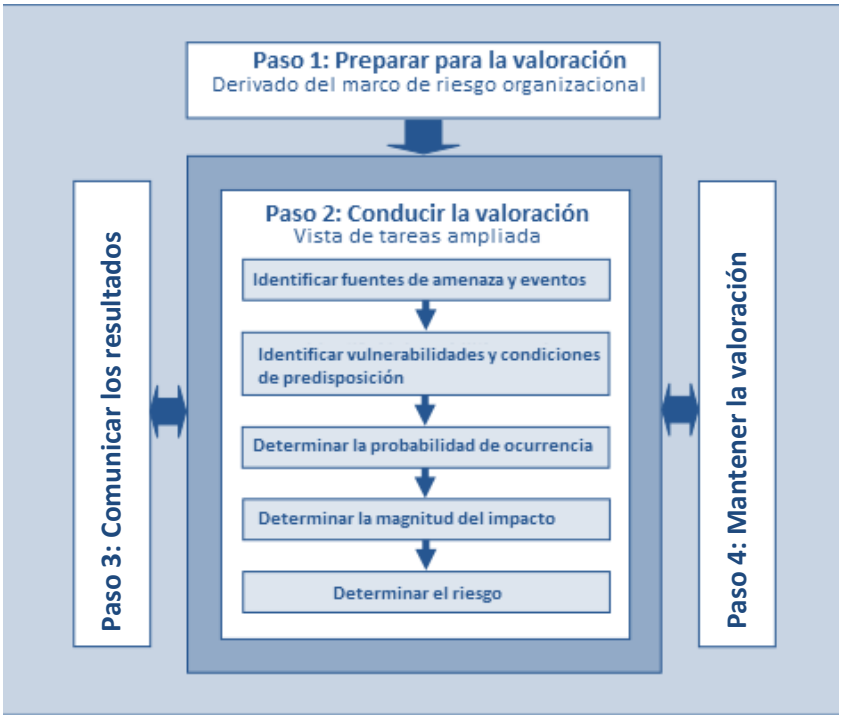
1. *Preparar la valoración:* en esta etapa se define el marco de riesgos de la organización, se identifica el objetivo, el alcance de la valoración, las fuentes de información, los modelos y criterios que serán utilizados para la valoración de los riesgos.

2. *Conducir la valoración:* en esta fase se identifican las fuentes de amenaza, las vulnerabilidades y la probabilidad de que sean atacadas por una amenaza determinada. La probabilidad y el impacto serán considerados para establecer el valor del riesgo.

3. *Comunicar los resultados:* el objetivo de esta etapa es asegurar que los tomadores de decisión cuenten con la información necesaria para comunicar y guiar las decisiones en materia de gestión de riesgos. Se deberán dar a conocer los resultados y las actividades requeridas para el tratamiento de los riesgos identificados.

4. *Mantener la valoración:* el propósito de esta fase es mantener actualizado el conocimiento sobre los riesgos de la organización, monitorizar e identificar mejoras en los controles implementados.

Figura 2. 10 Proceso para la valoración de riesgos NIST SP800-30



Fuente: Imagen obtenida de *NIST, National Institute of Standards and Technology. (2012). Risk Management Guide for Information Technology Systems Special Publication 800-30.* Consultado en http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

2.4.3 OCTAVE

El *Software Engineering Institute* (SEI) de la *Carnegie Mellon University* desarrolló una aproximación que incluye la valoración estratégica de los riesgos y el conjunto de técnicas de planeación para la seguridad de la información, denominado *Operationally Critical, Threat, Asset and Vulnerability Evaluation* (OCTAVE). El objetivo principal de OCTAVE es ayudar a las organizaciones a mejorar la forma en la cual evalúan y se protegen de los riesgos de seguridad de la información. Los involucrados en el proceso de gestión de riesgos necesitan entender el riesgo y sus componentes, información que será considerada para la toma de decisiones.

OCTAVE está integrado por tres fases (Véase figura 2.11 Fases OCTAVE):

1. *FASE 1* Generación perfiles de amenaza de los activos:

   Esta fase incluye una evaluación de la organización, donde el equipo de análisis determina, que activos son importantes para llevar a cabo las actividades principales de la entidad, así como las medidas que actualmente se tienen implementadas para protegerlos. Como resultado de esta etapa se obtiene un perfil de valoración,

determinado a partir de la identificación de los activos críticos, sus requerimientos de seguridad y las amenazas asociadas a cada uno.

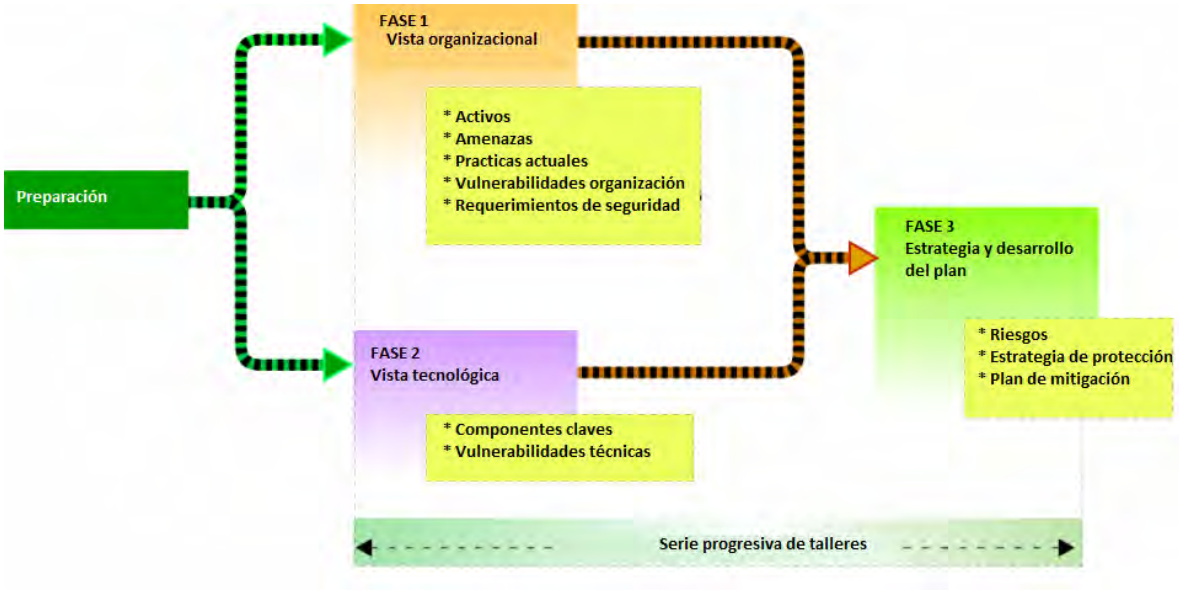
2. *FASE 2* Identificación de las vulnerabilidades de la infraestructura:

   En esta etapa se realiza una evaluación de la infraestructura de información, el equipo de análisis examina los accesos a las redes, identifica las clases de tecnologías de información que se relacionan con los activos críticos resultantes de la fase uno.

3. *FASE 3* Desarrollo de estrategias y planes:

   En este paso el equipo de análisis identifica los riesgos de los activos críticos de la organización y toma las decisiones necesarias para su tratamiento. Como resultado se obtiene una estrategia de protección.

Figura 2. 11 Fases OCTAVE.



Fuente: Imagen obtenida de:
SANS, SysAdmin Audit Networking and Security Institute (2012). An Introduction to Information System Risk Management. Consultado en http://www.sans.org/reading_room/whitepapers/auditing/introduction-information-system-risk-management_1204 y Christopher Alberts, Audrey Dorofee, James Stevens, & Woody, Carol. (2003). *Introduction to OCTAVE Approach C. M. S. E. Institute (Ed.)* Consultado en http://www.itgovernanceusa.com/files/Octave.pdf

2.4.4 FRAP

Creado por Thomas Peltier el modelo para la gestión de riesgos *Facilitated Risk Assessment Process* (FRAP) consiste en la aplicación de técnicas para gestionar los riesgos de una forma altamente rentable, utiliza un enfoque cualitativo y para su implementación considera el análisis

de vulnerabilidades, el análisis de impacto, el análisis de las amenazas y los cuestionarios *(Thomas, 2000).*

La implementación de FRAP considera las siguientes actividades:

1. Sesiones para identificar los activos y las amenazas asociados a éstos.
2. Asignación del valor del impacto y la probabilidad de ocurrencia para cada amenaza.
3. Definición del conjunto de controles y medidas de seguridad que serán implementadas.
4. Se elabora un resumen con los resultados obtenidos del proceso de gestión.

2.4.5 COSO

Ante la necesidad detectada para mejorar la forma en que las organizaciones gestionan los riesgos en las organizaciones, el *Committee of Sponsoring Organizations* de la *Treadway Commision* (COSO), define el modelo COSO- *Enterprise Risk Management* (ERM) con un marco integrado para la gestión del riesgo corporativo, éste último definido como un proceso efectuado por el consejo de administración de una entidad, su dirección y el personal que la conforman, para definir y aplicar estrategias que permitan identificar eventos potenciales que puedan dañar a la organización, de tal forma que se logra la gestión de los riesgos para llevarlos a un nivel aceptable.

El marco de gestión de riesgos corporativos está definido para que la organización alcance sus objetivos, que se clasifican en cuatro categorías:

a) *Estrategia:* objetivos alto nivel, alineados con la misión de la entidad.
b) *Operaciones:* objetivos relacionados con el uso eficaz y eficiente de los recursos.
c) *Información:* objetivos de fiabilidad de la información suministrada.
d) *Cumplimiento:* objetivos relacionados con el cumplimiento de leyes y normas aplicables.

Además el modelo considera ocho elementos que se derivan de la forma en que la dirección conduce a la organización y cómo están integrados dichos elementos en el proceso de gestión.

1. *Ambiente interno.*
2. *Establecimiento de objetivos.*
3. *Identificación de eventos.*
4. *Evaluación de riesgo.*
5. *Respuesta al riesgo.*
6. *Actividades de control.*
7. *Información y comunicación.*
8. *Supervisión.*

El modelo COSO relaciona directamente los objetivos que la organización desea lograr con los componentes de la gestión de riesgos corporativos, que representan aquello que hace falta para

lograr los objetivos, la relación se representa mediante un cubo tridimensional (Véase figura 2.12 Modelo COSO- ERM).

Este cubo muestra la capacidad de centrarse sobre la totalidad de la gestión de riesgos corporativos de una entidad o bien por categoría de objetivos, componente, unidad o cualquier subconjunto deseado.

Figura 2. 12 Modelo COSO- ERM.

Fuente: Imagen obtenida de: COSO. (2004). *Enterprise Risk Management — Integrated Framework*. Consultado en http://www.coso.org/erm-integratedframework.htm y COSO. (2009). *Guidance on Monitoring Internal Control Systems*.

2.4.6 MAGERIT

La Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (MAGERIT) fue creada por el Consejo Superior de Administración Electrónica (CSAE) con el objetivo de concienciar a los responsables de los sistemas de información de la existencia de riesgos y la necesidad de implementar medidas de protección, ofreciendo para ello un método sistemático para analizar los riesgos, lo que ayudará a descubrir y planificar medidas oportunas que permitan mantener los riesgos bajo control *(CSAE, 2012)*.

MAGERIT implementa el proceso de gestión de riesgos dentro de un marco de trabajo para que los órganos de gobierno tomen decisiones considerando los riesgos derivados del uso de tecnologías de la información. El análisis de riesgos consiste en una aproximación metódica para determinar el riesgo que considera los siguientes pasos:

a) Identificar los activos relevantes para la organización, su interrelación y su valor en caso de que sufrieran algún daño.

b) Determinar a qué amenazas están expuestos los activos previamente identificados.

c) Definir qué medidas para salvaguardas de los activos están implementadas y que tan eficaces son frente al riesgo.

d) Estimación del impacto, definido como el daño sobre el activo como consecuencia de la materialización de la amenaza.

e) Cálculo del riesgo, definido como el impacto ponderado con la tasa de ocurrencia (o expectativa de materialización) de la amenaza.

2.4.7 ISO 27005

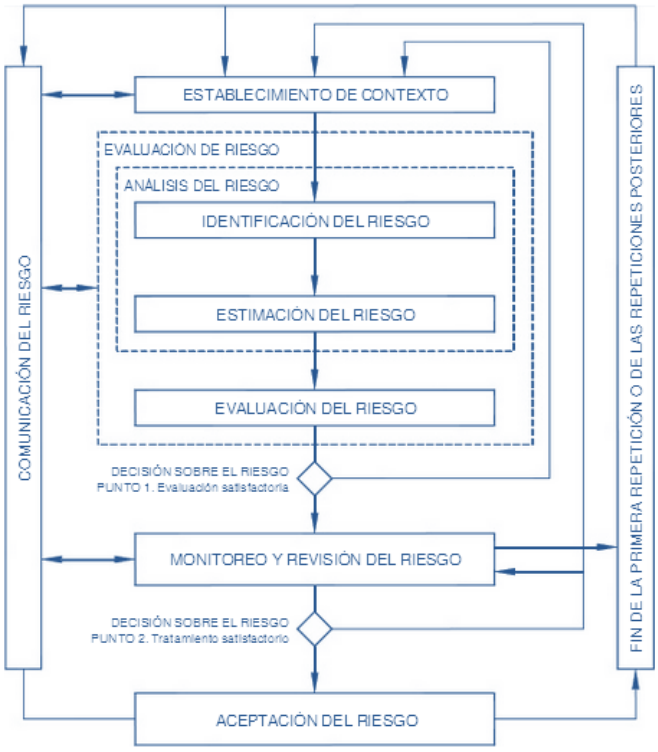
El estándar ISO 27005 *Information technology — Security techniques — Information security risk management.* proporciona directrices para la gestión del riesgo en la seguridad de la información en una organización, esta norma brinda un soporte particular a los requisitos de un sistema de gestión de seguridad de la información (SGSI).

ISO 27005 contiene una descripción de los procesos para llevar a cabo las actividades de gestión del riesgo en la seguridad de la información y sus actividades, tales como el establecimiento del contexto, la evaluación del riesgo, el tratamiento, la aceptación, la comunicación, el monitoreo y la revisión.

La visión general del proceso de gestión del riesgo en la seguridad de la información presentado por el ISO 27005 consta de las siguientes etapas (Véase figura 2.13 Proceso de gestión del riesgo en la seguridad de la información):

1. Establecimiento del contexto.
2. Evaluación del riesgo.
3. Tratamiento del riesgo.
4. Aceptación del riesgo.
5. Comunicación del riesgo.
6. Monitoreo y revisión del riesgo.

Figura 2. 13 Proceso de gestión del riesgo en la seguridad de la información.



Fuente: Imagen obtenida de *ISO/IEC. (2005). ISO 27002:2005-Information technology — Security techniques — Code of practice for information security management.*

2.4.8 COBRA

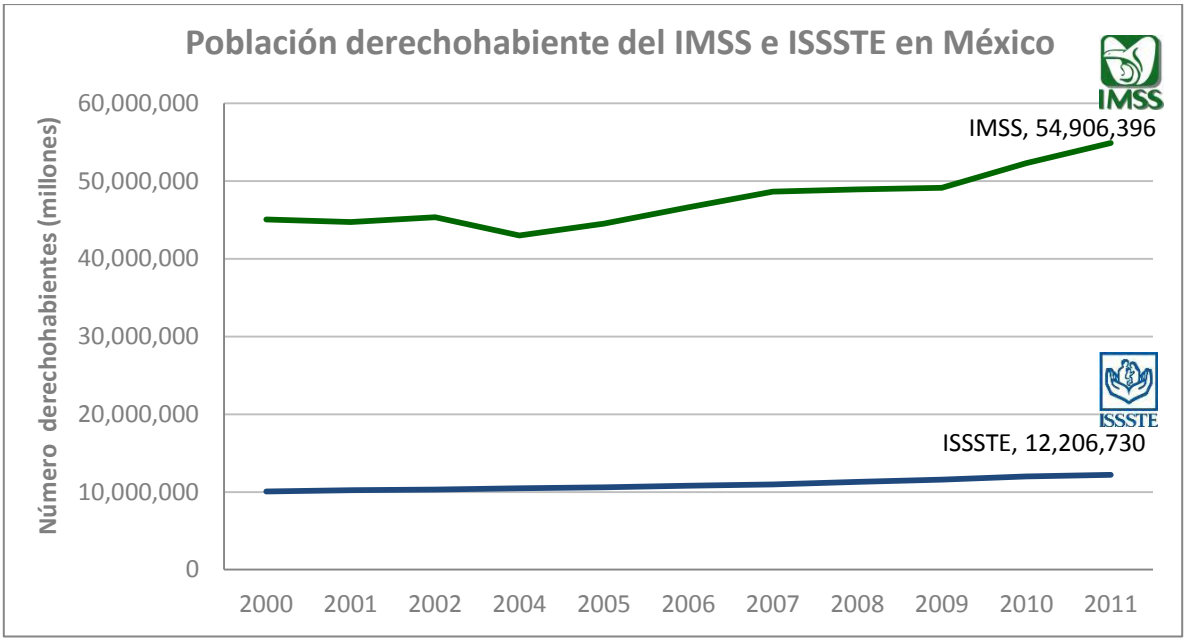
El *Consultative, Objective and Bi-functional Risk Analysis* (COBRA) es un proceso creado en 1991 por *C&A Systems Security Ltd.* su enfoque orienta la valoración de los riesgos desde el punto de vista de negocios, más que hacia un enfoque técnico. COBRA consiste en un conjunto de herramientas que pueden ser compradas y utilizadas para que la organización lleve a cabo auto-evaluaciones de riesgo *(SANS, 2012)*.

COBRA tiene dos productos primarios, consultor de riesgos y cumplimiento de ISO. Consultor de riesgos es una herramienta que permite construir plantillas de cuestionarios para recopilar información sobre los tipos de activos, vulnerabilidades, amenazas y controles, información con la cual el consultor de riesgos puede crear informes y emitir recomendaciones. El cumplimiento de ISO es similar al consultor de riesgos, enfocado al cumplimiento con ISO 27002 *Information technology – Security techniques – Code of practice for information security management.*

2.5 LA GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN EN EL SECTOR SALUD DE MÉXICO

En la actualidad el sector salud de México ha sufrido diversas transformaciones como resultado de varios factores, tal es el caso de la incorporación de las tecnologías de la información y comunicaciones, adoptadas como una solución para satisfacer la demanda de servicios, requeridos por una cantidad cada vez mayor de pacientes, quienes exigen una mejora en la calidad de la atención y la reducción de los tiempos de espera para ser atendidos. En la figura 2.14 Población derechohabiente del IMSS e ISSSTE en México, se observa como ha incrementado del año 2000 al 2011 la población derechohabiente de las principales instituciones de salud en México, el Instituto Mexicano del Seguro Social (IMSS) con 54,906,396 derechohabientes en 2011 y el Instituto de Seguridad y Servicios Sociales de los Trabajadores del Estado (ISSSTE) con 12,206,730 derechohabientes, siendo el Distrito Federal el lugar donde la población derechohabiente de estas instituciones es mayor en comparación con otros estados de la república mexicana.

Figura 2. 14 Población derechohabiente del IMSS e ISSSTE en México.



Fuente: Elaboración propia con información de INEGI. (2013). Derechohabiencia y uso de servicios de salud- Población protegida por los servicios de salud, 2000 a 2011. Consultado en: http://www3.inegi.org.mx/sistemas/sisept/default.aspx?t=msoc01&s=est&c=22594

Adicionalmente las instituciones de salud deben cumplir con políticas internas, normas externas, así como leyes generales y federales. Ante este escenario es necesario que las instituciones de salud cuenten con un conjunto de estrategias que les brinden una visión integral de su problemática, así como, identificar aquellas oportunidades para cambiar de un enfoque de respuesta reactivo a uno proactivo.

Los pilares fundamentales sobre los cuáles deben definirse las estrategias son:

a) *Gobierno de TI:* este pilar tiene un enfoque global, a través del cual los altos directivos dirigen y controlan a toda la organización, todas las decisiones deberán estar alineadas a la visión y objetivos estratégicos de la entidad, además deben considerarse los procesos, los sistemas, las tecnologías y las personas.

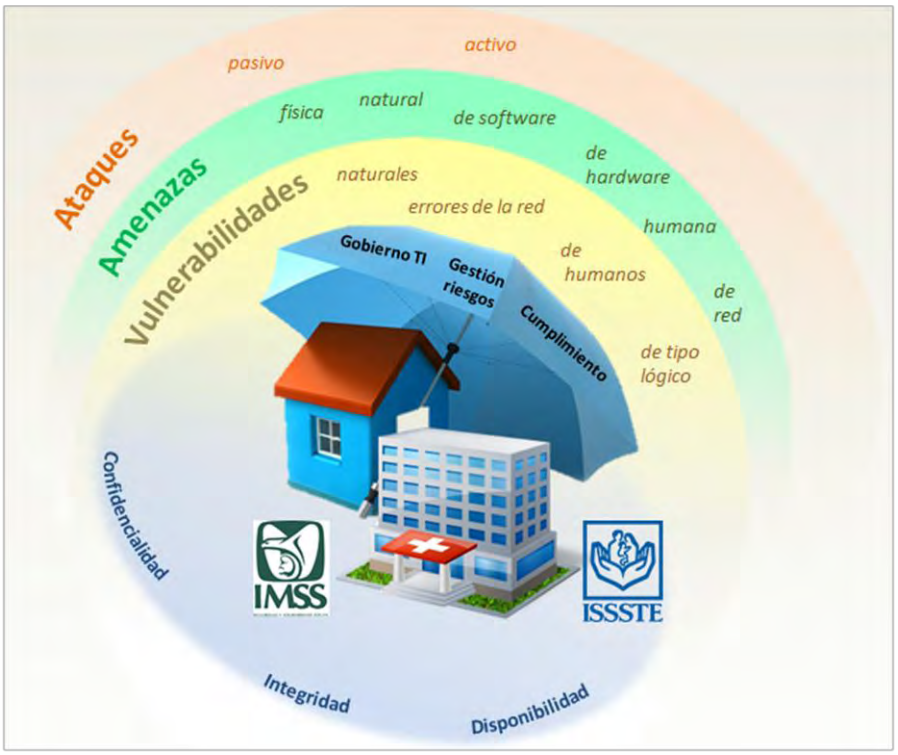
b) *Gestión de riesgos:* conjunto de procesos utilizados para identificar, analizar y responder a los riesgos que podrían afectar negativamente el cumplimiento con los objetivos de la organización.

c) *Cumplimiento:* a nivel organizacional es logrado a través de los procesos de gestión, las políticas, los contratos, las estrategias, las normas y las leyes. Además se evalúa el riesgo y posibles costos de incumplimiento, de forma que se establezcan prioridades y se identifiquen las medidas correctivas necesarias.

La gestión de riesgos como uno de los pilares fundamentales, al ser incorporado en el sector salud en México permitirá aprovechar y proteger los recursos de las tecnologías de la información de tal forma que contribuyan a mejorar la calidad y los tiempos requeridos para la prestación de los servicios, además de forjar una cultura en materia seguridad de la información, mediante programas de capacitación en materia de riesgos y seguridad, así como campañas de concienciación que difundan la importancia de contar con un proceso de gestión de riesgos de seguridad de la información en las instituciones de salud (Véase figura 2.14 Gestión de riesgos de seguridad de la información en el Sector salud en México).

El uso de las tecnologías de la información y comunicaciones en el sector salud en México ha incrementado, aumentando con ello el grado de exposición ante nuevas amenazas que pretenden afectar la confidencialidad, la disponibilidad y la integridad de los datos clínicos, ante esta situación es importante establecer medidas de protección para dar tratamiento a los riesgos identificados.

Figura 2. 15 Gestión de riesgos de seguridad de la información en el Sector salud en México.



Fuente: Elaboración propia.

Como un ejemplo sobre la importancia en identificar y dar tratamiento a los riesgos es el comunicado de las agencias estadounidenses *US Food and Drug Administration* (FDA)[2] e *Industrial Control Systems Cyber Emergency Response Team* (ICS-CERT)[3] emitido el 13 de junio de 2013 en el cual afirman la presencia de una vulnerabilidad en alrededor de 300 dispositivos médicos y cerca de 40 fabricantes distintos, la cual consiste en contraseñas por defecto embebidas en el código del controlador del dispositivo, que permite a un tercero con conocimientos sobre esta vulnerabilidad lograr un acceso privilegiado al dispositivo, alterando su funcionamiento y dejando en riesgo la integridad física del paciente, adicionando a ésta vulnerabilidad otros puntos débiles como son la falta de autenticación, la comunicación en texto plano, la carencia de firma digital en los firmwares y una programación sencilla, todo estos puntos presentados son áreas de oportunidad para los fabricantes que les permitirá mejorar la seguridad en sus productos, además de ser un llamado a las instituciones de salud para realizar revisiones tanto de funcionalidad como de seguridad en los dispositivos médicos utilizados en la operación.

[2] FDA *Safety Communication: Cybersecurity for Medical Devices and Hospital Networks:* http://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm356423.htm
[3] Alert (ICS-ALERT-13-164-01) *Medical Devices Hard-Coded Passwords* http://ics-cert.us-cert.gov/alerts/ICS-ALERT-13-164-01

Como se revisó a lo largo del capítulo existen varios modelos para gestionar y valorizar los riesgos de seguridad, sin embargo es fundamental que el sector salud en México cuente con una metodología personalizada a sus necesidades y objetivos, la cual brinde apoyo para lograr la identificación de sus activos críticos, le permita evaluar sus riesgos en términos de probabilidad de ocurrencia e impacto y una vez identificados, los tomadores de decisión cuenten con la información suficiente para definir las estrategias a seguir para su tratamiento. La metodología a su vez le permitirá el cumplimiento con leyes federales sobre la protección de los datos personales y datos personales sensibles.

Un proceso para la gestión de riesgos de seguridad de la información implementado en las instituciones de salud en México brindará una ventaja competitiva, además de un mayor control tanto de los recursos como de la seguridad de los mismos, favoreciendo la incorporación de nuevas tecnologías, así como de sistemas de información, lo cual actuará como catalizador para la madurez de los proyectos en curso, siendo uno de éstos la incorporación del expediente clínico electrónico.

En el siguiente capítulo se presenta el Sistema de Salud en México, acotando el análisis de estudio en dos de las instituciones de salud fundamentales para México, el Instituto Mexicano del Seguro Social (IMSS) y el Instituto de Seguridad y Servicios Sociales de los Trabajadores del Estado (ISSSTE), así como la identificación de las principales amenazas para los datos clínicos en México.

CAPÍTULO 3

SISTEMA DE SALUD EN MÉXICO

Los temas previamente abordados en capítulos anteriores sobre la importancia de la seguridad de la información aunada a la gestión de riesgos, son elementos fundamentales para enriquecer las estrategias actuales del Sector Salud. Para garantizar la efectividad de las estrategias en materia de seguridad de la información es fundamental conocer la estructura, el funcionamiento y el estado actual del Sistema de Salud en México, permitiendo así identificar tanto las áreas de oportunidad, como los principales riesgos en cuestiones relacionadas con la seguridad de la información.

En este capítulo se brinda información con mayor detalle sobre el Sistema de Salud en México, desde el marco jurídico, establecido en primera instancia por la Constitución Política de los Estados Unidos Mexicanos (CPEUM), seguido por la Ley General de Salud donde se definen las facultades del Sistema Nacional de Salud, los responsables de su coordinación y funcionamiento, además se presenta la estructura y los niveles de atención requeridos por el sistema para brindar el servicio. Como objeto de estudio se han seleccionado a dos de las instituciones de salud con mayor concentración de usuarios del servicio en México, el Instituto Mexicano del Seguro Social (IMSS) y el Instituto de Seguridad y Servicios Sociales de los Trabajadores del Estado (ISSSTE), razón por la cual a lo largo del capítulo se presentará a mayor detalle información sobre dichas instituciones.

Una vez que se cuenta con mayor conocimiento sobre el Sistema de Salud en México y de las instituciones de salud objeto de estudio, se identificarán las principales amenazas que atentan contra la seguridad de la información de los datos clínicos, análisis que permitirá identificar medidas preventivas y correctivas, dando como resultado nuevas directrices a seguir.

3.1 PANORAMA GENERAL DEL SISTEMA DE SALUD EN MÉXICO

El Sistema Nacional de Salud en México fue creado en cumplimiento al derecho que toda persona tiene a la protección de la salud, lo cual se encuentra establecido en el artículo 4° de la CPEUM. Formalmente se encuentra definido en la Ley General de Salud (LGS) en el Título Segundo

denominado Sistema Nacional de Salud, en el Capítulo 1 Disposiciones Comunes, en este apartado se presenta como está constituido el sistema, sus principales objetivos y la responsabilidad por parte de la Secretaría de Salud de llevar a cabo su coordinación *(LGS, 1984)*.

El Sistema Nacional de Salud es un instrumento para garantizar el derecho a la protección de la salud de la población, sus principales objetivos, según lo establecido en el artículo 6° de la LGS son:

a) Proporcionar servicios de salud a toda la población y mejorar la calidad de los mismos, atendiendo a los problemas sanitarios prioritarios y a los factores que condicionen y causen daños a la salud, con especial interés en las acciones preventivas.

b) Contribuir al desarrollo demográfico armónico del país.

c) Colaborar al bienestar social de la población mediante servicios de asistencia social, principalmente a menores en estado de abandono, ancianos desamparados y minusválidos, para fomentar su bienestar y propiciar su incorporación a una vida equilibrada en lo económico y social.

d) Dar impulso al desarrollo de la familia y de la comunidad, así como a la integración social y al crecimiento físico y mental de la niñez.

e) Impulsar el bienestar y el desarrollo de las familias y comunidades indígenas que propicien el desarrollo de sus potencialidades político sociales y culturales, con su participación y tomando en cuenta sus valores y organización social.

f) Apoyar el mejoramiento de las condiciones sanitarias del medio ambiente que propicien el desarrollo satisfactorio de la vida.

g) Impulsar un sistema nacional de administración y desarrollo de los recursos humanos para mejorar la salud.

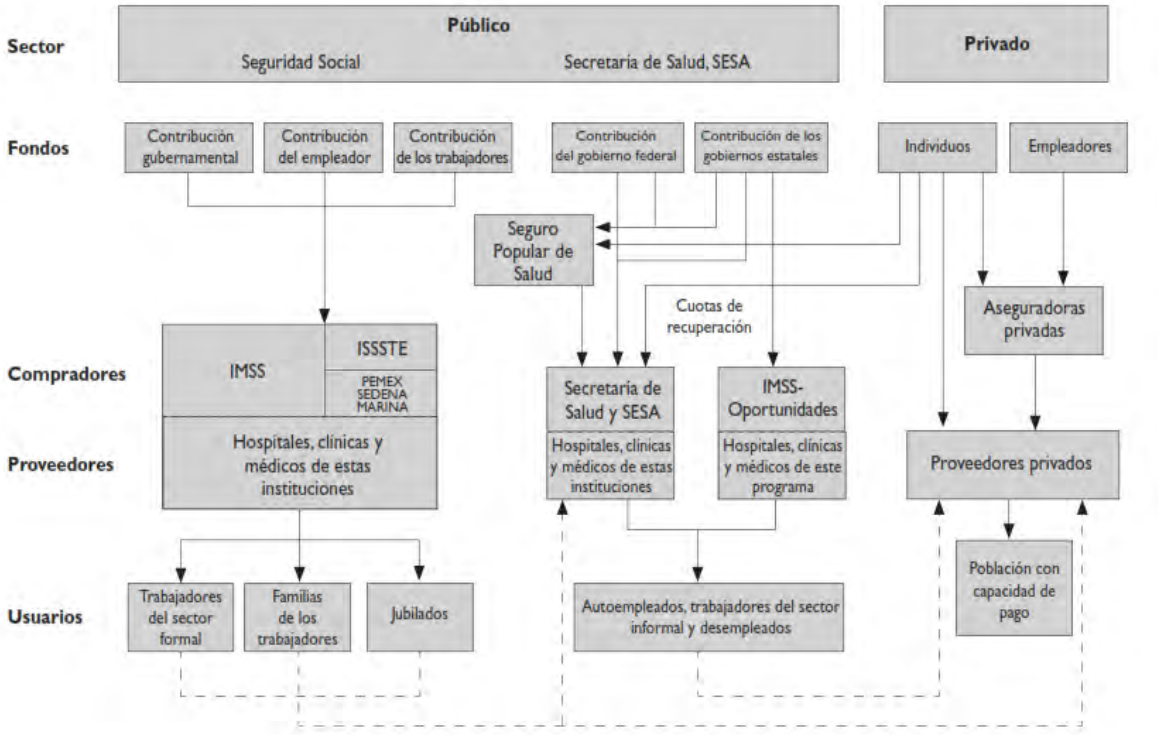
h) Promover el conocimiento y desarrollo de la medicina tradicional indígena y su práctica en condiciones adecuadas.

i) Coadyuvar a la modificación de los patrones culturales que determinen hábitos, costumbres y actitudes relacionados con la salud y con el uso de los servicios que se presten para su protección.

j) Promover un sistema de fomento sanitario que coadyuve al desarrollo de productos y servicios que no sean nocivos para la salud.

El sistema mexicano de salud se divide en dos sectores el público y el privado, su estructura se presenta en la figura 3.1 Estructura del Sistema de Salud de México y se describe más adelante.

Figura 3. 1 Estructura del Sistema de Salud de México



Fuente: Imagen obtenida de Gómez-Dantés, Octavio, Sesma, Sergio, Becerril, Victor M, Knaul, Felicia M, Arreola, Héctor, & Frenk, Julio. (2011). Sistema de salud de México. Salud Pública de México, 53(suplemento 2).

El sector público está integrado por instituciones de seguridad social como son el Instituto Mexicano del Seguro Social (IMSS), el Instituto de Seguridad y Servicios Sociales de los Trabajadores del Estado (ISSSTE), Petróleos Mexicanos (PEMEX), la Secretaría de la Defensa (SEDENA), la Secretaría de Marina (SEMAR) y otros, los servicios de salud que prestan estas instituciones a sus afiliados son financiados mediante contribuciones del empleador, que en el caso del ISSSTE, PEMEX y SEDENA es el gobierno, aunado a las contribuciones del empleado y aportaciones del gobierno. El sector público incluye además aquellas instituciones y programas que brindan atención a la población sin seguridad social, como son la Secretaría de Salud (SSa), los Servicios Estatales de Salud (SESA), el Programa IMSS-Oportunidades (IMSS-O) y el Seguro Popular de Salud (SPS), la SSa y los SESA se financian en gran parte con recursos del gobierno federal, además de recursos de gobiernos estatales y pagos de los usuarios en el momento en que reciben la atención, en el caso del IMSS-O es financiado con recursos del gobierno aunque la operación es responsabilidad del IMSS, por último el SPS se financia mediante contribuciones del gobierno federal, los gobiernos estatales y los individuos, quedando exentos de pago aquellos hogares de menores recursos *(Gómez-Dantés et al., 2011)*.

Por otro lado dentro del sector privado se encuentran las compañías aseguradoras y los prestadores de servicios que laboran en consultorios, clínicas y hospitales privados, incluyendo también los servicios de medicina alternativa. El financiamiento del sector privado incluye a los empleadores y los individuos que hacen uso del servicio.

Le estructura funcional del Sistema de Salud en México está integrado por tres niveles de atención *(González Guzmán & Castro Albarrán, 2010)*, lo cuales se describen a continuación y se ilustran en la figura 3.2 Estructura funcional del Sistema de Salud en México.

a) *Primer Nivel de atención:* formado por una red de unidades médicas que atienden a nivel ambulatorio, es decir tratamiento de enfermedades que no requieren hospitalización, este nivel es el primer contacto de las personas con el sistema formal de atención, el tamaño de las instituciones puede variar, desde unidades de un solo consultorio, hasta con 30 o más consultorios y servicios auxiliares (laboratorio, rayos X, ultrasonido, medicina preventiva, epidemiología, farmacia, central de esterilización y equipos, administración y aulas). En las unidades de primer nivel trabajan médicos generales con estudios de licenciatura o con estudios de especialidad en algún posgrado, médicos pasantes, así como enfermeras y técnicos.

b) *Segundo Nivel de atención:* integrado por una red de hospitales generales para brindar atención a problemas de salud que demanden internamiento hospitalario o atención de urgencias, las unidades del segundo nivel de atención están organizadas en cuatro especialidades básicas de la medicina, la cirugía, la pediatría, la ginecobstetricia y la medicina interna, el grado de complejidad en las unidades médicas de segundo nivel es mayor y en su organización destacan servicios como urgencias, hospitalización, admisión, banco de sangre, central de esterilización y equipos, quirófanos, consulta externa y farmacia, con frecuencia los hospitales de segundo nivel brindan atención de subespecialidades como dermatología, neurología, cardiología, cirugía pediátrica entre otras, razón por la cual cuentan con un mayor número de médicos especialistas.

c) *Tercer Nivel de atención:* una red de hospitales de alta especialidad forman parte de este nivel, en los cuáles hay subespecialidades y equipos de apoyo que no se encuentran en el segundo nivel de atención. Los hospitales de este nivel pueden contar con una gran cantidad de subespecialidades, como sucede con las Unidades Médicas de Alta Especialidad del IMSS o el Instituto Nacional de Ciencias Médicas y Nutrición, o pueden estar especializados en algún campo específico, como sucede con otros Institutos Nacionales de Salud, especializados en cancerología, cardiología, pediatría, enfermedades respiratorias, neurología, geriatría y rehabilitación. El tercer nivel brinda atención a problemas que no puedan ser resueltos en los otros dos niveles y que requieran conocimientos más especializados o una tecnología específica por lo general costosa.

Figura 3. 2 Estructura funcional del Sistema de Salud en México.

Fuente: Elaboración propia con información de González Guzmán, R Moreno Altamirano, L, & Castro Albarrán, JM. (2010). La salud pública y el trabajo en comunidad (M. G. Hill Ed. Primera Edición ed.).

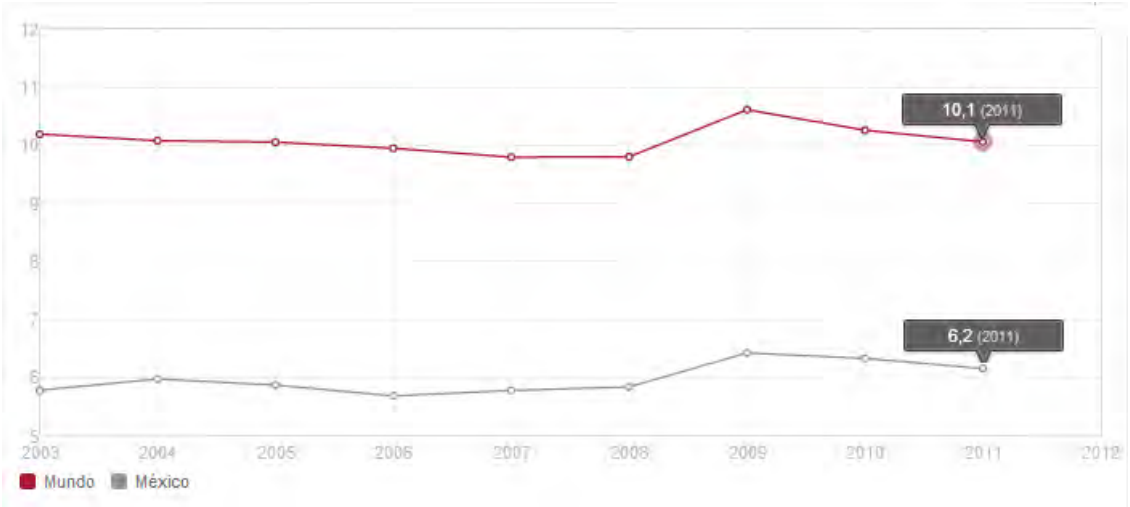
El Sistema Nacional de Salud en la actualidad se encuentra segmentado en diversas instituciones, que en algunos casos brindan el servicio de salud discriminando a las personas de acuerdo al lugar que éstos tienen en la sociedad, así como su perfil ocupacional o su capacidad de pago. La fragmentación del sistema genera que en la actualidad existan grupos de la población con derechos distintos y una calidad del servicio variable, en consecuencia a esta situación la población busca atención médica en el ámbito privado, la asistencia social o recurren a la automedicación.

Algunos de los factores que afectan la prestación de los servicios de salud en México son: los modelos de las instituciones de salud con una orientación más curativa que preventiva, la situación organizacional fragmentada tanto a nivel institucional como de forma interna, considerando que en la gran mayoría de las instituciones de salud existe una clara división entre el personal administrativo y el personal médico, lo cual genera la burocratización innecesaria de trámites, que en consecuencia impactan significativamente en los tiempos de atención, diagnóstico, calidad y tratamiento por parte del personal médico, además de políticas para mejorar los servicios de salud que no han sido adecuadamente implementadas o permeadas a nivel organizacional. Todos estos factores además de impactar en el tiempo y la calidad en la prestación de los servicios de salud, afecta considerablemente la seguridad de la información de los datos clínicos considerando que el eslabón más débil de la cadena en seguridad es el factor humano.

El Sistema de Salud en México cuenta con una amplia red de atención médica como resultado de la inversión que el gobierno federal ha designado para mejorar la prestación de servicios de salud, hecho que se ha reflejado, según datos del Banco Mundial en un incremento del porcentaje del PIB

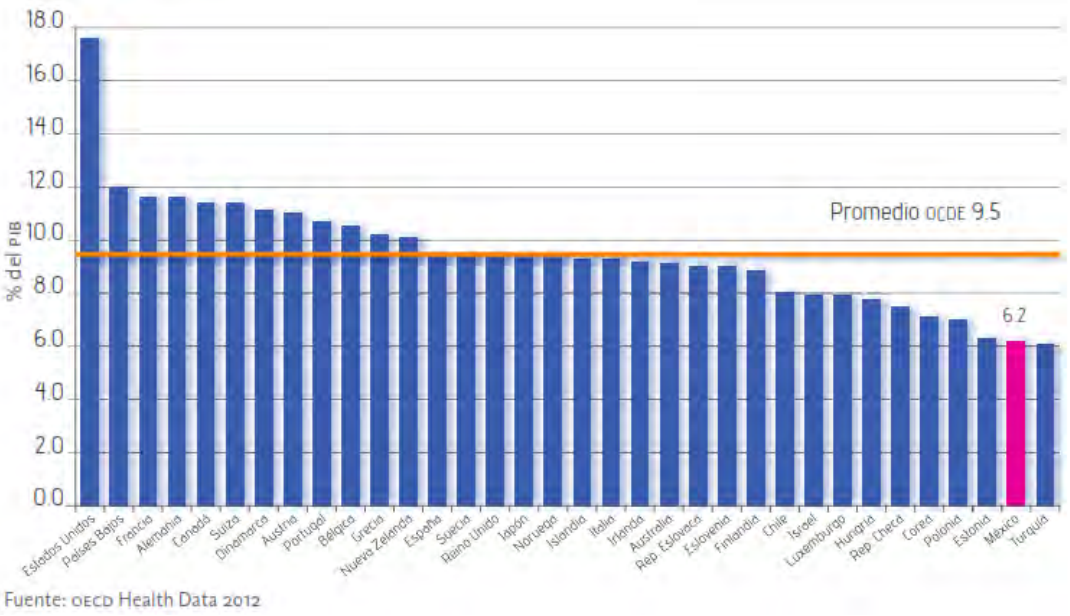
destinado para gastos en salud, de un 5.8 % en el año 2008 a un 6.2 % en el año 2011, decisión que ha favorecido al Sistema de Salud en México fortaleciendo la infraestructura y mejorando los recursos tecnológicos disponibles para la prestación de los servicios de salud a la población, sin embargo cabe señalar que aún con los esfuerzos realizados por el gobierno, México se encuentra por debajo del promedio a nivel mundial cuyo porcentaje del PIB destinado para gastos en salud es de 10.1% para el año 2011 (véase figura 3.3 Gasto en salud, total % del PIB- Banco Mundial) y de igual forma por debajo del promedio de los países de la Organización para la Cooperación y Desarrollo Económicos (OCDE) cuya inversión es de 9.5 %, en 2010 (véase figura 3.4 Gasto total en salud, % del PIB- Países de la OCDE 2010), situación que permite observar la necesidad de incrementar el gasto en salud en México, con el objeto de mejorar las instituciones responsables de prestar el servicio, como una forma de contribuir al cumplimiento del objetivo 2.3 Asegurar el acceso a los servicios de salud y sus estrategias establecidas en el Plan Nacional de Desarrollo (PND) 2013-2018, que de forma general buscan: avanzar hacia la universalidad de los servicios de salud, establecer como eje prioritario la protección, promoción y prevención, además de mejorar la atención de la salud para la población en situación de vulnerabilidad, garantizar el acceso efectivo a servicios de calidad y promover la cooperación internacional en materia de salud.

Figura 3. 3 Gasto en salud, total % del PIB- Banco Mundial



Fuente: Imagen obtenida de Banco Mundial, BM. (2013). Gasto en salud, total (% del PIB). Consultado en: http://datos.bancomundial.org/indicador/SH.XPD.TOTL.ZS/countries?display=graph

Figura 3. 4 Gasto total en salud, % del PIB- Países de la OCDE 2010.



Fuente: Imagen obtenida de FUNSALUD, Fundación Mexicana para la Salud. (2012). Universalidad de los Servicios de Salud. Propuesta de FUNSALUD, A. Fundación Mexicana para la Salud (Ed.). Consultado en: http://funsalud.org.mx/eventos_2012/Universalidad%20de%20los%20servicios%20de%20salud/UNIVERSALIDAD%20DE%20LOS%20SERVICIOS_DEF.pdf

Para dar una mejor respuesta a las necesidades de la población en materia de salud es necesaria una planeación interinstitucional de largo plazo, con estrategias claramente definidas, una mejor administración de riesgos, así como el compromiso y corresponsabilidad entre instituciones. Además es fundamental considerar los controles necesarios para garantizar la protección de la información que es creada, almacenada y transmitida en las instituciones de salud.

El Sistema de Salud en México enfrenta grandes retos tanto a nivel organizacional como operativo, por un lado es necesario ampliar la cobertura del servicio y por otro mejorar la calidad y eficiencia de las instituciones que se encuentran actualmente en operación y que dado el crecimiento de la población se encuentran saturadas y con escasos recursos, lo cual complica significativamente la prestación de servicios que garanticen la satisfacción de los usuarios.

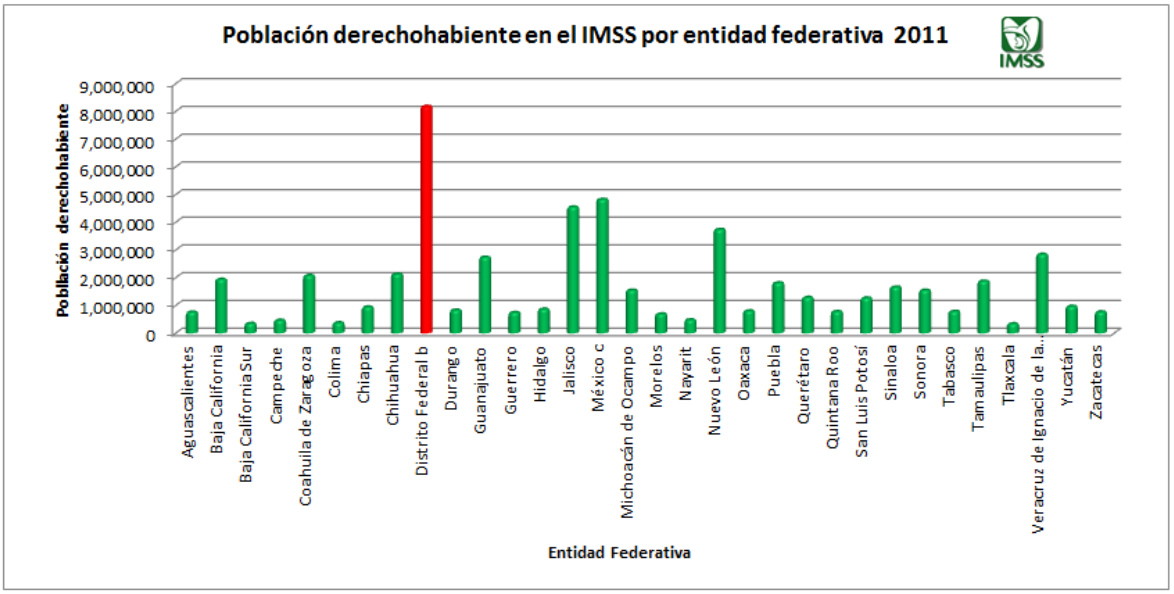
3.1.1 IMSS

El Instituto Mexicano del Seguro Social (IMSS) surge en 1943 con el objetivo de mantener la salud de los trabajadores de México y de sus familias, cubre a los trabajadores del sector formal de la economía, su forma de financiamiento es tripartita, es decir, financiado por las contribuciones de los trabajadores, los patrones y el gobierno federal.

Para el año 2011 según informes del Instituto Nacional de Estadística y Geografía (INEGI) el IMSS contaba con 54,906,396 derechohabientes en todo el país y 8,176,887 en el Distrito Federal lugar donde se presenta la mayor concentración de derechohabientes (véase figura 3.5 Población derechohabiente en el IMSS por entidad federativa 2011) .

Para el año 2012 el IMSS reportó 57,475,897 derechohabientes en todo el país y 8,396,096 para el Distrito Federal *(INEGI, 2012)*.

Figura 3. 5 Población derechohabiente en el IMSS por entidad federativa 2011



Fuente: Elaboración propia con información de INEGI. (2012). Población derechohabiente en el IMSS según tipo de derechohabiencia por entidad federativa, 2011. Consultado en: http://www3.inegi.org.mx/sistemas/sisept/default.aspx?t=msoc04&s=est&c=27724

Los servicios de atención médica del IMSS son otorgados en unidades organizadas considerando dos criterios principales:

1. *Por niveles de atención:* estos niveles responden a la complejidad del daño que atienden y a la frecuencia en la que se presenta en la población, considerando estas dos variables son creadas las instalaciones y asignados los recursos.

2. *Por regiones:* este criterio considera la distribución geográfica de las unidades de servicios en regiones del país, donde cada una deberá contar con los tres niveles de atención.

Con base en el Informe al Ejecutivo Federal y al Congreso de la Unión sobre la situación financiera y los riesgos del Instituto Mexicano del Seguro Social 2012-2013, en su apartado XI. Instalaciones y Equipo del Instituto se definen los tres niveles de atención y sus principales características:

a) *Primer nivel de atención*: se desarrolla en unidades de medicina familiar, brindan atención a problemas de salud frecuentes y relativamente de baja complejidad, para dar atención a la población en este nivel, el instituto cuenta con 1,499 unidades, de las cuales, 1,118 son Unidades de Medicina Familiar (UMF), 381 corresponden a unidades auxiliares, con una antigüedad promedio de 34 y 27 años respectivamente.

b) *Segundo nivel de atención:* nivel que cuenta con recursos que permiten la atención de problemas más complejas y menos frecuentes, este servicio se brinda en hospitales generales, actualmente el instituto cuenta con 38 Unidades Médicas de Atención Ambulatoria (UMAA), de las cuales 10 corresponden a unidades independientes y 28 a unidades anexas a UMF u hospitales. Las UMAA tienen una edad promedio de siete años.

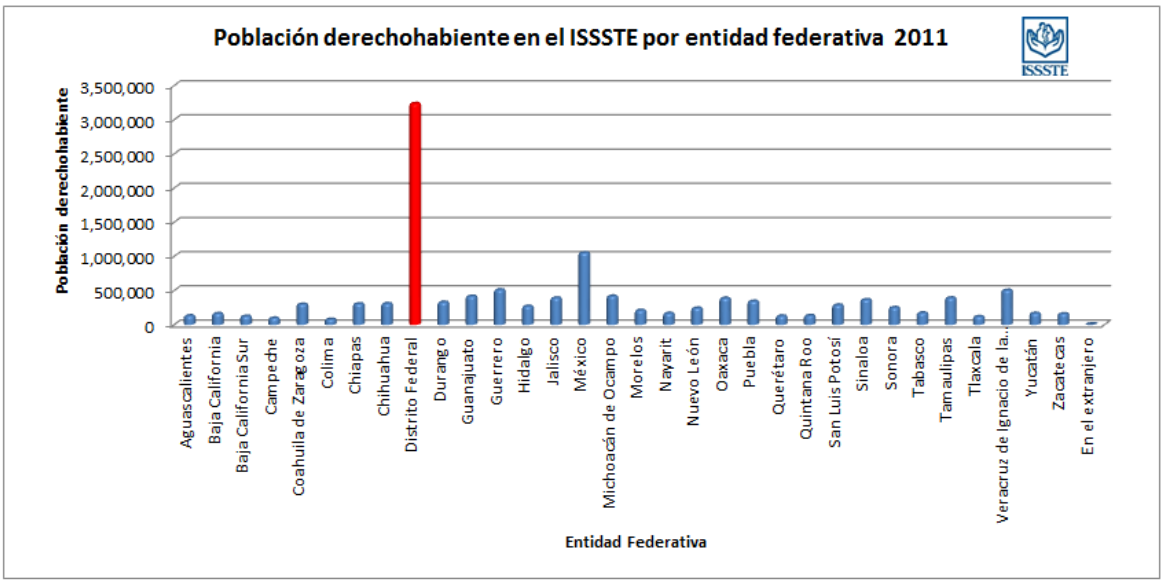
c) *Tercer nivel de atención:* este nivel se restringe a la atención de problemas de salud complejos y poco frecuentes, aquellos que requieren de una gran especialización en determinadas áreas de la medicina, la cirugía y alta tecnología. Para prestar el servicio a los derechohabientes el instituto cuenta con 25 Unidades Médicas de Alta Especialidad (UMAE) y 11 unidades médicas complementarias. La infraestructura que forma parte del tercer nivel tiene, en promedio 39 años de antigüedad.

3.1.2 ISSSTE

El Instituto de Seguridad y Servicios Sociales de los Trabajadores del Estado (ISSSTE) fue creado en 1960, contribuye a satisfacer los niveles de bienestar integral de los trabajadores al servicio del estado, familiares de los derechohabientes, pensionados y jubilados. Su financiamiento depende de las contribuciones del gobierno federal como patrón, con un monto fijo, así como de los trabajadores.

Para el año 2011 el Instituto Nacional de Estadística y Geografía (INEGI) indica que el ISSSTE contaba con 12,206,730 derechohabientes en todo el país y 3,237,015 en el Distrito Federal, lugar donde se presenta la mayor concentración de derechohabientes (véase figura 3.6 Población derechohabiente en el ISSSTE por entidad federativa 2011).

Figura 3. 6 Población derechohabiente en el ISSSTE por entidad federativa 2011



Fuente: Elaboración propia con información de INEGI. (2011b). Población derechohabiente en el ISSSTE según tipo de derechohabiencia por entidad federativa, 2011. Consultado en: http://www3.inegi.org.mx/sistemas/sisept/default.aspx?t=msoc05&s=est&c=27726

El ISSSTE cuenta con el Sistema Institucional de Servicios de Salud que se organiza y opera en tres niveles de atención, a través de 4 delegaciones regionales en el Distrito Federal y una delegación en cada estado de la República Mexicana. El tipo de unidad determina la capacidad física instalada, el equipamiento, la dotación de insumos, la asignación de personal médico y enfermeras que satisfagan las demandas en materia de salud de los derechohabientes.

Al 31 de diciembre del 2011 según el Informe Financiero y Actuarial 2012, el ISSSTE contaba con 1,182 unidades médicas distribuidas entre los tres niveles de atención, que se describen a continuación:

a) *Primer nivel de atención:* representa el primer contacto en el servicio a la salud del derechohabiente con el ISSSTE, en este nivel se realizan acciones enfocadas básicamente a ofrecer servicios curativos, preventivos y de atención a riesgos. La infraestructura de este nivel está conformada por consultorios auxiliares, unidades y clínicas de medicina familiar. El ISSSTE cuenta con 1,051 unidades que corresponden al primer nivel de atención y que representan para el instituto el 89% de la infraestructura médica con la que cuenta, en promedio la antigüedad de los inmuebles es de 21.3 años siendo la antigüedad máxima de 52 años y la menor de un año.

b) *Segundo nivel de atención:* en este nivel se otorgan servicios de consulta externa de especialidades y hospitalización de las cuatro especialidades básicas: cirugía general, ginecobstetricia, medicina interna y pediatría, así como auxiliares para el diagnóstico y tratamiento con procedimientos de mediana complejidad. La infraestructura médica destinada a cubrir este nivel está constituida por las clínicas de especialidad, las clínicas y hospitales generales. El ISSSTE cuenta con 118 unidades para prestar el servicio en este nivel, que representan el 10% de los inmuebles médicos del instituto, la antigüedad promedio de éstos es de 26.6 años, siendo la máxima antigüedad de 57 años y la mínima de un año.

c) *Tercer nivel de atención:* las 13 unidades que integran este nivel corresponden a hospitales con mayor capacidad resolutiva y física instalada, cuentan con personal especializado y tecnologías de vanguardia para la integración de diagnósticos y ejecución de procedimientos médico quirúrgicos de alta complejidad. El 1% del total de los inmuebles médicos que tiene el instituto pertenecen a unidades de tercer nivel de atención conformado por Hospitales de Alta Especialidad y el Centro Médico Nacional.

3.2 PRINCIPALES AMENAZAS EN LOS DATOS CLÍNICOS

El Sistema de Salud en México ha recurrido a la incorporación de tecnologías de la información en su operación, como una estrategia para ampliar la cobertura en la atención médica, mejorar la calidad del servicio, reducir los errores médicos, optimizar la disponibilidad de acceso, legibilidad y difusión de la información, si bien esta medida ha mejorado la operación en las diferentes instituciones de salud en México, a su vez ha generado nuevos retos en materia de seguridad de la información que deben ser considerados para el cumplimiento con las leyes en materia de datos personales y privacidad. En la actualidad las instituciones de salud cuentan con medidas para la protección de la información, que en algunos casos son deficientes debido a que no están respaldadas por estrategias sólidas, necesarias para una adecuada gestión de seguridad de la información. El documento del año 2012 denominado XIV Encuesta Global de seguridad de la información de la firma *Ernst & Young* muestra aspectos importantes sobre las principales medidas implementadas para controlar la fuga de información sensible en México tanto en el sector público como privado (véase figura 3.7 Acciones tomadas para controlar la fuga de información), en este gráfico se presentan las cinco principales acciones tomadas para evitar la fuga de información, como son:

a) Definición de políticas sobre la clasificación y manejo de información sensible.
b) Programas de concientización.
c) Auditorías internas para verificar los controles implementados.
d) Implantar mecanismos de seguridad adicionales para proteger la información, por ejemplo el cifrado.

e) Restricción o prohibición de mensajería instantánea o uso de correo para el envío de información sensible.

Figura 3. 7 Acciones tomadas para controlar la fuga de información.

Fuente: Imagen obtenida de EY. (2012). XIV Encuesta Global de Seguridad de la Información: Ernst & Young. Consultado en: http://www.ey.com/Publication/vwLUAssets/Salir_de_la_niebla_para_entrar_a_la_nube/$FILE/XIV_EGSI_Salir_niebla_%20para_entrar_nube.pdf

Además este mismo documento muestra la situación actual en México en materia de administración de riesgos de tecnologías de información, claramente reflejando que un 45% de las instituciones encuestadas no cuentan con un programa formal para administrar sus riesgos, pero sí tienen iniciativas para implementarlo en los próximos doce meses (véase figura 3.8 Situación actual en México en materia de administración de riesgos de TI), situación que es altamente alarmante debido a que la gestión de riesgos es uno de los pilares sobre los cuales se debe fundamentar cualquier estrategia relacionada con la seguridad de la información, ya que permite identificar las amenazas y vulnerabilidades que pueden dañar los activos de la organización, además como resultado de este proceso se obtienen los controles adecuados para garantizar la seguridad de la información.

Figura 3. 8 Situación actual en México en materia de administración de riesgos de TI.

Fuente: Imagen obtenida de EY. (2012). XIV Encuesta Global de Seguridad de la Información: Ernst & Young. Consultado en: http://www.ey.com/Publication/vwLUAssets/Salir_de_la_niebla_para_entrar_a_la_nube/$FILE/XIV_EGSI_Salir_niebla_%20para_entrar_nube.pdf

Ante estos escenarios es necesario establecer planes estratégicos avalados por la dirección, para optimizar los controles de seguridad ya existentes e incorporar aquellos que sean necesarios para mejorar los niveles de seguridad en las instituciones de salud, los controles deberán ser resultado de un proceso para la gestión de riesgos eficazmente implementado, que proporcione toda la información relacionada con amenazas, vulnerabilidades y riesgos asociados a los activos críticos de la entidad, así como estar respaldados por estándares nacionales e internacionales, buenas prácticas y marcos de referencia en materia de seguridad de la información.

El estándar *ISO 27799:2008 Health informatics- Information security management in health using ISO/IEC 27002* en su anexo A presenta 25 amenazas que afectan la seguridad de los datos clínicos, información que es presentada a continuación:

1. *Suplantación por empleados:* esta amenaza consiste en hacer uso de sistemas mediante el acceso con una cuenta que corresponde a otro usuario, en muchos casos esta situación se presenta como una forma de facilitar el trabajo, por ejemplo cuando el médico que toma la guardia continúa con las anotaciones en el sistema haciendo uso de la sesión que dejo abierta su compañero del turno anterior. El hacerse pasar por personal de la institución afecta la confidencialidad de la información y también puede llevarse a cabo con la intención de encubrir casos en que el daño ha sido causado.

2. *Suplantación por proveedores de servicios:* incluyen personal de mantenimiento como ingenieros de software, personal de reparación de hardware u otras personas con acceso a los sistemas y los datos, que mediante los privilegios concedidos en razón de sus funciones acceden de forma no autorizada a los datos. La materialización de esta amenaza muestra las debilidades existentes en el proceso de subcontratación de los proveedores de servicios.

3. *Suplantación por externos:* se produce cuando terceras personas no autorizadas, como hackers, periodistas e investigadores privados tienen acceso a datos o recursos de los sistemas, ya sea mediante la suplantación de un usuario autorizado o recurriendo a técnicas de ingeniería social u otro tipo de ataques para obtener el acceso. Para llevar a cabo esta amenaza se aprovechan fallos en controles como la identificación y autenticación de usuarios, controles de acceso y la gestión de privilegios.

4. *Uso no autorizado en programas o aplicaciones de información de salud:* consiste en obtener acceso a programas o aplicaciones utilizadas en la operación para la creación, almacenamiento y transferencia de la información en materia de salud, afectando la confidencialidad y en algunos casos la integridad de la misma. Esta amenaza puede llevarse a cabo tanto por personal interno como externo, aprovechando fallas en los controles de acceso y en la seguridad del personal.

5. *Introducción de software dañino o perjudicial*: esta amenaza incluye virus, gusanos y otro tipo de malware, que afecte los dispositivos que forman parte de la infraestructura de TI de la institución, la materialización de esta amenaza reflejará una clara deficiencia en los controles implementados para la detección de malware, como son los antivirus, así como software para el control de cambios en las configuraciones de los equipos.

6. *Mal uso de los recursos de los sistemas:* esta amenaza considera el mal uso de los recursos con que cuentan las instituciones de salud por parte del personal, por ejemplo la descarga de información no relacionada con el trabajo haciendo uso de los recursos de red de la institución, afectando el ancho de banda y con ello la disponibilidad de la información, para evitar la materialización de esta amenaza es necesario concientiza a los usuarios para hacer uso adecuado de los recursos disponibles para llevar a cabo su trabajo.

7. *Infiltración de las comunicaciones:* implica una interferencia en el flujo normal de los datos a través de una red, siendo el resultado más común un ataque de denegación de servicio, esta amenaza puede ser materializada al presentarse deficiencias en los sistemas de detección de intrusos, en los controles de acceso a la red o en el análisis de vulnerabilidades como parte de un análisis de riesgos.

8. *Intercepción de las comunicaciones:* si la información no se cifra durante la trasmisión la confidencialidad de la misma puede ponerse en riesgo, ya que esta amenaza considera que cualquier persona que cuente con acceso a la red local podría instalar algún software que le permita el monitoreo del tráfico en la red y conocer la información que es transmitida, esta

amenaza puede ser materializada cuando se presentan fallas en la seguridad de las comunicaciones.

9. *Desconocimiento:* esta amenaza considera la negación por parte del usuario de la recepción o envió de mensajes, para ello se aprovechan fallas en la aplicación de controles como la firma digital o controles de lectura y envío en los correos electrónicos.

10. *Falla en la conexión:* se relaciona con la calidad de los servicios de red, requeridos por la institución para llevar a cabo la operación diaria, puede generar una divulgación no autorizada de la información al obligar a los usuarios a enviar mensajes mediante medios menos seguros.

11. *Incorporación de código malicioso:* esta amenaza hace referencia a los virus de correo electrónico, así como a códigos maliciosos en otro tipo de dispositivos, como resultado del creciente uso de tecnologías inalámbricas y móviles por profesionales de la salud incrementando así el riesgo de sufrir daños por este tipo de amenaza. La afectación por códigos maliciosos constituye una falla en programas para su detección como son los antivirus y el software para controlar y prevenir intrusiones.

12. *Enrutamiento erróneo accidental:* consiste en la posibilidad de que la información que es enviada a través de la red sea entregada a una dirección incorrecta, este tipo de incidentes reflejan una falla en la formación de los usuarios o la incapacidad de mantener la integridad en los directorios de los proveedores de salud o ambas.

13. *Fallas técnicas en los equipos, instalaciones de almacenamiento o en la infraestructura de red:* estas amenazas incluyen fallos en el hardware, errores en la red o afectaciones en las instalaciones que almacenan la información, la pérdida de la disponibilidad de dichos recursos puede ocasionar un daño considerable en la vida de los pacientes ya que afecta la continuidad de la operación.

14. *Fallas de soporte ambiental:* incluye los apagones e interrupciones de servicio generados por desastres naturales o producido por el hombre, los sistemas de información de salud son activos críticos que deben ser protegidos de este tipo de eventos, cuyas consecuencias pueden ser catastróficas. Para reducir el impacto de estos incidentes es necesario realizar evaluaciones de riesgos periódicas e implementar controles que garanticen la continuidad de las operaciones y la seguridad de los activos críticos en caso de una contingencia, esta información deberá estar plasmada en un plan de recuperación de desastres y un plan para la continuidad del negocio que deberá ser difundido a todo el personal de la institución.

15. *Fallas en software de red o de sistemas:* ataques de denegación de servicio son posibles en gran medida debido a las deficiencias o errores en las configuraciones de los sistemas operativos y en el software de red. La presencia de estos eventos indican una deficiencia en

la verificación de la integridad del software, en las pruebas a los sistemas o en los controles de mantenimiento.

16. *Fallas en software de aplicación:* estas fallas pueden ser explotadas por ataques de denegación de servicio y ser utilizadas para comprometer la confidencialidad de los datos, estos ataques pueden ocurrir como resultado de aprovechar los fallos en controles como son las pruebas, la verificación de integridad y los controles de cambio en el software instalado.

17. *Uso indebido:* el uso indebido de cuentas representa un pequeño pero significativo porcentaje de las revelaciones no intencionadas de información confidencial y una gran parte de las disposiciones accidentales de datos, el llevar a cabo esta amenaza indica fallos en los controles operativos, en la seguridad del personal y en la recuperación de desastres.

18. *Error de mantenimiento:* son errores cometidos por aquellos responsables del mantenimiento de los sistemas de hardware y software, ya sea miembros de la institución o terceros que sean contratados para realizar dichas tareas, la presencia de este tipo de errores pone en peligro la confidencialidad de los datos y a su vez afecta la continuidad de las operaciones. Una mala configuración en el software durante la instalación es una de las vulnerabilidades aprovechadas con mayor frecuencia por los hackers.
    La presencia de este tipo de errores constituye una deficiencia en los controles relacionados con el mantenimiento de hardware, software así como en el control de cambios.

19. *Errores de usuarios:* ejemplo de este tipo se presenta cuando un usuario envía por descuido información a destinatarios erróneos, estos incidentes se presentan por fallas en los controles de usuario como son el diseño de interfaces de los sistemas o la falta de capacitación.

20. *Escases de personal:* esta amenaza se refiere a la posibilidad de perder personal clave para la institución y la dificultad para reemplazarlo, la vulnerabilidad a esta amenaza depende de la medida en que la escasez de personal pueda afectar los procesos de la institución. Un fallo de este tipo constituye un fracaso en la gestión de la continuidad del negocio.

21. *Robo de información privilegiada por personal interno:* se presenta cuando personal de la institución que aprovechando su posición favorable dentro de la misma, roba información con la finalidad de divulgarla o lucrar con ella. El robo de información privilegiada constituye una clara deficiencia en controles relacionados con la seguridad física, la información impresa, el control de acceso y la protección de los equipos entre otros.

22. *Robo de información privilegiada por sujetos externos:* el robo de datos y equipo es un grave problema para los hospitales que afecta considerablemente la confidencialidad de la información, el robo por personal externo implica deficiencias en controles de informática móvil, el manejo de incidentes, cumplimiento o la protección contra el robo físico.

23. *Daños intencionales por los internos:* esta amenaza incluye actos de vandalismo y otros casos donde el daño físico causado a los sistemas informáticos o al entorno, es generado por personal que cuenta con accesos, incidentes de este tipo reflejan una falla en la seguridad de los recursos humanos, además de una falta de concientización en materia de protección de la información y sobre uso de los recursos.

24. *Daños intencionales por externos:* esta amenaza incluye actos de vandalismo, así como daños físicos a los sistemas informáticos o al entorno, en este caso los daños son ocasionados por personal que no han tenido acceso a este tipo de sistemas. En la mayoría de los sectores industriales para evitar esta amenaza se implementan rigurosos controles de seguridad física, en el caso de los hospitales, donde ingresan diariamente una gran cantidad de personas a las instalaciones, esta amenaza es más difícil de impedir y los controles a implementarse deben ser seleccionados con mayor cuidado.

25. *Terrorismo:* incluye actos cometidos por grupos extremistas que desean dañar o perturbar el trabajo de las organizaciones de salud, afectar a los proveedores o perturbar el funcionamiento de los sistemas de información sanitaria.

La protección de los datos personales y los datos clínicos son temas que genera una gran preocupación, en el documento *Unlocking the value of Personal Data: from collection to Usage* del Foro Económico Mundial se hace mención sobre el impacto generado por las nuevas tecnologías, políticas, modelos de negocio y normas sociales que han influido en el manejo y la generación de los datos personales, donde el principal cambio radica en que actualmente los individuos son más que los propietarios de los datos, el acceso a nuevas tecnologías como son los dispositivos móviles han generado que en la actualidad los individuos sean productores de los datos, un ejemplo de ello es el uso de aplicaciones móviles para el monitoreo de la salud, de igual forma el surgimiento de nuevas tecnologías como la telemedicina, el cómputo móvil y el uso del expediente clínico electrónico están revolucionando la prestación de servicios de salud, siendo responsabilidad de las instituciones establecer medidas y controles para garantizar la seguridad de la información que es creada, almacenada y transmitida en todos los dispositivos requeridos en la operación diaria, de tal forma que sea transparente para el individuo la forma en que son utilizados y protegidos sus datos *(WEF, 2013b).*

Para la definición de una estrategia de seguridad de la información efectiva las instituciones de salud deben considerar, el nivel de concientización en materia de seguridad de la información del personal, los cambios y riesgos asociados con el uso de redes sociales, el apoyo y patrocinio de la dirección, los cambios organizaciones y las tecnologías emergentes *(Piñar & Ornelas, 2013).*

Dentro de las medidas implementadas en México para la protección de los datos personales que están en posesión de las dependencias y entidades de la administración pública federal el Instituto Federal de Acceso a la Información y Protección de Datos (IFAI) ha creado el documento denominado “Recomendaciones sobre medidas de seguridad aplicables a los sistemas de datos personales”, el cual es una lista de verificación para evaluar el cumplimiento de los sujetos

obligados por la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental (LFTAIPG) respecto al resguardo de los datos personales en posesión del estado. En el caso del sector salud la Dirección General de Información en Salud (DGIS) de la Secretaría de Salud coordina la elaboración de guías y formatos que orientan a los prestadores de servicios de salud para lograr la interoperabilidad semántica y técnica en escenarios concretos de intercambio de información entre Sistemas de Información de Registro Electrónico en Salud (SIRES), además se cuenta con una guía denominada "Guía de intercambio de información en salud para un Sistema de Gestión de la Seguridad de la Información en salud" documentos elaborados considerando estándares internacionales como el ISO 27001, ISO 27002 y el ISO 27799.

Una vez presentado el marco teórico, en estos tres capítulos que han dado sustento a la investigación, y donde se han definido desde conceptos generales como los datos clínicos, la seguridad de la información, la gestión de riesgos y la descripción del Sistema de Salud en México, se presentará en el siguiente capítulo el diseño formal de la investigación, desde el planteamiento del problema, las variables involucradas, las preguntas de investigación, los objetivos y la hipótesis de trabajo, además en este apartado se diseñará el instrumento que será aplicado en la unidad de análisis.

CAPÍTULO 4

DISEÑO DE LA INVESTIGACIÓN

En capítulos previos se estableció el marco teórico que reúne la información documental sobre el tema de investigación, vinculando de esta forma los conceptos de seguridad de la información, los datos clínicos y la gestión de riesgos. En el presente capítulo se describe el diseño de la investigación, definido como un esquema o programa para llevar a cabo un proyecto, especifica los detalles de los procedimientos que son necesarios para obtener la información requerida, para estructurar y/o resolver los problemas identificados *(Malhotra, Martínez, & Rosales, 2004)*, de tal forma que se plantea el problema de investigación, las preguntas y los objetivos, además de la hipótesis de trabajo, las variables y la metodología que será utilizada. En este apartado se describe como está constituido el instrumento y el procedimiento a seguir para su aplicación en la unidad de análisis seleccionada.

4.1 PLANTEAMIENTO DEL PROBLEMA DE INVESTIGACIÓN

En un mundo hiperconectado donde la incorporación de tecnologías ha evolucionado no sólo la creación, el intercambio y la difusión de información, a su vez han dado lugar a nuevas amenazas que afectan la confidencialidad, la disponibilidad y la integridad de los datos, esta situación no es única en sectores tecnológicos o en grandes empresas o instituciones. El sector salud en México enfrenta grandes retos en materia de seguridad de la información, considerando que en los últimos años se han incorporado nuevas tecnologías, como una medida para renovar y agilizar la prestación de servicios, aunado a iniciativas de integrar los datos clínicos en un expediente electrónico y la existencia de leyes en México que regulan la protección de los datos personales y los datos personales sensibles, es fundamental establecer estrategias para proteger los recursos tecnológicos utilizados en la prestación de los servicios de salud, así como implementar controles para prevenir el mal uso de los datos clínicos de los derechohabientes.

Ante esta situación el objeto de estudio de esta investigación se concentra en identificar si la gestión de riesgos es considerada por las instituciones de salud con mayor concentración de

derechohabientes en México (IMSS e ISSSTE en el Distrito Federal), como parte de sus estrategias actualmente implementadas para proteger los datos clínicos, así como saber si cuentan con una metodología para gestionar los riesgos de seguridad personalizada a sus necesidades en materia de seguridad de la información y cumplimiento. En caso de no contar con ésta, como resultado de la presente investigación se busca proporcionar una metodología para gestionar los riesgos de seguridad que pueda ser implementada para trabajar de forma conjunta con las estrategias actuales y que contribuya a mejorar la protección de la integridad, disponibilidad y confidencialidad de los datos clínicos, mediante un enfoque proactivo de respuesta y aprovechando al máximo los recursos tecnológico disponibles.

La gestión de riesgos al ser incorporada dentro de la estrategia de seguridad de la información de las instituciones de salud en México permitirá identificar los activos que son críticos para la operación, así como las amenazas y vulnerabilidades asociados a éstos y una vez cuantificados los riesgos establecer controles para mitigarlos hasta llevarlos a un estado aceptable, de tal forma que las instituciones logren un mayor control de sus activos, mejoren la seguridad de la información en los datos clínicos de los derechohabientes reduciendo de esta forma incidentes como la fuga de información, con la cual pueda lucrarse o causar un daño en la privacidad de los pacientes, además de operar en condiciones que les permita garantizar la calidad y rapidez del servicio y cumplir con los requerimientos legales en materia de protección de datos personales.

4.1.1 JUSTIFICACIÓN DE LA INVESTIGACIÓN

Los retos actuales en materia de seguridad de la información que enfrenta el sector salud en México al incorporar las TIC para la prestación de sus servicios, abre nuevas oportunidades para especialistas en seguridad informática, una de las motivaciones para enfocar el análisis a éste sector surge de la experiencia propia como usuario del servicio, identificando así áreas de oportunidad en ámbitos como la protección de la datos clínicos que son registrados en los expedientes, que en algunas clínicas son almacenados en grandes archiveros que carecen de mecanismos para controlar el acceso seguro y la integridad de la información, considerando que en algunas instituciones para dar seguimiento a una enfermedad que requiera un nivel más avanzado de atención, es necesario acudir a otra clínica u hospital donde se generará nuevamente un expediente en la mayoría de los casos físico, que vendrá acompañado del diagnóstico emitido por el médico de primer nivel y la justificación de la referencia, quedando de esta forma limitada la disponibilidad de la información sobre el histórico de los padecimientos del paciente y en algunos casos complicando para el médico de nivel de atención más avanzado, el diagnóstico oportuno de enfermedades que pueden atentar incluso contra la vida misma del derechohabiente, además de sistemas de cómputo que son desarrollados como apoyo para incorporar gradualmente el uso de un expediente clínico electrónico y que no son utilizados adecuadamente por el personal tanto administrativo como médico, ya sea por resistencia al cambio, falta de capacitación para su uso o como consecuencia de la clara división a nivel organizacional existente entre estos grupos. Ante estos escenarios se pueden identificar claramente grandes oportunidades para proponer, actuar y como profesional contribuir por

medio de conocimientos, tecnologías y personal calificado para mejorar la seguridad de la información en el Sector Salud en México.

Otra de las motivaciones para llevar a cabo esta investigación es ampliar el campo de acción de la gestión de riesgos, identificada como un elemento fundamental en una estrategia de seguridad de la información, al paso de los años se ha observado en otros sectores como el de TI o el financiero cómo gestionar los riesgos ayuda a cambiar a una forma de actuación proactiva ante eventos inesperados, de la misma forma se propone llevar este enfoque hacia el Sector Salud mediante una metodología que les permita identificar los riesgos potenciales, brindarles un tratamiento para mantener un control sobre los mismo y mejorar la gestión de la seguridad de la información de los datos clínicos lo cual sin duda será un gran beneficio en materia de cumplimiento con las leyes sobre datos personales.

4.2 PREGUNTAS DE INVESTIGACIÓN

En este apartado se presentan de forma precisa las preguntas que dan origen y resumen el tema de investigación, las respuestas a estas interrogantes se obtendrán como resultado de aplicar el instrumento en las instituciones de salud consideradas en el alcance del estudio.

4.2.1 PREGUNTA GENERAL

¿La gestión de riesgos de seguridad de la información forma parte de la estrategia para la protección de los datos clínicos en unidades de segundo y tercer nivel de atención del IMSS e ISSSTE del Distrito Federal?

4.2.2 PREGUNTAS ESPECÍFICAS

1. ¿Cuál es la relación existente entre la gestión de riesgos de seguridad de la información y la protección de los datos clínicos?

2. ¿El personal que hace uso de la información conoce las principales amenazas que atentan contra la seguridad de los datos clínicos?

3. ¿Cuáles son las medidas implementadas en las instituciones de salud para proteger los datos clínicos de los pacientes?

4. ¿Se cuenta con alguna metodología para la gestión de riesgos de seguridad de la información implementada en las instituciones de salud?

5. ¿El personal responsable de la protección de los datos clínicos conoce y cumple con las leyes relacionadas con la protección de datos personales y sensibles?

4.3 OBJETIVOS

4.3.1 OBJETIVO GENERAL

Diseñar una metodología para la gestión de riesgos de seguridad de la información que trabaje de forma coordinada con las estrategias actuales y fortalezca la protección de los datos clínicos en las unidades de segundo y tercer nivel de atención del IMSS e ISSSTE en el Distrito Federal.

4.3.2 OBJETIVOS ESPECÍFICOS

1. Establecer el estado del arte de la gestión de riesgos de seguridad de la información y los datos clínicos para identificar los indicadores que midan las variables de estudio.

2. Identificar el grado de conocimiento que posee el personal responsable de la protección de los datos clínicos, sobre las principales amenazas y vulnerabilidades que pueden afectar la seguridad de la información.

3. Analizar las medidas implementadas por las instituciones de salud para proteger los datos clínicos de los pacientes.

4. Determinar si se cuenta con una metodología para la gestión de riesgos operando en las instituciones de salud como parte de su estrategia de seguridad de la información.

5. Establecer si el personal responsable de la seguridad de la información de las instituciones de salud conoce y cumple con la legislación relacionada con datos personales y sensibles.

4.4 FORMULACIÓN DE HIPÓTESIS

La hipótesis que se propone se presenta a continuación:

> Las instituciones de salud de segundo y tercer nivel de atención del IMSS e ISSSTE del Distrito Federal que cuentan con una metodología para la gestión de riesgos de seguridad de la información mejoran la protección de los datos clínicos.

4.5 VARIABLES

Figura 4. 1 Tabla de variables presentes en la investigación.

VARIABLES PRESENTES EN LA INVESTIGACIÓN	
Variables demográficas	**Descripción institucional** • *Definición conceptual:* esta variable se refiere a la información demográfica del organismo de seguridad social sujeto de análisis, responsable de prestar el servicio de salud a los derechohabientes. • *Definición operacional:* para identificar esta variable se consideran los datos de los informes de las instituciones IMSS e ISSSTE, que serán corroborados durante la aplicación del instrumento en la unidad analizada.
Variable dependiente	**Seguridad de la información** • *Definición conceptual:* se define como la protección de la información y de los sistemas de información, de acciones no autorizadas como el acceso, el uso, la divulgación, la alteración y la modificación, con la finalidad de brindar servicios de seguridad como son la integridad, la confidencialidad y la disponibilidad *(NIST, 2011).* • *Definición operacional:* para medir esta variable serán considerados los once dominios del estándar *ISO 27002 Information technology – Security techniques – Code of practice for information security management*, para la elaboración de las preguntas del instrumento.
Variable independiente	**Gestión de riesgos de seguridad** • *Definición conceptual:* definido por el estándar *ISO 27002* como las actividades coordinadas para dirigir y controlar los asuntos relacionadas con el riesgo en la organización, incluyendo aspectos como la evaluación, el tratamiento, la aceptación y la comunicación para proteger la confidencialidad, la integridad y la disponibilidad de la información. • *Definición operacional:* la medición de esta variable se realizará considerando el grado de cumplimiento de las instituciones con las etapas para la gestión de riesgos incluidas en los estándares *ISO 31000 Risk management – Principles and guidelines* y el *ISO 27005 Information technology – Security techniques – Information Security Risk Management.*

Fuente: Elaboración propia.

A continuación se presentan las dimensiones de las variables demográfica, dependiente e independiente previamente definidas:

Figura 4. 2 Dimensiones de la variable demográfica.

Variable demográfica	Dimensiones
Descripción institucional	1. Institución. 2. Número de derechohabientes. 3. Especialidades atendidas. 4. Recursos tecnológicos. 5. Recursos humanos.

Fuente: Elaboración propia.

Figura 4. 3 Dimensiones de la variable dependiente.

Variable dependiente	Dimensiones
Gestión de riesgos de seguridad	1. Contexto de la institución. 2. Identificación de los riesgos. 3. Análisis de los riesgos. 4. Tratamiento del riesgo. 5. Comunicación del riesgo. 6. Monitoreo y revisión del riesgo.

Fuente: Elaboración propia.

Figura 4. 4 Dimensiones de la variable independiente.

Variable independiente	Dimensiones
Seguridad de la información	1. Política de seguridad. 2. Organización de la seguridad de la información. 3. Gestión de activos. 4. Control de accesos. 5. Cumplimiento. 6. Seguridad de recursos humanos. 7. Gestión de continuidad del negocio. 8. Mantenimiento, desarrollo y adquisición de sistemas de información. 9. Gestión de comunicaciones y operaciones. 10. Seguridad física y ambiental. 11. Gestión de incidentes de seguridad de la información.

Fuente: Elaboración propia.

4.6 METODOLOGÍA EMPLEADA

Para el desarrollo del marco teórico se llevó a cabo un metaanálisis sobre los temas de gestión de riesgos, seguridad de la información y datos clínicos, bajo un enfoque bibliométrico, para obtener un estudio informacional con el objetivo de identificar el estado del arte de los temas tratados, esta información puede ser consultada en el Anexo C Estudio informacional.

En la figura 4.5 Estructura de la investigación, se resumen los criterios considerados para el diseño de la investigación.

Figura 4. 5 Estructura de la investigación.

CRITERIO DE LA ESTRUCTURA DE LA INVESTIGACIÓN	
Objetivo general de la investigación	Diseñar una metodología para la gestión de riesgos de seguridad de la información que trabaje de forma coordinada con las estrategias actuales y fortalezca la protección de los datos clínicos en las unidades de segundo y tercer nivel de atención del IMSS e ISSSTE en el Distrito Federal.
Pregunta principal de la investigación	¿La gestión de riesgos de seguridad de la información forma parte de la estrategia para la protección de los datos clínicos en unidades de segundo y tercer nivel de atención del IMSS e ISSSTE del Distrito Federal?
Alcance del estudio	En la primera etapa es **descriptivo** ya que considera el estudio de la gestión de riesgos de seguridad de la información en los datos clínicos, para lo cual en el marco teórico y en el presente capítulo fueron definidos los conceptos, los componentes y las variables que intervienen en la investigación. Además es **exploratorio** hecho que fue identificado al observar que en la literatura revisada no se encontraron estudios que vinculen la gestión de riesgos con la seguridad de la información y los datos clínicos.
Hipótesis	Las instituciones de salud de segundo y tercer nivel de atención del IMSS e ISSSTE del Distrito Federal que cuentan con una metodología para la gestión de riesgos de seguridad de la información mejoran la protección de los datos clínicos.
Diseño de la investigación	El diseño de la investigación es **cuantitativo no experimental** dado que las variables no son manipuladas deliberadamente únicamente se observa la situación ya existente, en materia de seguridad de la información y los datos clínicos.
Dimensión temporal	Es **transversal** dado que la investigación se lleva a cabo en un momento determinado, donde el principal interés es el estudio de la

Figura 4. 6 Estructura de la investigación. (Continuación)

	situación en el presente, para lo cual fue construido el instrumento tomando como base los resultados obtenidos en el estado del arte.
Sujetos de estudio	El instrumento será aplicado en hospitales del IMSS e ISSSTE de segundo y tercer nivel de atención ubicados en el Distrito Federal.
Unidad de análisis	Corresponde a las instituciones de salud IMSS e ISSSTE que forman parte del sector de seguridad social del Sistema de Salud de México.
Universo	El universo está conformado por todas las instituciones responsables de prestar el servicio de salud en México.
Enfoque de colección de datos	Para la recolección de los datos se empleará un **cuestionario** que evaluará el comportamiento de las variables involucradas en el estudio. El instrumento será aplicado mediante una **entrevista estructurada**, a los directores o jefes de departamento encargados de las oficinas de tecnologías de la información o archivo clínico.
Ambiente de la investigación	El ambiente donde se llevará a cabo la investigación será en las instalaciones de los hospitales de segundo y tercer nivel de atención del IMSS e ISSSTE ubicados en el Distrito Federal.

Fuente: Elaboración propia con información de: Rivas, TLA. (2006). Como hacer una tesis de maestría. Editorial "Taller Abierto SCL" 2ª edición. México.

4.7 SELECCIÓN DE LA MUESTRA

La muestra se conforma por hospitales de especialidades y de alta especialidad, que corresponden a unidades de segundo y tercer nivel de atención, de las instituciones de seguridad social que cuentan con la mayor concentración de derechohabientes en el Distrito Federal, el Instituto Mexicano de Seguridad Social (IMSS) y el Instituto de Seguridad y Servicios Sociales de los Trabajadores del Estado (ISSSTE). Para la selección de los hospitales fueron considerados aquellos que brindan atención a enfermedades terminales, infectocontagiosas o que encabezan el listado de las principales causas de mortalidad, bajo éstos parámetros fue construido un directorio con datos recopilados en informes institucionales del IMSS[4] e ISSSTE[5], con el objeto de identificar los hospitales, una vez obtenida esta información mediante búsquedas en Google fueron recopilados los datos de contacto.

[4] IMSS: Informe al Ejecutivo Federal y al Congreso del Unión 2011-2012. http://www.imss.gob.mx/estadisticas/Documents/20112012/C11.pdf
[5] ISSSTE: Catálogo único de Unidades Médicas del ISSSTE, diciembre 2011. http://sgm.issste.gob.mx/medica/medica_documentacion/cat_unico_uni_med_dic2011.pdf

4.8 ELABORACIÓN DEL INSTRUMENTO

Para la construcción del instrumento se siguen los lineamientos de la metodología de Hernández Sampieri (2008) la cual se resume en la siguiente figura:

Figura 4. 7 Diagrama del proceso para construir un instrumento de medición.

Fuente: Elaboración propia con información de: Sampieri, Roberto, Collado, Carlos Fernández, & Lucio, Pilar Baptista. (2008). Metodología de la investigación. Editorial Mc Graw Hill, 1, 998.

4.8.1 REDEFINICIONES FUNDAMENTALES

a) *¿Qué va a ser medido?*

El instrumento permitirá identificar si las instituciones de salud analizadas consideran la gestión de riesgos de seguridad para la protección de los datos clínicos, además mostrará el estado actual de las instituciones, en materia de seguridad de la información, así como el cumplimiento con leyes y normas relacionado con la protección de datos personales y sensibles.

b) *¿Qué o quién va a ser medido?*

Directores o jefes de departamento encargados de las oficinas de tecnologías de información o archivo clínico.

c) *¿Cuándo?*

Primera y segunda semana del mes de octubre de 2013.

d) *¿Dónde?*

En los hospitales de segundo y tercer nivel incluidos en la muestra definida en el apartado 4.7 Selección de la muestra.

e) *¿El propósito al recolectar los datos?*

Identificar la necesidad de integrar una metodología para la gestión de riesgos de seguridad para fortalecer las estrategias actualmente implementadas en las instituciones de salud en materia de protección de datos clínicos.

f) *¿Las definiciones operacionales son?*

Se han definido previamente en el apartado 4.5 Variables del presente capítulo.

g) *¿Qué tipo de datos se van a obtener?*

La información recolectada serán datos estadísticos y descriptivos de las instituciones de salud.

4.8.2 REVISIÓN ENFOCADA DE LA LITERATURA

El desarrollo del marco teórico en los capítulos anteriores ha permitido definir las variables involucradas en la investigación, considerando para su operacionalización los indicadores teóricos identificados durante la revisión de la literatura, para el caso de la variable gestión de riesgos se han considerado los estándares *ISO 31000 Risk management – Principles and guidelines* y el *ISO 27005 Information technology – Security techniques – Information Security Risk Management*, para la variable seguridad de la información se ha optado por utilizar los once dominios del estándar *ISO 27002 Information technology – Security techniques – Code of practice for information security management*.

4.8.3 IDENTIFICACIÓN DEL DOMINIO DE LAS VARIABLES A MEDIR Y SUS INDICADORES

Figura 4. 8 Matriz de operacionalización de las variables presentes en la investigación.

CRITERIO DE LA ESTRUCTURA DE LA INVESTIGACIÓN

Variable	Dimensión	Indicador	Ítems y nivel de edición	Amplitud de la escala	Fuente
Descripción institucional	Institución	Nombre de la institución de seguridad social	ins1.Seleccione la institución de seguridad social a la que pertenece *Nominal*	- IMSS - ISSSTE	- Consulta informes IMSS-ISSSTE
	Número de derechohabientes	Total de derechohabientes de la institución	der1. Indique el número aproximado de derechohabientes que reciben el servicio de salud en la institución de seguridad social a la que pertenece *Razón*	Número entero	- Instrumento - Entrevista estructurada
	Especialidades atendidas	Nombre especialidades atendidas	esp1. Del siguiente listado seleccione las especialidades o subespecialidades que son atendidas en la institución donde labora, en caso de dar atención a otras especifique cuáles son: *Nominal*	- Medicina interna - Oncología Cirugía - Cardiología Ginecobstetricia - Ginecología Pediatría - Geriatría Dermatología - Traumatología y ortopedia Neurología - Dermatología Neumología - Hematología Otras:	- Instrumento - Entrevista estructurada

Figura 4. 7 Matriz de operacionalización de las variables presentes en la investigación. (Continuación)

Variable	Dimensión	Indicador	Ítems y nivel de edición	Amplitud de la escala	Fuente
Descripción institucional	Especialidades atendidas	Número de especialidades atendidas por la institución	esp2. Del siguiente listado seleccione las especialidades o subespecialidades atendidas en la institución donde labora, en caso de dar atención a otras especifique cuáles son: *Razón*	Número entero	- Instrumento - Entrevista estructurada
	Recursos tecnológicos	Número de computadoras	tec1. Número aproximado de computadoras disponibles para la prestación del servicio de salud en las diferentes especialidades. *Intervalo*	- 0-50 - 51- 100 - 101-150 - 151-200 - más de 200	- Instrumento - Entrevista estructurada
		Número de computadoras portátiles	tec2.Número aproximado de computadoras portátiles disponibles para la prestación del servicio de salud en las diferentes especialidades. *Intervalo*	- 0-50 - 51- 100 - 101-150 - 151-200 - más de 200	- Instrumento - Entrevista estructurada
		Número de impresoras	tec3.Número aproximado de impresoras disponibles para la prestación del servicio de salud en las diferentes especialidades. *Intervalo*	- 0-10 - 11- 20 - 21- 30 - 31- 40 - más de 40	- Instrumento - Entrevista estructurada
		Conexión a internet	tec4. La institución cuenta con infraestructura que permita al personal interno el uso de Internet *Nominal*	- SI - NO	- Instrumento - Entrevista estructurada
	Recursos humanos	Total de personas que laboran en la institución	rh1. Indique el número aproximado de personas que laboran en la institución. *Razón*	Número entero	- Instrumento - Entrevista estructurada

Figura 4. 7 Matriz de operacionalización de las variables presentes en la investigación. (Continuación)

Variable	Dimensión	Indicador	Ítems y nivel de edición	Amplitud de la escala	Fuente
Descripción institucional	Recursos humanos	Porcentaje de recursos responsables de las TIC	rh2. ¿Cuál es el número de personas responsables de las tecnologías de información y comunicaciones (TIC) de la institución? *Razón*	Número entero	- Instrumento - Entrevista estructurada
		Porcentaje de recursos responsables de la seguridad de la información	rh3. ¿Cuál es el número de personas de TIC, destinado para temas relacionados con la seguridad de la información? *Razón*	Número entero	- Instrumento - Entrevista estructurada
Gestión de riesgos de seguridad	Contexto de la institución	Conocimiento sobre la documentación de los procesos de la institución	con1. ¿Se tienen identificados y documentados los procesos utilizados en la operación de la institución? *Nominal*	- SI - NO	- Instrumento - Entrevista estructurada
		Listado de activos críticos	con2. 12.¿Se cuenta con algún listado de recursos críticos en materia de TIC (Tecnologías de Información y Comunicaciones), que sean fundamentales para la operación diaria? *Nominal*	- SI - NO	- Instrumento - Entrevista estructurada
		Existencia de una metodología para la evaluación de riesgos	con3. ¿Existe alguna metodología para evaluar los riesgos de seguridad de la información? *Nominal*	- SI - NO	- Instrumento - Entrevista estructurada
	Identificación de los riesgos	Nivel de conocimiento sobre amenazas	ide1. Del siguiente listado marque las principales amenazas (aquello que pretende causar algún daño) que usted considere afectan la confidencialidad, la integridad y la disponibilidad de los datos clínicos de la institución a la que pertenece: *Nominal*	- Suplantación por empleados - Suplantación por proveedores de servicio - Suplantación por externos	- Instrumento - Entrevista estructurada

Figura 4. 7 Matriz de operacionalización de las variables presentes en la investigación. (Continuación)

Variable	Dimensión	Indicador	Ítems y nivel de edición	Amplitud de la escala	Fuente
Gestión de riesgos de seguridad	Identificación de los riesgos	Nivel de conocimiento sobre amenazas	ide1. Del siguiente listado marque las principales amenazas (aquello que pretende causar algún daño) que usted considere afectan la confidencialidad, la integridad y la disponibilidad de los datos clínicos de la institución a la que pertenece: *Nominal*	- Uso no autorizado de programas y aplicaciones de información de salud - Introducción de software dañino o perjudicial - Mal uso de los recursos de los sistemas - Infiltración de las comunicaciones - Intercepción de las comunicaciones - Desconocimiento de actividades por parte de los empleados - Fallas en las conexiones o servicios de TI - Incorporación de virus, programas maliciosos. - Envío erróneo o accidental de información - Fallas generadas por desastres naturales Fallas en los sistemas de información de salud - Uso indebido de los recursos de TI.	- Instrumento - Entrevista estructurada

Figura 4. 7 Matriz de operacionalización de las variables presentes en la investigación. (Continuación)

Variable	Dimensión	Indicador	Ítems y nivel de edición	Amplitud de la escala	Fuente
Gestión de riesgos de seguridad	Identificación de los riesgos			- Errores en el mantenimiento de los equipos de TI. - Errores de los usuarios. - Escases de personal.	- Instrumento - Entrevista estructurada
		Existencia de un procedimiento para la identificación de amenazas y vulnerabilidades	ide2. ¿Existe algún procedimiento sobre cómo se identifican las amenazas y debilidades en materia de seguridad de la información? *Nominal*	- SI - NO	- Instrumento - Entrevista estructurada
	Análisis de los riesgos	Enfoque empleado para la evaluación del riesgo	ana1. ¿Cuál es el enfoque empleado para la evaluación de riesgos en materia de seguridad de la información. *Nominal*	- Cualitativo (Alto-Medio-Bajo) - Cuantitativo (Numérico)	- Instrumento - Entrevista estructurada
		Cuentan con matrices de probabilidad de ocurrencia e impacto	ana2. Para la valoración de los riesgos de seguridad, ¿Cuentan con matrices de probabilidad de ocurrencia e impacto? *Nominal*	- SI - NO	- Instrumento - Entrevista estructurada
	Tratamiento del riesgo	Nivel de conocimiento sobre las opciones para tratar el riesgo	tra1. ¿Cuáles de las siguientes opciones para tratar el riesgo conoce? *Nominal*	- Reducción - Aceptación - Evitación - Transferencia	- Instrumento - Entrevista estructurada

Figura 4. 7 Matriz de operacionalización de las variables presentes en la investigación. (Continuación)

Variable	Dimensión	Indicador	Ítems y nivel de edición	Amplitud de la escala	Fuente
Gestión de riesgos de seguridad	Comunicación del riesgo	Existencia de campañas de concientización	com1. ¿Se llevan a cabo campañas de concientización para el personal sobre los riesgos de seguridad de la información y sobre las medidas implementadas para su tratamiento? *Nominal*	- SI - NO	- Instrumento - Entrevista estructurada
	Monitoreo y revisión del riesgo	Cada cuanto tiempo son revisados los controles implementados	mon1. Cada cuánto tiempo son revisadas las medidas implementados para dar tratamiento a los riesgos de seguridad de la información identificados? *Nominal*	- Cada 6 meses - Cada año - Cada dos años - Más de dos años - No se revisan	- Instrumento - Entrevista estructurada
Seguridad de la información	Política de seguridad	Existencia de un manual de políticas de seguridad informática, actualizado y aprobado por la dirección	pol1. ¿Cuenta la institución con un manual de políticas de seguridad informática? *Nominal*	- SI - NO -	- Instrumento - Entrevista estructurada
			pol2. ¿El manual de políticas de seguridad informática se encuentra aprobado por el director de la institución? *Nominal*	- SI - NO	- Instrumento - Entrevista estructurada
		Campañas de difusión para las políticas de seguridad informática	pol3. ¿Se llevan a cabo de forma periódica campañas para la difusión de las políticas de seguridad informática? *Nominal*	- SI - NO	- Instrumento - Entrevista estructurada
	Organización de la seguridad de la información	Existencia de un comité de seguridad de la información	org1. ¿La institución cuenta con algún comité para abordar temas relacionados con la seguridad de la información? *Nominal*	- SI - NO	- Instrumento - Entrevista estructurada

Figura 4. 7 Matriz de operacionalización de las variables presentes en la investigación. (Continuación)

Variable	Dimensión	Indicador	Ítems y nivel de edición	Amplitud de la escala	Fuente
Seguridad de la información	Organización de la seguridad de la información	Existencia de procedimientos especiales personal externo	org2. ¿Se cuentan con procedimientos especiales en materia de seguridad de la información para personal externo (proveedores)? *Nominal*	- SI - NO	- Instrumento - Entrevista estructurada
	Gestión de activos	Se cuenta con un inventario de activos y sus responsables	ges1.Seleccione los inventarios de recursos con los que cuente la institución *Nominal*	- Información - Software - Recursos físicos - Servicios - Personal - Intangibles	- Instrumento - Entrevista estructurada
		Existencia de una clasificación de información.	ges2. ¿La institución cuenta con una clasificación para los diferentes tipos de información? *Nominal*	- SI - NO	- Instrumento - Entrevista estructurada
		Uso de distintivos para manejar o etiquetar información con base en su clasificación	gest3. ¿Se cuentan con distintivos para manejar o etiquetar la información considerando su clasificación? *Nominal*	- SI - NO	- Instrumento - Entrevista estructurada
	Control de accesos	Uso de una bitácora para controlar los accesos	acc1. ¿Se cuenta con algún registro para controlar los accesos a los sistemas de información? *Nominal*	- SI - NO	- Instrumento - Entrevista estructurada
		Control de privilegios	acc2. ¿Son considerados los roles al otorgar los privilegios necesarios para el acceso a los sistemas o información? *Nominal*	- SI - NO	- Instrumento - Entrevista estructurada

Figura 4. 7 Matriz de operacionalización de las variables presentes en la investigación. (Continuación)

Variable	Dimensión	Indicador	Ítems y nivel de edición	Amplitud de la escala	Fuente
Seguridad de la información	Control de accesos	Uso de contraseñas	acc3. ¿El personal cuenta con contraseñas para ingresar a los equipos de cómputo y/o sistemas de información? *Nominal*	- SI - NO	- Instrumento - Entrevista estructurada
		Controles de acceso a la red	acc4. ¿Se cuentan con mecanismos para controlar el acceso a la red local y/o Internet? *Nominal*	- SI - NO	- Instrumento - Entrevista estructurada
		Mecanismos control de dispositivos móviles	acc5. ¿Se cuentan con mecanismos para controlar el acceso a la red local y/o Internet de los dispositivos móviles (celulares, smartphones, tablets)? *Nominal*	- SI - NO	- Instrumento - Entrevista estructurada
	Cumplimiento	Conocimiento y cumplimiento de normas relacionadas con la protección de datos clínicos	cum1. Del siguiente listado seleccione las normas, leyes o estándares relacionados con la seguridad de la información que conoce y/o que estén implementados en la institución: *Nominal*	- Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental - Ley General de Salud - Reglamento de la Ley General de Salud en Materia de Prestación de Servicios de Atención Médica - NOM-040-SSA2-2004. - NOM-004-SSA3-2012	- Instrumento - Entrevista estructurada

Figura 4.7 Matriz de operacionalización de las variables presentes en la investigación. (Continuación)

Variable	Dimensión	Indicador	Ítems y nivel de edición	Amplitud de la escala	Fuente
Seguridad de la información	Cumplimiento	Conocimiento y cumplimiento de normas relacionadas con la protección de datos clínicos	cum1. Del siguiente listado seleccione las normas, leyes o estándares relacionados con la seguridad de la información que conoce y/o que estén implementados en la institución: *Nominal*	- NOM-024-SSA3-2010 - ISO 27001 - ISO 27002 - ISO 27799 - ISO 27005 - ITIL	- Instrumento - Entrevista estructurada
	Seguridad de recursos humanos	Existencia de roles y responsabilidades claramente definidos	srh1. ¿Se cuentan con roles y responsabilidades del personal de la institución claramente definidos? *Nominal*	- SI - NO	- Instrumento - Entrevista estructurada
		Existencia de programas de capacitación para uso de sistemas de información o clasificación de la misma	srh2. ¿Se realizan de forma periódica programas de capacitación para el personal sobre el uso de los sistemas o sobre la clasificación de información? *Nominal*	- SI - NO	- Instrumento - Entrevista estructurada
	Gestión de continuidad del negocio	Cuentan con planes para la continuidad del negocio	gcn1. ¿Se cuentan con planes para la continuidad del negocio (Plan de Continuidad del Negocio-PCN, Plan de Recuperación de Desastres-PRD)? *Nominal*	- SI - NO	- Instrumento - Entrevista estructurada
		Pruebas a los planes de continuidad del negocio	gcn2. ¿Se realizan pruebas a los planes para la continuidad del negocio (PCN-PRD)? *Nominal*	- SI - NO	- Instrumento - Entrevista estructurada
	Mantenimiento, desarrollo y adquisición de sistemas de información	Consideración de mecanismos de seguridad de la información para el desarrollo de sistemas de información	sis1. Seleccione los mecanismos para la seguridad de la información que son considerados al desarrollar sistemas de información (Puede seleccionar más de una opción): *Nominal*	- Validaciones de datos (entrada-salida) - Pruebas - Cifrado - Control de vulnerabilidades - Control de versiones	- Instrumento - Entrevista estructurada

Figura 4. 7 Matriz de operacionalización de las variables presentes en la investigación. (Continuación)

Variable	Dimensión	Indicador	Ítems y nivel de edición	Amplitud de la escala	Fuente
Seguridad de la información	Gestión de comunicaciones y operaciones	Cuentan con mecanismos para protección contra código malicioso	gco1. ¿Se cuentan con mecanismos para protección contra programas malicioso (virus, gusanos)? *Nominal*	- SI - NO	- Instrumento - Entrevista estructurada
		Se llevan a cabo respaldos de la información	gco2. ¿Se llevan a cabo respaldo de la información de equipos de cómputo y de los sistemas de información? *Nominal*	- SI - NO	- Instrumento - Entrevista estructurada
	Seguridad física y ambiental	Existencia de controles físicos de entrada para protección de información	sfa1.Seleccione los mecanismos físicos utilizados por la institución para protección de la seguridad de la información (Puede seleccionar más de una opción): *Nominal*	- Puertas en archiveros - Cámaras de video vigilancia - Escáner corporal - Sensores - Controles biométricos en zonas restringidas - Bitácoras de registro - Custodio (policía)	- Instrumento - Entrevista estructurada
		Se cuentan con servicios de apoyo contra fallas de energía	sfa2. ¿Se cuentan con servicios de apoyo contra fallas eléctricas u otras interrupciones? *Nominal*	- SI - NO	- Instrumento - Entrevista estructurada
		Existencia de un programa de mantenimiento	sfa3. ¿Existe algún programa de mantenimiento para los equipos de TI de la institución? *Nominal*	- SI - NO	- Instrumento - Entrevista estructurada

Figura 4.7 Matriz de operacionalización de las variables presentes en la investigación. (Continuación)

Variable	Dimensión	Indicador	Ítems y nivel de edición	Amplitud de la escala	Fuente
Seguridad de la información	Seguridad física y ambiental	Existencia de medidas para evitar fuga de información o salida de equipo sin autorización.	sfa4. ¿Existen medidas para evitar la fuga de información, o salida de equipos sin autorización? *Nominal*	- SI - NO	- Instrumento - Entrevista estructurada
	Gestión de incidentes de seguridad de la información	Existencia de un procedimiento para el reporte de eventos de seguridad de la información	gis1. ¿Existe algún procedimiento para el reporte de incidentes de seguridad de la información? *Nominal*	- SI - NO	- Instrumento - Entrevista estructurada
		Se cuenta con una base de conocimiento de los incidentes	gis2. ¿Existe alguna base de conocimiento sobre los incidentes de seguridad de la información reportados y atendidos? *Nominal*	- SI - NO	- Instrumento - Entrevista estructurada

Fuente: Elaboración propia.

4.8.4 TOMA DE DECISIONES CLAVE

Como resultado del marco teórico se han seleccionado los estándares ISO 31000, ISO 27005 e ISO 27002 para definir las dimensiones, indicadores e ítems de la matriz de las variables involucradas en la investigación (véase figura 4.7 Matriz de operacionalización de las variables presentes en la investigación), las cuáles serán la base para la construcción del instrumento de medición.

4.8.5 CONSTRUCCIÓN DEL INSTRUMENTO

Para el desarrollo de los reactivos se tomó como base la matriz de la figura 4.7 Matriz de operacionalización de las variables presentes en la investigación, en la mayoría de las preguntas se considera una escala nominal. A continuación se presenta el instrumento utilizado en la investigación, especificando entre paréntesis para cada una de las preguntas, las dimensiones de cada una de las variables, así como el ítem con la codificación establecida en la matriz de operacionalización.

PREGUNTAS INSTRUMENTO

REACTIVOS VARIABLE DESCRIPCIÓN INSTITUCIONAL

1. Seleccione la institución de seguridad social a la que pertenece: **(Institución, ins1)**
   ☐IMSS ☐ISSSTE

2. Indique el número aproximado de derechohabientes que reciben el servicio de salud en la institución de seguridad social a la que pertenece: **(Número de derechohabientes, der1)**
   _____

3. Del siguiente listado seleccione las especialidades o subespecialidades que son atendidas en la institución donde labora, en caso de dar atención a otras especifique cuáles son: **(Especialidades atendidas, esp1 esp2)**

   ☐Medicina interna
   ☐Cirugía
   ☐Ginecobstetricia
   ☐Pediatría
   ☐Dermatología
   ☐Neurología
   ☐Neumología
   ☐Otras: _____
   ☐Oncología
   ☐Cardiología
   ☐Ginecología
   ☐Geriatría
   ☐Traumatología y ortopedia
   ☐Dermatología
   ☐Hematología

4. Número aproximado de computadoras de escritorio disponibles para la prestación del servicio de salud en las diferentes especialidades. **(Recursos tecnológicos, tec1)**
   ☐0-50 ☐51- 100 ☐101-150 ☐151-200 ☐más de 200

5. Número aproximado de computadoras portátiles disponibles para la prestación del servicio de salud en las diferentes especialidades. **(Recursos tecnológicos, tec2)**
   ☐0-50 ☐51- 100 ☐101-150 ☐151-200 ☐más de 200

6. Número aproximado de impresoras disponibles para la prestación del servicio de salud en las diferentes especialidades. **(Recursos tecnológicos, tec3)**
☐0-10 ☐11- 20 ☐21-30 ☐31-40 ☐más de 40

7. La institución cuenta con infraestructura que permita al personal interno el uso de Internet. **(Recursos tecnológicos, tec4)**
☐SI ☐NO

8. Indique el número aproximado de personas que laboran en la institución: **(Recursos humanos, rh1)**
_____

9. ¿Cuál es el número de personas responsables de las tecnologías de información y comunicaciones (TIC) de la institución? **(Recursos humanos, rh2)**
_____

10. ¿Cuál es el número de personas de TIC, destinado para temas relacionados con la seguridad de la información? **(Recursos humanos, rh3)**
_____

REACTIVOS VARIABLE GESTIÓN DE RIESGOS DE SEGURIDAD

11. ¿Se tienen identificados y documentados los procesos utilizados en la operación de la institución? **(Contexto de la institución, con1)**
☐SI ☐NO

12. ¿Se cuenta con algún listado de recursos críticos en materia de TIC (Tecnologías de Información y Comunicaciones), que sean fundamentales para la operación diaria? **(Contexto de la institución, con2)**
☐SI ☐NO

13. ¿Existe alguna metodología evaluar los riesgos de seguridad de la información? **(Contexto de la institución, con3)**
☐SI ☐NO

14. Del siguiente listado marque las principales amenazas (aquello que pretende causar algún daño) que usted considere afectan la confidencialidad, la integridad y la disponibilidad de los datos clínicos de la institución a la que pertenece: **(Identificación de los riesgos, ide1)**

☐Suplantación por empleados	☐Desconocimiento de actividades por parte de los empleados	☐Errores de los usuarios.
☐Suplantación por proveedores de servicio	☐Fallas en las conexiones o servicios de TI	☐Escases de personal.
☐Suplantación por externos.	☐Incorporación de virus, programas maliciosos.	☐Acceso a información privilegiada por personal no autorizado
☐Uso no autorizado de programas y aplicaciones de información de salud	☐Envío erróneo o accidental de información	☐Daños intencionales por personal interno.
☐Introducción de software dañino o perjudicial	☐Fallas generadas por desastres naturales	☐Daños intencionales por personal externo.

☐Mal uso de los recursos de los sistemas	☐Fallas en los sistemas de información de salud	☐Terrorismo
☐Infiltración de las comunicaciones	☐Uso indebido de los recursos de TI.	☐Uso de programas sin licencia para su uso
☐Intercepción de las comunicaciones	☐Errores en el mantenimiento de los equipos de TI.	☐Desconocimiento de leyes en materia de seguridad de la información

15. ¿Existe algún procedimiento sobre cómo se identifican las amenazas y debilidades en materia de seguridad de la información? **(Identificación de los riesgos, ide2)**
    ☐SI ☐NO

16. ¿Cuál es el enfoque empleado para la evaluación de riesgos en materia de seguridad de la información? **(Análisis de los riesgos, ana1)**
    ☐Cualitativo (Alto-Medio-Bajo) ☐Cuantitativo (Numérico)

17. Para la valoración de los riesgos de seguridad, ¿Cuentan con matrices de probabilidad de ocurrencia e impacto? **(Análisis de los riesgos, ana2)**
    ☐SI ☐NO

18. ¿Cuáles de las siguientes opciones para tratar el riesgo conoce? *Puede seleccionar más de una opción.* **(Tratamiento del riesgo, tra1)**
    ☐Reducción ☐Aceptación ☐Evitación ☐Transferencia

19. ¿Se llevan a cabo campañas de concientización para el personal sobre los riesgos de seguridad de la información y sobre las medidas implementadas para su tratamiento? **(Comunicación del riesgo, com1)**
    ☐SI ☐NO

20. ¿Cada cuánto tiempo son revisadas las medidas implementados para dar tratamiento a los riesgos de seguridad de la información identificados? **(Monitoreo y revisión del riesgo, mon1)**
    ☐Cada 6 meses ☐Cada año ☐Cada dos años ☐Más de dos años ☐No se revisan

REACTIVOS VARIABLE SEGURIDAD DE LA INFORMACIÓN

21. ¿Cuenta la institución con un manual de políticas de seguridad informática? **(Política de seguridad, pol1)**
    ☐SI ☐NO

22. ¿El manual de políticas de seguridad informática se encuentra aprobado por el director de la institución? **(Política de seguridad, pol2)**
    ☐SI ☐NO

23. ¿Se llevan a cabo de forma periódica campañas para la difusión de las políticas de seguridad informática? **(Política de seguridad, pol3)**
    ☐SI ☐NO

24. ¿La institución cuenta con algún comité para abordar temas relacionados con la seguridad de la información? **(Organización de la seguridad de la información, org1)**
    ☐SI ☐NO

25. ¿Se cuentan con procedimientos especiales en materia de seguridad de la información para personal externo (proveedores)? **(Organización de la seguridad de la información, org2)**
☐SI ☐NO

26. Seleccione los inventarios de recursos con los que cuente la institución (*Puede seleccionar más de una opción)*: **(Gestión de activos, ges1)**
☐Información ☐Recursos físicos ☐Personal
☐Software ☐Servicios ☐Intangibles

27. ¿La institución cuenta con una clasificación para los diferentes tipos de información? **(Gestión de activos, ges2)**
☐SI ☐NO

28. ¿Se cuentan con distintivos para manejar o etiquetar la información considerando su clasificación? **(Gestión de activos, ges3)**
☐SI ☐NO

29. ¿Se cuenta con algún registro para controlar los accesos a los sistemas de información? **(Control de accesos, acc1)**
☐SI ☐NO

30. ¿Son considerados los roles al otorgar los privilegios necesarios para el acceso a los sistemas o información? **(Control de accesos, acc2)**
☐SI ☐NO

31. ¿El personal cuenta con contraseñas para ingresar a los equipos de cómputo y/o sistemas de información? **(Control de accesos, acc3)**
☐SI ☐NO

32. ¿Se cuentan con mecanismos para controlar el acceso a la red local y/o Internet? **(Control de accesos, acc4)**
☐SI ☐NO

33. ¿Se cuentan con mecanismos para controlar el acceso a la red local y/o Internet de los dispositivos móviles (smartphones, tablets)? **(Control de accesos, acc5)**
☐SI ☐NO

34. Del siguiente listado seleccione las normas, leyes o estándares relacionados con la seguridad de la información que conoce y/o que estén implementados en la institución: **(Cumplimiento, cum1)**

Norma-Estándar-Ley	Conoce	Implementada/o
Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental	☐	☐
Ley General de Salud	☐	☐
Reglamento de la Ley General de Salud en Materia de Prestación de Servicios de Atención Médica	☐	☐
NOM-040-SSA2-2004, Norma Oficial de Información en Salud	☐	☐
NOM-004-SSA3-2012, Norma Oficial Del expediente clínico	☐	☐
NOM-024-SSA3-2010 Norma sobre los productos de Sistemas de Expediente Clínico Electrónico	☐	☐
ISO 27001	☐	☐

ISO 27002	☐	☐
ISO 27799	☐	☐
ISO 27005	☐	☐
ITIL	☐	☐

35. ¿Se cuentan con roles y responsabilidades del personal de la institución claramente definidos? **(Seguridad de recursos, srh1)**
☐SI ☐NO

36. ¿Se realizan de forma periódica programas de capacitación para el personal sobre el uso de los sistemas o sobre la clasificación de información? **(Seguridad de recursos, srh2)**
☐SI ☐NO

37. ¿Se cuentan con planes para la continuidad del negocio (Plan de Continuidad del Negocio-PCN, Plan de Recuperación de Desastres-PRD)? **(Gestión de continuidad del negocio, gcn1)**
☐SI ☐NO

38. ¿Se realizan pruebas a los planes para la continuidad del negocio (PCN-PRD)? **(Gestión de continuidad del negocio, gcn2)**
☐SI ☐NO

39. Seleccione los mecanismos para la seguridad de la información que son considerados al desarrollar sistemas de información (*Puede seleccionar más de una opción)*: **(Mantenimiento, desarrollo y adquisición de sistemas de información, sis1)**
☐Validaciones de datos (entrada-salida)
☐Pruebas
☐Cifrado
☐Control de vulnerabilidades
☐Control de versiones

40. ¿Se cuentan con mecanismos para protección contra programas malicioso (virus, gusanos)? **(Gestión de comunicaciones y operaciones, gco1)**
☐SI ☐NO

41. ¿Se llevan a cabo respaldo de la información de equipos de cómputo y de los sistemas de información? **(Gestión de comunicaciones y operaciones, gco2)**
☐SI ☐NO

42. Seleccione los mecanismos físicos utilizados por la institución para protección de la seguridad de la información *(Puede seleccionar más de una opción)*: **(Seguridad física y ambiental, sfa1)**

☐Puertas en archiveros
☐Cámaras de video vigilancia
☐Escáner corporal
☐Sensores
☐ Controles biométricos en zonas restringidas
☐Bitácoras de registro
☐Custodio (policía)

43. ¿Se cuentan con servicios de apoyo contra fallas eléctricas u otras interrupciones? **(Seguridad física y ambiental, sfa2)**
☐SI ☐NO

44. ¿Existe algún programa de mantenimiento para los equipos de TI de la institución? **(Seguridad física y ambiental, sfa3)**
☐SI ☐NO

45. ¿Existen medidas para evitar la fuga de información, o salida de equipos sin autorización? **(Seguridad física y ambiental, sfa4)**
☐SI ☐NO

46. ¿Existe algún procedimiento para el reporte de incidentes de seguridad de la información? **(Gestión de incidentes de seguridad de la información, gis1)**
☐SI ☐NO

47. ¿Existe alguna base de conocimiento sobre los incidentes de seguridad de la información reportados y atendidos? **(Gestión de incidentes de seguridad de la información, gis2)**
☐SI ☐NO

4.8.6 PRUEBA PILOTO

Para la prueba piloto se aplicó el instrumento en hospitales del segundo y tercer nivel de atención en el Distrito Federal, los cuáles fueron seleccionados por conveniencia y por las facilidades otorgadas para llevar a cabo el cuestionario, donde el objetivo principal fue obtener los comentarios y sugerencias acerca de los reactivos, para identificar las áreas de oportunidad en la redacción de las preguntas y sus opciones.

4.8.7 ELABORACIÓN DE LA VERSIÓN FINAL DEL INSTRUMENTO Y SU PROCEDIMIENTO DE APLICACIÓN

Al aplicar la prueba piloto se identificaron en las opciones de algunos reactivos rangos que eran superiores a los requeridos en la realidad, además se realizaron modificaciones en palabras que fueron consideradas por las personas que contestaron el cuestionario como tecnicismos que complicaban la comprensión de la pregunta.

Para aplicar el cuestionario fue necesario solicitar el apoyo del Programa de Posgrado en Ciencias de la Administración de la UNAM, para obtener un oficio que sustentará el objetivo de la investigación y enfatizará sobre los fines académicos, la confidencialidad de los resultados obtenidos y el compromiso de compartir con las instituciones participantes los hallazgos al concluir la investigación (véase Anexo B Oficio de presentación del estudio) .

Una vez que se contó con el oficio, se concertaron reuniones con cada uno de los directores de las instituciones sujetas de análisis, con la finalidad de darles a conocer los objetivos de la

investigación y a su vez exhortarlos a participar en ella, de forma que se obtuviera su consentimiento para llevar a cabo la aplicación del instrumento.

4.8.8 ENTRENAMIENTO DEL PERSONAL QUE VA ADMINISTRAR EL INSTRUMENTO

La administración del instrumento fue realizada por cuenta propia, considerando que el tamaño de la muestra era reducido, razón por la cual no fue necesaria la colaboración de personal adicional para la aplicación del cuestionario.

4.8.9 AUTORIZACIÓN PARA APLICAR EL INSTRUMENTO

La autorización para llevar a cabo el cuestionario fue obtenida a través de los directores de las instituciones sujetas de análisis, logrando con ello establecer el contacto directo, con las personas que darían respuesta a las preguntas del instrumento.

4.8.10 ADMINISTRACIÓN DEL INSTRUMENTO

El cuestionario fue aplicado a los directores o jefes de departamento, encargados de las oficinas de tecnologías de información o personal de archivo clínico, el cual fue aplicado bajo un enfoque de entrevista estructurada, que permitió resolver las dudas o inquietudes que pudieran surgir durante la aplicación.

4.9 CONFIABILIDAD Y VALIDEZ

La confiabilidad de un instrumento de medición se refiere al grado en que su aplicación repetida al mismo individuo u objeto produce resultados iguales *(Sampieri et al., 2008)*. Los enfoques para evaluar la confiabilidad incluyen los métodos test-retest, formas alternativas y consistencia interna, una breve descripción de éstos se presenta a continuación *(Malhotra et al., 2004)*:

a) *Confiabilidad test-retest:* consiste en un método en el cual se aplica a los encuestados conjuntos idénticos de reactivos en dos momentos diferentes en condiciones tan equivalentes como sea posible.

b) *Confiabilidad de formas alternativas:* enfoque que requiere la construcción de dos formas equivalentes de la escala y que los mismos encuestados sean medidos en dos momentos diferentes.

c) *Confiabilidad de consistencia interna:* método que evalúa la consistencia interna del conjunto de reactivos cuando varios reactivos son sumados para obtener una clasificación total de la escala.

Para la presente investigación no será posible utilizar técnicas de confiabilidad, dado que el instrumento de la investigación describe y explora solo hechos.

Por otro lado la validez se define como el grado en que un instrumento realmente mide la variable que pretende medir, algunos tipos de evidencias que pueden ser utilizadas para determinar la validez de un instrumento son *(Sampieri et al., 2008)*:

a) *Validez de contenido (evidencia relacionada con el contenido):* se refiere al grado en que el instrumento refleja un dominio específico de contenido de lo que se mide.

b) *Validez de criterio (evidencia relacionada con el criterio):* se establece al validar un instrumento de medición al compararlo con algún criterio externo que pretende medir lo mismo.

c) *Validez de constructo (evidencia relacionada con el constructo):* este tipo de evidencia debe explicar el modelo teórico empírico que subyace a la variable de interés.

El tipo de validez en la cual se sustenta el instrumento desarrollado para la investigación es la validez de contenido ya que los reactivos fueron desarrollados a partir de la literatura del estado del arte que fue revisada y que forma parte del marco teórico, permitiendo así la integración de la matriz de operacionalización que sustenta la validez de contenido de la investigación.

En el siguiente capítulo se presentará a detalle el análisis de los resultados obtenidos al aplicar el instrumento en las unidades de análisis seleccionadas, a partir de esta información se estudiará el comportamiento de las variables, se dará respuesta a las preguntas y objetivos de investigación, se comprobará la hipótesis y se determinarán las directrices, que servirán de base para el diseño de la metodología de gestión de riesgos de seguridad que se propondrá en el capítulo 6 y que fungirá como una herramienta auxiliar para dar respuesta a las áreas de oportunidad en materia de seguridad de la información previamente identificadas.

CAPÍTULO 5

ANÁLISIS DE LOS RESULTADOS

Una vez aplicado el instrumento en las instituciones de salud, los resultados serán analizados en el presente capítulo, de tal forma que se identifique el comportamiento de las variables de estudio, con el objetivo de dar respuesta a las preguntas de investigación establecidas en el capítulo 4, comprobar la hipótesis y de forma adicional analizar las áreas de oportunidad en materia de seguridad de la información para la protección de los datos clínicos en las instituciones de salud, que serán la base para el desarrollo de la metodología de gestión de riesgos de seguridad de la información, elaborada como una propuesta que ayude a las instituciones de salud a mejorar su respuesta ante eventos inesperados que atenten contra la confidencialidad, la integridad y disponibilidad de los datos clínicos.

Para el análisis de los datos se tomaran en consideración los resultados proporcionados en el instrumento, fueron aplicados cuatro cuestionarios considerando unidades de segundo y tercer nivel del IMSS e ISSSTE, es importante hacer mención sobre las limitantes que se presentaron y que impidieron aplicar los cuestionarios en algunas instituciones, esto en respuesta a varios factores, los cuales se enlistan a continuación:

- Burocratización de la solicitud.
- Falta de respuesta por parte de la institución.
- Falta de interés en el tema.
- Hermetismo en consideración al tema de seguridad de la información.

Es por ello que para realizar un análisis a mayor detalle se considerarán de forma adicional los informes oficiales de las instituciones de salud IMSS (Instituto Mexicano de Seguridad Social) y el ISSSTE (Instituto de Seguridad y Servicios Sociales de los Trabajadores del Estado), así como datos de las instituciones presentados en la página del IFAI (Instituto Federal de Acceso a la Información y Protección de Datos) y mediante solicitudes de información realizadas a través del sistema INFOMEX del IFAI, como parte del programa transparencia y rendición de cuentas, además de estadísticas obtenidas en el INEGI (Instituto Nacional de Estadística y Geografía).

Es importante destacar que a través del sistema INFOMEX se han realizado el 96.6% del total de las solicitudes, que desde el año 2003 hasta noviembre de 2013 han llegado al millón, según datos presentados por el IFAI. Entre las diez dependencias que han recibido el mayor número de solicitudes de información, encabeza el listado el IMSS, en cuarto lugar el ISSSTE y en quinto la Secretaría de Salud, lo cual es un reflejo claro de las inquietudes e inconformidades que la población tiene con relación a estas instituciones y que a través del IFAI buscan obtener una respuesta.

5.1 DESCRIPCIÓN INSTITUCIONAL

Con base en información del INEGI el Instituto Mexicano del Seguro Social (IMSS) en el Distrito Federal se divide en dos regiones DF norte y sur, el ISSSTE (Instituto de Seguridad y Servicios Sociales de los Trabajadores del Estado) se divide en cuatro delegaciones área norte, oriente, poniente y sur, el número de unidades de segundo y tercer nivel con las que cuenta cada delegación se presenta en la figura 5.1 Número de unidades IMSS-ISSSTE segundo y tercer nivel:

Figura 5. 1 Número de unidades IMSS-ISSSTE segundo y tercer nivel

IMSS-DF 2012		
Unidades de segundo tercer nivel en el DF 2012		
Región/delegación	**Segundo nivel**	**Tercer nivel**
DF norte	8	10
DF sur	15	7

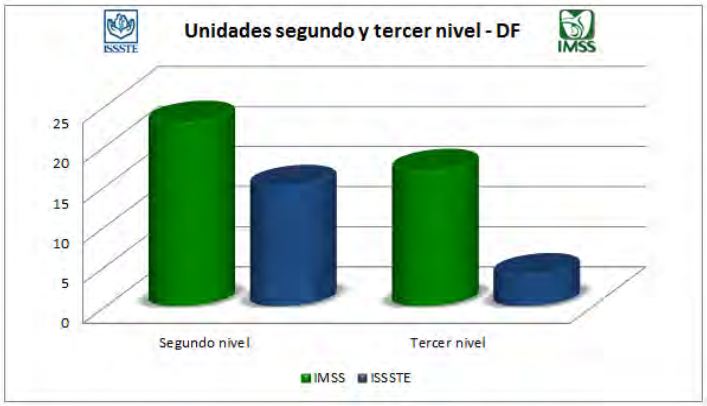
ISSSTE- DF 2012		
Unidades de segundo tercer nivel en el DF 2012		
Región/delegación	**Segundo nivel**	**Tercer nivel**
Área norte	6	1
Área oriente	2	1
Área poniente	3	0
Área sur	4	2

Fuente: Elaboración propia, con información de:

- IMSS. (2013). Informe al Ejecutivo Federal y al Congreso de la Unión sobre la situación financiera y los riesgos del IMSS 2012-2013. Consultado en: http://www.imss.gob.mx/estadisticas/Documents/20122013/InformeCompleto.pdf
- ISSSTE. (2013). Informe financiero y actuarial 2012. Consultado en: http://www2.issste.gob.mx:8080/images/downloads/instituto/quienes-somos/ifa_2012.pdf

Específicamente el total de unidades de segundo y tercer nivel del IMSS e ISSSTE con las que cuenta el Distrito Federal, se ilustra en la figura 5.2 Unidades segundo y tercer nivel-DF:

Figura 5. 2 Unidades segundo y tercer nivel -DF.



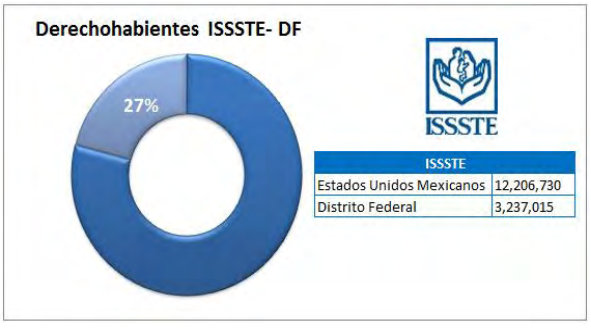
	Segundo nivel	Tercer nivel
IMSS	23	17
ISSSTE	15	4

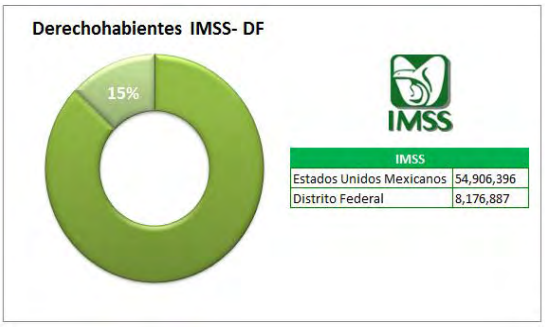
Fuente: Ídem

Del gráfico anterior se identifica que el IMSS en el Distrito Federal cuenta con más unidades de segundo y tercer nivel en comparación con el ISSSTE, de igual forma puede observarse que el número de hospitales de segundo nivel para el IMSS son mayores en comparación con los de tercer nivel, lo que evidencia los grandes retos que enfrenta en IMSS al ser una de las instituciones que concentra la mayor cantidad de derechohabientes y de instalaciones de segundo y tercer nivel.

Mediante el análisis de las estadísticas del año 2011 presentadas por el INEGI para las instituciones consideradas en el alcance de la presente investigación, de un total de 12,206,730 derechohabientes afiliados al ISSSTE, el 27% se concentra en el Distrito Federal, para el caso de IMSS de un total 54,906,396 derechohabientes el 15% se encuentran ubicados en esta misma entidad (véase figura 5.3 Derechohabientes ISSSTE-IMSS en el Distrito Federal).

Figura 5. 3 Derechohabientes ISSSTE-IMSS en el Distrito Federal.





Fuente: Ídem

La gran concentración de derechohabientes en el Distrito Federal, genera que las unidades médicas de estas instituciones se encuentren en la mayoría de los casos saturadas, con

tecnologías en algunos casos obsoletas y con una prestación de servicios deficiente, éstos factores favorecen la presencia de incidentes de seguridad de la información, como resultado de errores, descuidos y abusos por parte de personal tanto interno como externo.

En las unidades donde se aplicó el instrumento se brinda atención médica para las siguientes especialidades y subespecialidades: medicina interna, cirugía, ginecobstetricia, pediatría, dermatología, neurología, neumología, oncología, cardiología, ginecología, geriatría, traumatología y ortopedia, dermatología y hematología.

Durante la aplicación se observaron una gran cantidad de derechohabientes solicitando el servicio médico en las unidades analizadas, además de recursos tecnológicos desaprovechados que se traducía en grandes tiempos de espera para recibir la atención médica, situación que lógicamente generaba un descontento en los derechohabientes que esperaban impacientes para ser atendidos y quienes aunado a su malestar físico debían tolerar las deficiencias operacionales y administrativas de la unidad médica.

En cuanto al tratamiento de los expedientes clínicos de los pacientes, en algunas unidades se observó que éstos se encontraban apilados en escritorios o en las áreas de archivo clínico, con medidas para controlar el acceso deficientes, además de equipos de cómputo sin bloqueo de sesión cuando el usuario del mismo no se encontraba cerca, esto aunado a comentarios de médicos que como usuarios de los sistemas de información manifestaban su descontento sobre campos innecesarios o excesivos en los formularios de los sistemas o sobre diseños que complicaban los tiempos para dar atención al paciente y que dadas las condiciones establecidas por la demanda del servicio ellos deben cumplir.

Con relación a los recursos tecnológicos los resultados del instrumento reflejan que las unidades de segundo nivel cuentan en promedio con más de 200 computadoras, las de tercer nivel entre 400 y 500 equipos, en el caso de las computadoras portátiles, las unidades de segundo y tercer nivel cuentan en promedio con un número entre 50 y 100 equipos. Sobre las impresoras las unidades de segundo y tercer nivel tienen entre 100 y 250 dispositivos disponibles para brindar el servicio de impresión en las diferentes unidades de atención.

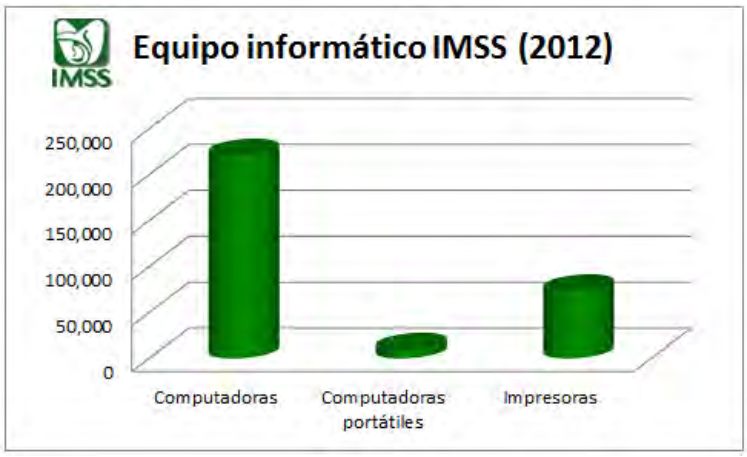
Para mayor detalle y precisión sobre esta información se analizaron los informes de ambas instituciones donde se obtuvieron los siguientes datos en materia de recursos tecnológicos:

- *IMSS:*
  Según los datos presentados en el documento denominado *"Informe al ejecutivo Federal y al Congreso de la Unión sobre la situación financiera y los riesgos del Instituto Mexicano del Seguro Social 2012-2013"* se presenta a continuación la información sobre los recursos informáticos y de comunicaciones con los que cuenta el instituto, para la prestación de los servicios de salud a la población derechohabiente.

Las cifras que se incluyen en la figura 5.4 Equipo informático y de comunicación, corresponden a todas las entidades que forman parte del IMSS, en su régimen ordinario.

Figura 5. 4 Equipo informático y de comunicación IMSS (2012).

IMSS	
Computadoras	220,654
Computadoras portátiles	9,332
Impresoras	72,981
Internet	Si
Sistemas de cómputo	100
Bases de datos	4000
Red Privada Virtual	si



Fuente: Elaboración propia, con información de: IMSS. (2013). Informe al Ejecutivo Federal y al Congreso de la Unión sobre la situación financiera y los riesgos del IMSS 2012-2013. Consultado en: http://www.imss.gob.mx/estadisticas/Documents/20122013/InformeCompleto.pdf

En la actualidad la estrategia tecnológica ha privilegiado el diseño e implantación de sistemas disasociados, lo que ha frenado la modernización del instituto, el cual sigue operando bajo modelos convencionales de atención y operación, ésta situación explica que la gran mayoría de los trámites sean presenciales, que la comunicación entre las principales bases de datos no sea eficiente y que la adopción de la firma electrónica avanzada no haya sido una prioridad.

Sobre los servicios de red el instituto cuenta con una Red Privada Virtual, siendo ésta la más grande en su tipo en México, esta red es de vital importancia para la operación, dado que a través de ella se realiza la transferencia de voz, datos y video. La red interconecta 2,910 nodos que incluyen desde las delegaciones, subdelegaciones y unidades médicas de los tres niveles de atención, hasta velatorios y centros

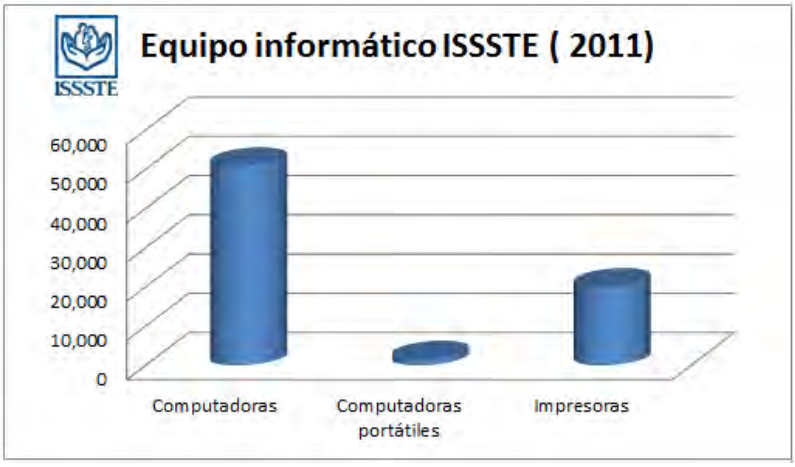
vacacionales a lo largo de todo el país. Actualmente esta red ha sido rebasada en su capacidad tecnológica dado que su diseño es obsoleto, generando bajo rendimiento operativo, el IMSS sigue operando con este red aún con los problemas anteriormente descritos dado que no cuenta con el tiempo ni con los elementos necesarios para realizar una nueva adquisición.

- *ISSSTE:*

  Con base en la información del documento denominado *"Informe de Rendición de Cuentas de la Administración Pública Federal 2006 – 2012 del ISSSTE"*, se identifican los recursos informáticos disponibles para que el instituto brinde el servicio de salud a los derechohabientes. Esta información se resume en la figura 5.5 Equipo informático ISSSTE.

Figura 5. 5 Equipo informático ISSSTE (2011)

	ISSSTE
Computadoras	50,853
Computadoras portátiles	1,541
Impresoras	20,066
Internet	Si
Sistemas informáticos	35



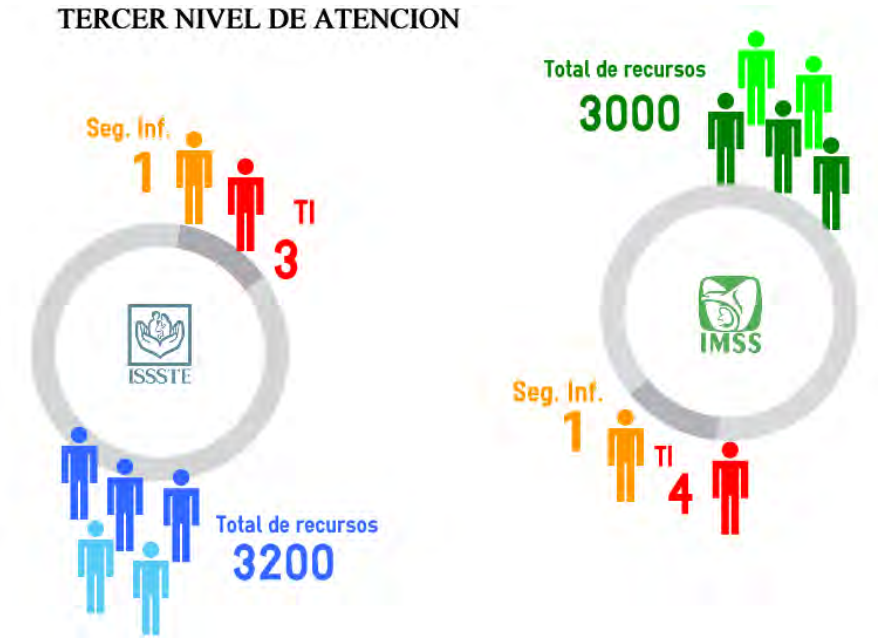
Fuente: Elaboración propia, con información de: ISSSTE. (2011). Informe de Rendición de Cuentas de la Administración Pública Federal 2006 – 2012 del ISSSTE. Consultado en: http://www2.issste.gob.mx:8080/images/downloads/transparencia/rendicion-de-cuentas/Compilado_Informes_Rendicion_Cuentas_ISSSTE.pdf

El instituto desde el año 2006 ha enfocado sus esfuerzos en la renovación tecnológica del equipo de cómputo, mediante la contratación de servicios administrados que le permitan controlar los costos, reducir los riesgos asociados, generar ahorros considerables y contar con equipos de última generación. Es hasta el año 2007 que el

equipo de cómputo existente en las diferentes unidades del instituto se adquiría y era integrado al inventario institucional, a través de cada unidad administrativa, delegación estatal y regional, así como de los hospitales regionales. Es a partir del 2008 cuando entran en vigencia los contratos de servicios administrados cuyo objetivo principal, es la contratación de la prestación de paquetes de servicios integrales de cómputo administrativos, para satisfacer las necesidades y especificaciones del instituto. Los servicios que incluyen estos contratos son: provisión, entrega, instalación y soporte en sitio de equipos de cómputo y periféricos, además de una mesa de servicios con capacidad para soportar la atención de incidentes.

Sobre los recursos humanos con los que cuentan las instituciones IMSS e ISSSTE, para dar atención a temas de TIC[6] y seguridad de la información, con base en los resultados obtenidos a través del instrumento se observó, que en la mayoría de las unidades entrevistadas, la cantidad de personas asignadas a estas tareas oscilaba entre 2 y 4 para TI y entre 1 y 2 para seguridad de la información, lo cual evidencia la falta de personal en estas áreas de apoyo, que son vitales para la prestación de los servicios de salud a los derechohabientes (véase figura 5.6 Recursos de TI y seguridad de la información tercer nivel y 5.7 Recursos de TI y seguridad de la información segundo nivel).

Figura 5. 6 Recursos de TI y seguridad de la información tercer nivel.



Fuente: Elaboración propia

[6] **TIC:** Tecnologías de información y comunicaciones.

Figura 5. 7 Recursos de TI y seguridad de la información segundo nivel.

Fuente: Elaboración propia

Al llevar a cabo el análisis de los diferentes informes de ambas instituciones no se encontraron datos sobre la distribución de los recursos humanos para las áreas de TI o seguridad de la información.

5.2 GESTIÓN DE RIESGOS DE SEGURIDAD

Los resultados de las unidades analizadas, sobre temas relacionados con la gestión de riesgos de seguridad de la información indican para el caso del ISSSTE, que unidades tanto de segundo como de tercer nivel tienen identificados y documentados sus procesos y en algunos casos se cuentan con Sistemas de Gestión de la Calidad, si bien cuentan con inventarios de los recursos en las unidades médicas, éstos no identifican los recursos críticos en materia de tecnologías de información y comunicaciones, fundamentales para la operación diaria. Además no se cuenta con una metodología para la gestión de riesgos de seguridad de la información.

Las principales amenazas que afectan la seguridad de los datos clínicos y que se presentan tanto en las unidades de segundo y tercer nivel del ISSSTE, que fueron entrevistadas se muestran en la figura 5.8 Principales amenazas que afectan la seguridad de los datos clínicos en el ISSSTE:

Figura 5. 8 Principales amenazas que afectan la seguridad de los datos clínicos en el ISSSTE.

Fuente: Elaboración propia

El tratamiento de los riesgos, se realiza mediante la evitación de la actividad que da origen al riesgo o cambiando las condiciones bajo las cuales se efectúa dicha actividad, es importante destacar que la forma de reacción ante eventos no deseados en materia de seguridad de la información es de tipo reactiva.

En aspectos de concientización, para la unidad de segundo nivel se llevan a cabo campañas informativas sobre la protección de la información y el uso adecuado de los recursos de TI, en la unidad de tercer nivel entrevistada se menciona la falta de campañas en materia de seguridad de la información.

Para el IMSS la situación es similar se tienen identificados y documentados los procesos en las unidades entrevistada tanto de tercer nivel como de segundo, en ambos casos no se cuentan con un listado de los recursos críticos en materia de TI, pero a nivel operación se encuentran identificados de forma física, en las unidades analizadas no se tiene una metodología para gestionar los riesgos de seguridad de la información y las principales amenazas se muestra en la figura 5.9 Principales amenazas que afectan la seguridad de los datos clínicos en el IMSS:

Figura 5. 9 Principales amenazas que afectan la seguridad de los datos clínicos en el IMSS.

Fuente: Elaboración propia

El tratamiento de los riesgos, se realizan mediante la mitigación implementando mecanismos para reducir los riesgos identificados, de igual forma la reacción ante eventos no deseados en materia de seguridad de la información es de tipo reactiva.

Sobre las campañas de concientización sobre seguridad de la información en las unidades entrevistadas se menciona que no se llevan a cabo.

En los informes de las instituciones del IMSS e ISSSTE no se mencionan información o datos relacionado con el tema de gestión de seguridad de la información.

5.3 SEGURIDAD DE LA INFORMACIÓN

En temas relacionados con seguridad de la información con base en los resultados se obtuvo que para el caso de las unidades analizadas del ISSSTE e IMSS, éstas cuentan con un manual de políticas de seguridad en ambos casos aprobadas por el director, el personal entrevistado refiere la falta de campañas que contribuyan para dar a conocer y cumplir las políticas, además se indica que no se cuenta con un comité que tome decisiones en temas relacionados con la seguridad de la información ni con procedimientos especiales sobre este mismo tema para los proveedores.

Sobre la información gestionada por estas instituciones, ésta es clasificada y etiquetada, los sistemas de información cuentan con una bitácora que permite controlar los accesos. Para el uso de los sistemas se definen privilegios tomando como base los roles del personal, el acceso a los equipos de cómputo y sistemas de información se realiza mediante contraseñas en algunos casos proporcionadas por el personal o por las áreas de TI. Las unidades analizadas cuentan con una red interna y conexión a Internet cuyo acceso es controlado, el personal puede conectar sus dispositivos móviles a la red de la institución.

En materia de cumplimiento las unidades entrevistadas conocen la legislación aplicable a su sector, siendo éstas la Ley Federal de Transparencia y Acceso la Información Pública, la Ley General de salud y su reglamento, las normas oficiales mexicanas 001, 024 y 040, las unidades desconocen estándares internacionales y marcos de referencia sobre seguridad de la información y buenas prácticas de servicios de TI.

En temas de continuidad desconocen si existe un plan de continuidad del negocio, pero si hacen mención de un plan ante desastres, el cual incluye actividades como la generación de respaldos de la información, la contratación de servicios para brindar soporte ante fallas eléctricas y de forma preventiva se cuenta con un programa de mantenimiento de los equipos.

Para el desarrollo de sistemas se consideran validaciones de los datos, el cifrado de información sensible y se llevan a cabo pruebas previas a su implantación en producción.

Sobre la gestión de incidentes de seguridad las unidades del ISSSTE e IMSS analizadas indican que no existe un procedimiento para llevar a cabo este control y por lo tanto no cuentan con una base de

conocimiento que les permita monitorear los incidentes de seguridad que atenten contra la confidencialidad, integridad y disponibilidad de la información.

Estos resultados son una muestra del estado de la seguridad de la información en estas instituciones, al solicitar información estadística para corroborar los resultados obtenidos mediante el instrumento se presentaron limitantes por parte de las instituciones IMSS e ISSSTE que aún mediante una solicitud formal de información a través del sistema de INFOMEX hasta la fecha enero de 2014 no se ha obtenido respuesta concreta a los datos solicitados. Además durante la revisión de los informes de ambas instituciones no se menciona información alguna relacionada con las necesidades en temas de seguridad de la información que sin duda requiere el sector salud, considerando que la mayoría de los datos que son utilizados para la prestación del servicio son sensibles.

De ahí que instituciones como el Instituto Federal de Acceso a la Información y Protección de Datos (IFAI) a través de la comisionada María Elena Pérez-Jaén durante el Segundo Foro Nacional de Transparencia y Datos Personales[7] celebrado el 15 de febrero del 2013 haga énfasis en la necesidad de que las instituciones prestadoras de servicios de salud establezcan reglas y estándares de comportamiento para la protección de los datos personales gestionados por este sector, indicando a su vez que el IFAI ya se encuentra tomando medidas sobre el tema, llevando a cabo estudios y encuestas que le permitan conocer el sector y contribuir para la adopción de las mejores prácticas en materia de protección de datos personales.

De igual forma el gobierno federal ha definido nuevas estrategias, una de estas iniciativas se encuentra plasmada en la recién liberada "Estrategia Digital Nacional"[8], la cual tiene como objetivo mejorar el uso de la tecnología para contribuir al desarrollo del país, cinco objetivos son los que conforman dicha estrategia, en aspectos relacionados con la salud se encuentra el objetivo número cuatro denominado Salud universal y efectiva, creado con la finalidad de aprovechar la incorporación de las tecnologías de información y comunicaciones como medio para aumentar la cobertura, el acceso y la calidad de los servicios de salud, además para lograr el uso eficiente de la infraestructura y los recursos destinados para proveer el servicio de salud a la población, previo a esta estrategia se contaba ya con iniciativas de integrar los datos clínicos en un expediente electrónico, lo cual ha sido implantado en algunas entidades, así como la existencia de leyes en México que regulan en el sector público y privado, la protección de los datos personales, los datos personales sensibles y normas oficiales mexicanas en materia de salud.

Todas estas iniciativas que si bien son de gran ayuda deben ir de la mano con una estrategia en materia de seguridad de la información, que considere la gestión de nuevos riesgos asociados a la incorporación de las TIC, donde previamente sea evaluada y considerada la problemática a nivel organizacional que enfrenta el sector y la fuerte resistencia al cambio que prevalece, aunado a una gran falta de conciencia sobre temas relacionados con la seguridad de la información, factores que

[7] Imprescindible, unir esfuerzos para garantizar confidencialidad de Datos personales en el sector salud: María Elena Pérez-Jaén http://inicio.ifai.org.mx/Comunicados/Comunicado%20IFAI-019-13.pdf

[8] Estrategia Digital Nacional para transformar a México: http://www.presidencia.gob.mx/estrategia-digital-nacional-para-transformar-a-mexico/

de no ser considerados podrían convertirse en una gran limitante para que esta estrategia sea implementada.

Otra evidencia que muestra la necesidad de mejorar la seguridad de la información son los incidentes relacionados con casos de robo de identidad que se han presentado en el IMSS[9], o robo de medicamentos en el ISSSTE[10], aunado a los desfalcos financieros en ambas instituciones evidenciados por la Auditoría Superior de la Federación (ASF)[11], problemas que en gran parte se presentan como resultado de controles de acceso a la información deficientes que permiten que redes de corrupción internas hagan mal uso de la información a la que tienen acceso.

Los resultados de las auditorías de la ASF sobre el aprovechamiento de la infraestructura y servicios de las TIC del Instituto Mexicano del Seguro Social (ASF, 2014c) y el Instituto de Seguridad y Servicios Sociales de los Trabajadores del Estado (ASF, 2014b) reflejan la situación actual en temas de seguridad de la información y los principales retos que deben ser considerados por estas instituciones. (ASF, 2014a)

En el caso del IMSS el informe de la ASF presenta los siguientes resultados:

- Con base en los registro contables del ejercicio 2012, el IMSS ha empleado, 2,569,632.9 miles de pesos en contrato relacionados con las TIC, lo cual muestra la importancia que éstas representan en la actualidad para la operación del instituto y la necesidad no sólo aprovechar los recursos adecuadamente, además es fundamental incluir medidas para proteger la información que es tratada mediante el uso de diversos recursos tecnológicos.

- En cuanto a los registro contables sobre los equipos de cómputo es necesario que instituto lleve un adecuado control sobre los equipos que están ya obsoletos, que se encuentran totalmente depreciados o que hayan sido retirado de la operación con el objetivo de tener un control adecuado sobre los activos.

- En el tema de cumplimiento el IMSS debe implementar dentro de sus actividades y procesos el Manual Administrativo de Aplicación General en Materia de Tecnologías de la Información y Comunicaciones y de Seguridad de la Información (MAAGTIC-SI), siendo el 52.1% el avance con el que hasta el momento el instituto cuenta, los principales riesgos que la ASF identificó como resultado de no contar con el 100% de avance en la implementación de MAAGTIC-SI son, la carencia en la planeación, evaluación y monitoreo de los procesos de TICs, lo cual complica las tareas de mejora continua, además la falta de un catálogo de servicios que permitan identificar la capacidad y los riesgos de interrupción o degradación, aunado a la necesidad de definir

[9] Denuncian presunto robo de identidad en el IMSS http://info7.mx/a/noticia/452892
[10] Habían denunciadodesde2011 robo en ISSSTE http://www.eluniversal.com.mx/nacion-mexico/2013/issste-irregularidades-denuncia-942889.html
[11] Detecta Federación gastos millonarios sin justificar en IMSS, ISSSTE y CFE: http://www.cambiodigital.com.mx/mosno.php?nota=133256#.UtXT__TuJfA

mecanismos para el monitoreo e identificación de las soluciones tecnológicas de TICs incluidas en la operación.

- Sobre la política de seguridad de la información a nivel institucional, ésta no ha sido desarrollada, implementada y documentada.

- De la documentación relacionada con el análisis de riesgos, las vulnerabilidades no están identificadas, generando en consecuencia que el análisis y selección de los controles a implementar no sean los adecuados y estén incompletos por no cubrir con todos los requerimientos de seguridad de la información.

- Se carece de políticas institucionales sobre, el borrado seguro de información, la revisión periódica de los registros de actividades de los usuarios en los sistemas, la clasificación de información que permita identificar la criticidad y confidencialidad.

- No se cuenta con un programa de trabajo actualizado para generar conciencia al personal sobre la seguridad de la información.

- No se mantiene supervisión y vigilancia sobre el cumplimiento de las propias políticas de seguridad institucionales.

- La configuración y estructura de las contraseñas no es aplicada de manera consistente y con base a la política de usuarios y contraseñas institucional.

- Las bajas o eliminación de cuentas no son notificadas de forma oportuna.

- Los controles requeridos para la continuidad de la operación son insuficientes, no se cuenta con un plan de pruebas periódicas para la restauración de los respaldos en cintas magnéticas, considerando que se tienen más de 7,000 cintas con información histórica del instituto, aunado a equipos de extinción de incendio que no han sido probados.

- No se cuentan con procedimientos documentados, formalmente establecidos y difundidos para llevar a cabo cambios en la infraestructura.

- En algunos sistemas las bases de datos tiene datos incorrectos, se presentan redundancias, inconsistencias, y carencia de los mismos, lo cual evidencia una debilidad en los controles que validan la captura de información.

- Sobre el inventario se identificaron casos de equipos que están subutilizados y de otros que no se encontraban físicamente en las instalaciones, pero de los cuales se contaba con su registro en el inventario.

- En el tema del expediente clínico electrónico este sólo se ha desplegado en 40 unidades que representan el 2.2% de las 1,797 con las que cuenta el instituto, donde la principal problemática para su adopción ha sido la resistencia al cambio por parte del personal para su uso y la gestión deficiente de recursos financieros dedicados a proyectos relacionados con el expediente clínico electrónico.

- En cuanto a recursos tecnológicos empleados en la operación diaria en la muestra analizada por la ASF se identificaron problemas como la saturación de la red, la falta de identificación del tráfico, la disponibilidad de los aplicativos, la congestión de las aplicaciones y en la operación de las mismas.

- El dictamen que la ASF emitió como resultado de la auditoría realizada al IMSS en el Aprovechamiento de Infraestructura y Servicios de las TIC fue negativo.

Para el ISSSTE la situación no es diferente, los resultados del informe de la ASF indican lo siguiente:

- El ISSSTE asignó 1,255,316.5 miles de pesos para proyectos y servicios destinados a las TIC, con el objetivo de incluir tecnología para mejorar la atención y agilizar la prestación de los servicios de salud, del listado de proyectos se identificaron dos relacionados con el gobierno de tecnologías de información y datos, así como para la administración del ciclo de vida y protección de los datos reservados.

- Sobre el cumplimiento con el Manual Administrativo de Aplicación General en Materia de Tecnologías de la Información y Comunicaciones y de Seguridad de la Información (MAAGTIC-SI) los resultados de la evaluación de los procesos y actividades por la ASF identificó que el porcentaje de implementación de MAAGTIC-SI en el ISSSTE es de 37.9%, donde los principales riesgos identificados son: la carencia de revisión y actualización de estándares tecnológicos, la falta de análisis de los riesgos y de los escenarios operativos, carencia de un procedimiento que indique los criterios técnicos a evaluar para aceptar las soluciones tecnológicas, no se cuentan con documentación relacionada con lecciones aprendidas lo cual genera reincidencia en situaciones que afectan el aprovechamiento de la tecnología adquirida, se carece de un sistema de gestión y mejora de procesos que facilite la actualización de los mismos, no se cuentan con controles adecuados para los recursos asignados, además falta un catálogo de servicios y de un portafolio de proyectos completo y actualizado de TIC, que permita llevar la gestión de los mismos, no existe un plan de continuidad de servicios, un análisis de impacto, ni un plan de recuperación de desastres, no se tiene definido un plan de seguridad de la información, que permita garantizar la protección de los activos de información que son utilizados en la operación diaria, lo que implica una deficiente capacidad para administrar la seguridad de la información en el ISSSTE y para mitigar el impacto de eventos adversos.

- No se cuenta con una política institucional para el borrado seguro de los equipos de escritorio y de los dispositivos de almacenamiento de la infraestructura tecnológica.

- El instituto carece de un plan de recuperación de desastres.

- No se cuenta con un procedimiento de administración de usuarios unificado, ni mecanismos para el monitoreo de las atribuciones que pueden tener los usuarios en cada aplicativo, además no se cuentan con bitácoras para la detección de actividades no autorizadas.

- No existe un Sistema de Gestión de Seguridad de la Información (SGSI), además no existen evidencias de esfuerzo alguno para la creación de un análisis de impacto al negocio, ni de un plan para la continuidad del negocio.

- Se tiene el riesgo de pérdida de información confidencial y existe la posibilidad de "fuga de información", mediante la extracción de equipos que sean enviados a reparación, sean reemplazados o reasignados a otro usuario dado que no se cuenta con un procedimiento para realizar el borrado seguro de la información.

- Las acciones para asegurar la operación de los servicios y procesos críticos son deficientes.

- Incumplimiento con los "Lineamientos de Protección de Datos" emitidos por el Instituto Federal de Acceso a la Información Pública (IFAI) esto como resultado de la revisión por parte de la ASF en los datos, que tuvo como resultado deficiencias del 99% en la estructura correcta del Registro Federal de Contribuyentes (RFC) que puede provocar problemas de homonimias y el 54.8% de los registros no tienen número telefónico.

- Sobre el expediente clínico electrónico el instituto indicó a la ASF que la plataforma ISSSTEMED en su versión 5 se encuentra en operación y en uso, con base en datos de noviembre de 2012 a diciembre de 2013 indica que 1,644.5 miles de consultas son registradas en el sistema. Para la revisión del uso de ISSSTEMED la ASF tomó una muestra y llevó a cabo auditorías para verificar la información, de lo cual presentó los siguientes resultados, la capacitación que el proveedor impartió en algunas unidades médicas consistió en un asesoría de veinte minutos y para un número bajo de personal, en otras unidades la capacitación fue mediante una plática general y asistencia personal a cada médico en su consultorio.

- Sobre el servicio de ISSSTEMED la ASF determinó como resultado de sus auditorías que éste no está implementado en segundo y tercer nivel de atención del ISSSTE, por lo que trabajan de forma manual con excepción del Centro Médico Nación "20 de

Noviembre" que cuenta con una aplicación propietaria llamada " Sistema Integral de Administración Hospitalaria".

- En las clínicas auditadas por la ASF, los médicos manifestaron problemas con la red de datos, lentitud del sistema, deficiencias con la operación y mantenimiento de los equipos de cómputo, lo cual complica el uso del sistema.

- Se determinaron como resultados de las auditorías de la ASF incumplimientos de leyes, reglamentos y disposiciones normativas.

- El dictamen que la ASF emitió como resultado de la auditoría realizada al ISSSTE en el Aprovechamiento de Infraestructura y Servicios de las TIC fue negativo.

5.4 CONCLUSIONES

Los resultados de aplicar el instrumento fueron utilizados para dar respuesta a las preguntas de investigación planteadas en el capítulo 4, obteniendo lo siguiente:

- *¿Cuál es la relación existente entre la gestión de riesgos de seguridad de la información y la protección de los datos clínicos?*

  Considerando el estado del arte, que se encuentra en el Anexo C, el marco teórico comprendido en los capítulos 1, 2 y 3 y los resultados del instrumento, se identifica la necesidad de que el Sector Salud cuente con una gestión adecuada de los riesgos de seguridad de la información, que forme parte de una estrategia institucional, para la protección de la confidencialidad, integridad y disponibilidad de los datos clínicos, tomando en consideración la presencia cada vez mayor que tienen las tecnologías de la información y comunicaciones en la operación, como medio para mejorar la prestación del servicio, aunado a la gran demanda y las condiciones actuales de las instituciones IMSS e ISSSTE. Una metodología para gestionar los riesgos de seguridad de la información alineada a sus objetivos organizacionales y que contribuya a identificar las posibles amenazas y de forma proactiva definir controles que permitan reducir el impacto en caso de que éstas se materialicen, logrando con ello reducir los incidentes que por ahora afectan las finanzas, la productividad y la reputación de las instituciones.

- *¿El personal que hace uso de la información conoce las principales amenazas que atentan contra la seguridad de los datos clínicos?*

  Del trabajo de campo se observó que el personal de las unidades analizadas no tiene conciencia sobre los riesgos y el impacto que puede tener si los datos clínicos son comprometidos, la preocupación está más enfocada en la prestación del servicio, dejando de lado el tema de seguridad de la información, aunado a la falta de capacitación sobre estos temas.

- *¿Cuáles son las medidas implementadas en las instituciones de salud para proteger los datos clínicos de los pacientes?*

  Las medidas implementadas son desde físicas como las cámaras de vigilancia, bitácoras de registro antes de ingresar a las instalaciones y custodios (policías) para controlar el acceso a las áreas restringidas, archiveros con llave, hasta medidas electrónicas como antivirus en los equipos de cómputo, controles en la red y medidas básicas para la seguridad en el desarrollo de sistemas de información, es necesario mencionar que algunas medidas son deficientes y requieren contar con un procedimiento para ser monitoreadas y medir su efectividad y eficiencia. Además aplicar estándares internacionales, marcos de referencia y buenas prácticas que podrían ser de gran utilidad para mejorar las condiciones actuales en que son protegidos los datos clínicos.

- *¿Se cuenta con alguna metodología para la gestión de riesgos de seguridad de la información implementada en las instituciones de salud?*

  Durante la revisión de la literatura y al llevar a cabo el trabajo de campo no se identificó que existiera alguna metodología para gestión de los riesgos en materia de seguridad de la información ni implementada ni documentada.

- *¿El personal responsable de la protección de los datos clínicos conoce y cumple con las leyes relacionadas con la protección de datos personales y sensibles?*

  El personal conoce y parcialmente cumple con las leyes aplicables al sector, es necesario destacar que la actualmente no existen tantas exigencias en aspectos legales sobre la protección de los datos personales y personales sensibles para el sector público, en comparación con el sector privado donde la carencia de medidas de protección para los datos personales son sancionadas con multas por parte del IFAI.

Si bien el instrumento diseñado permitió conocer el estado actual en cuanto a la protección de los datos clínicos, la seguridad de la información en las instituciones IMSS e ISSSTE, e identificar las áreas de oportunidad, la hipótesis se cubrió parcialmente dado que no se cuenta hasta el momento con alguna metodología implantada en las instituciones, ya que su enfoque ante eventos de seguridad de la información es de tipo reactiva, no obstante se considera que la investigación realizada representa un avance en este campo, que abre un área de oportunidad para futuras líneas de investigación por ser un tema que al paso de los años cobra mayor relevancia, además este trabajo tiene por objetivo una vez identificadas la áreas de oportunidad proponer una metodología para gestionar los riesgos de seguridad de la información, basada en estándares internacionales y las principales metodologías para la gestión de riesgos de seguridad, que le permita al Sector Salud actuar de forma proactiva y reducir el impacto de eventos inesperados que atenten contra la confidencialidad, integridad y disponibilidad de los datos clínicos, la cual será presentada a detalle en el capítulo 6.

CAPÍTULO 6

METODOLOGÍA PARA LA GESTIÓN DE RIESGOS DE SEGURIDAD DEL SECTOR DE SALUD EN MÉXICO

Es indudable que el sector salud tiene diversas áreas de oportunidad en temas relacionados con la seguridad de la información para la protección de los datos clínicos, esto se concluye con base en los resultados obtenidos durante la revisión de la literatura y en la investigación en campo, por tal motivo este capítulo ofrece como propuesta una metodología para la gestión de riesgos de seguridad de la información, elaborada a partir de un análisis e integración de los mejores elementos de estándares internacionales y metodologías para la gestión de riesgos, de tal forma que como resultado se obtenga una metodología personalizada a las necesidades del sector salud, que permita mejorar las condiciones actuales en que son tratados los datos clínicos de los pacientes.

La metodología para la gestión de riesgos de seguridad de la información se encuentra alineada a los objetivos establecidos en el Plan Nacional de Desarrollo (PND) 2013-2018 y al Programa Sectorial de Salud (PSS) 2013-2018, los objetivos considerados se presentan en la figura 6.1 Objetivos considerados del PND y PSS:

Figura 6. 1 Objetivos considerados del PND y PSS.

Plan Nacional de Desarrollo
Objetivo 2.3 Asegurar el acceso a los servicios de salud Estrategia 2.3.1 Avanzar en la construcción de un Sistema Nacional de Salud La metodología de riesgos de seguridad propuesta debe ser utilizada como un instrumento que permita mejorar la efectividad de las instituciones de salud IMSS e ISSSTE logrando así el control, el uso de sus recursos y la seguridad de la información de los datos clínicos.

Figura 6. 1 Objetivos considerados del PND y PSS. (Continuación)

Programa Sectorial de Salud
Estrategia 2.2 Mejorar la calidad de los servicios de salud del Sistema Nacional de Salud. Líneas de acción 2.2.1 Impulsar acciones de coordinación encaminadas a mejorar la calidad y seguridad del paciente en las instituciones de salud. 2.2.2 Impulsar el cumplimiento de estándares de calidad técnica y seguridad del paciente en las instituciones de salud. 2.2.6 Fomentar el uso de las NOM, guías de práctica clínica, manuales y lineamientos para estandarizar la atención en salud. *Estrategia 5.1. Fortalecer la formación y gestión de recursos humanos en salud.* Líneas de acción 5.1.4 Promover la capacitación para mejorar los procesos de atención en salud, gerenciales y de apoyo administrativo. La metodología de riesgos de seguridad propuesta permitirá controlar y proteger los recursos de las instituciones lo que dará como resultados mejoras en cuanto a la productividad, dado que la metodología se basa en estándares internacionales en materia de seguridad de la información y gestión de riesgos que ayudarán a que las instituciones de salud IMSS e ISSSTE adopten medios para proteger la seguridad de la información de sus activos, favoreciendo el cumplimiento de las normas oficiales mexicanas que apliquen. Como aportación a la capacitación la metodología sugiere el desarrollo de un programa basado en roles, para mejorar la cultura organizacional en temas relacionados con la protección de la confidencialidad, integridad y disponibilidad de los datos clínicos.

Fuente: Elaboración propia

6.1 OBJETIVO

El objetivo de la metodología CADERVIM es lograr el equilibrio óptimo entre la prestación del servicio con eficiencia, el cumplimiento con los objetivos institucionales, la reducción de las vulnerabilidades y pérdidas que afectan la reputación y la operación de las instituciones IMSS e ISSSTE.

La implantación de la metodología en las instituciones, permitirá identificar los riesgos y priorizarlos, además de contar con mayor información para la toma de decisiones, lo que dará como resultado una mejor selección de los controles estratégicos, tácticos y operativos, que permitan reducir los eventos adversos que atenten contra la confidencialidad, integridad y disponibilidad de los datos clínicos.

La adopción de la metodología para la gestión de riesgos de seguridad de la información requiere que las instituciones y su personal asuman el compromiso, para que los cambios derivados de la implementación formen parte de la cultura organizacional, de tal forma que cada área acepte la responsabilidad que le corresponde y contribuya a la implantación eficiente y efectiva de los controles requeridos para el tratamiento de los riesgos.

6.2 ROLES Y RESPONSABILIDADES

Los roles y las responsabilidades requeridas para la implementación y mantenimiento de la metodología para la gestión de riesgos de seguridad de la información en los datos clínicos se dividen en estratégicos, tácticos y operativos y se describen a continuación:

- *Roles estratégicos:* estos incluyen aquellos órganos colegiados o unipersonales que toman decisiones orientadas al cumplimiento de la misión, visión y objetivos de la institución. En esta categoría se incluyen generalmente los altos cargos de la unidad médica, es recomendable que exista la figura de un Comité de Seguridad de la Información, quien tendrá la autoridad para aceptar los diferentes criterios requeridos en la metodología para la evaluación, tratamiento y aceptación de los riesgos.

    - *Comité de seguridad de la información:* órgano colegiado integrado por el director de la unidad médica y los directores de las diferentes áreas. Las responsabilidades de este órgano serán identificar las áreas y los procesos críticos de la unidad médica, establecer la clasificación de información que será considerada por todo el personal, revisar y aprobar los criterios para evaluar y aceptar los riesgos identificados, además de la aprobación del plan de tratamiento de riesgos.

    - *Director de la unidad médica:* garantizar que los recursos se apliquen efectivamente para lograr la misión, además debe valorar e incorporar la información resultante de la evaluación de riesgos en el proceso de toma de decisiones. Una de las actividades fundamentales que debe realizar este rol es respaldar y participar activamente en la gestión de los riesgos de seguridad de la información.

- *Roles tácticos:* en esta clasificación se encuentran los órganos colegiados o unipersonales que toman decisiones para llevar a cabo los objetivos institucionales marcados o señalados por los roles estratégicos, generalmente se incluyen en esta categoría a los responsables de las diferentes áreas que conforman a la unidad médica.

    - *Directores y subdirectores de áreas:* estos roles deben asumir una posición activa en el proceso de gestión de riesgos, dada la autoridad y la responsabilidad que sobre ellos recae deben tomar decisiones que favorezcan la selección,

implementación y mantenimiento de los controles requeridos para el tratamiento de los riesgos. Para ello deberán hacer consideraciones basadas en el costo – beneficio.

- *Director de tecnologías de información:* es el responsable de la planificación, el presupuesto y el rendimiento de las tecnologías de información y comunicaciones, incluyendo sus componentes de seguridad de la información.

- *Responsable de la gestión de riesgos:* personal responsable de llevar a cabo la implementación, mantenimiento y mejora de la metodología de gestión de riesgos de seguridad de la información, coordinar las actividades con las diferentes áreas y comunicar el plan de tratamiento a los interesados para su eficaz y eficiente implantación.

- *Roles operativos:* incluye aquellos órganos colegiados o unipersonales que toman decisiones prácticas para materializar las indicaciones establecidas por los roles tácticos. En esta categoría se incluyen a los responsable de llevar a cabo las operaciones y actividades diarias requeridas para la prestación de los servicios de salud.

  - *Jefes de departamento:* este rol por su cercanía con los procesos operativos de la unidad médica, es el responsable de guiar la implantación y la vigilancia de los controles requeridos para el tratamiento de los riesgos de seguridad de la información.

  - *Profesionales de seguridad de TI:* ejemplos de este rol son, administradores de red, sistemas, aplicaciones, base de datos, especialistas en computación, analistas y consultores de seguridad, quienes son responsables de la implementación apropiada de los requerimientos de seguridad en sus sistemas de tecnologías de información y comunicaciones. El compromiso de los profesionales de seguridad de TI es respaldar o utilizar el proceso de gestión de riesgos para identificar y valorar nuevos riesgos potenciales y definir medidas proactivas para reducir la presencia y el impacto de eventos inesperados.

  - *Propietarios de sistemas e información:* son los responsables de garantizar la existencia de controles apropiados para abordar la integridad, la confidencialidad y la disponibilidad de los sistemas de TI y datos que poseen. Los propietarios de sistemas y de información deben comprender su rol y su responsabilidad en el proceso de gestión de riesgos y respaldar totalmente este proceso.

  - *Empleados:* son los usuarios de los sistemas y quienes tienen acceso a los datos clínicos y deben contribuir al cumplimiento de las políticas, directrices, reglas y

controles establecidos por la institución, con el objetivo de reducir los riesgos de seguridad de la información.

6.3 DEFINICIONES

Las definiciones que se presentan a continuación fueron tomadas de los estándares internacionales ISO 27001:2005, ISO 27005:2008, ISO 3100:2009 y de las publicaciones especiales del NIST sobre la gestión y evaluación de riesgos de seguridad de la información:

- *Activo:* es algo a lo que una organización directamente le asigna un valor y por lo tanto debe proteger.

- *Ambiente externo:* es el entorno en el cual opera la organización, suele incluir el ambiente legal y regulatorio, las condiciones sociales y culturales, las partes interesadas externas.

- *Ambiente interno:* incluye las áreas claves que deben evaluarse a fin de brindar un panorama integral del ambiente interno de la organización.

- *Amenaza:* es cualquier evento o circunstancia con el potencial de impactar negativamente en las operaciones, los activos de una organización, los individuos, otras organizaciones, o de un país mediante el acceso no autorizado a un sistema de información o la destrucción, la divulgación o modificación de la información, así como la denegación.

- *Análisis de riesgos:* se define como la identificación y estimación del riesgo.

- *Controles:* Medios para administrar el riesgo, incluyendo políticas, procedimientos, lineamientos, prácticas o estructuras organizacionales, que pueden ser de naturaleza administrativa, técnica, de gestión o legal.

- *Dueño:* Individuo o entidad que tiene la responsabilidad aprobada por la dirección para controlar la producción, desarrollo, mantenimiento, uso y seguridad de los activos.

- *Evaluación de riesgos:* se define como el proceso para identificar y establecer un orden de prioridad del riesgo para la institución.

- *Gestión de riesgos:* aplicación sistemática de las políticas, procedimientos y prácticas de gestión a las tareas de identificar, analizar, evaluar, informar, tratar y monitorear el riesgo relacionado con la información. Es el proceso para reducir el riesgo a un nivel aceptable.

- *Impacto:* Cambio adverso al nivel de los objetivos del negocio alcanzados.

- *Riesgo de seguridad de la información:* son aquellos riesgos que surgen de la pérdida de la confidencialidad, integridad y disponibilidad de la información, de los sistemas de información y que representan un impacto potencial adverso para la operación de la organización y sus recursos.

- *Riesgo:* Una medida del grado en que está amenazada una entidad por una circunstancia o evento potencial, y por lo general una función de: (i) los efectos negativos que se producirían si la circunstancia o evento se materializa, y (ii) de la probabilidad de ocurrencia.

- *Vulnerabilidad:* debilidad en un sistema de información, procedimiento de seguridad, controles internos o implementación, que podría ser explotada por una fuente de amenaza, ya sea de forma intencional o accidental, dando como resultado una brecha de seguridad o una violación a una política de seguridad.

6.4 ENFOQUE

El enfoque considerado por la metodología para la gestión de riesgos de seguridad es semi-cuantitativa ya que utiliza una combinación de los métodos cuantitativos y cualitativos para la evaluación del riesgo.

6.5 METODOLOGÍA

Para definir las etapas de la metodología fueron considerados los siguientes modelos para la gestión de riesgos de seguridad incluyendo la perspectiva desde el ciclo de Deming (véase figura 6.2 Cuadro comparativo modelos para la gestión de riesgos de seguridad y ciclo PDCA):

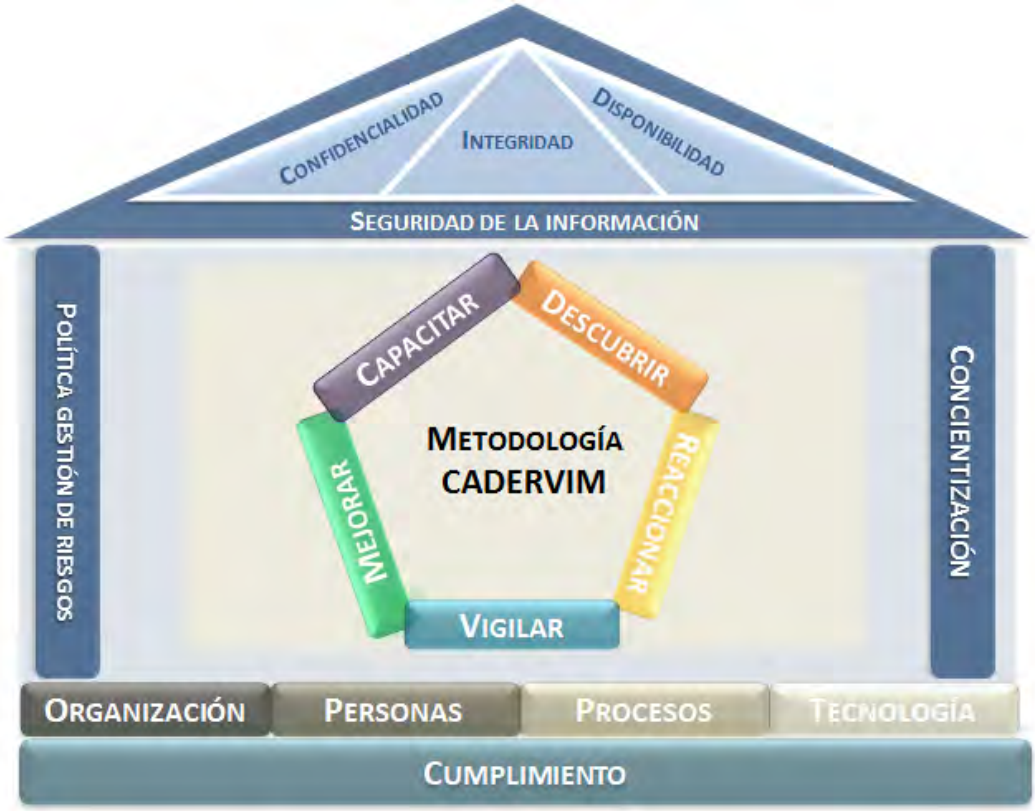
Figura 6. 2 Cuadro comparativo modelos para la gestión de riesgos de seguridad y ciclo PDCA.

NIST SP 800-30	*ISO 27005*	*ISO 31000*	*Octave Allegro*	*FAIR*	*PDCA*
1. Preparación para la evaluación del riesgo: - Propósito - Alcance - Fuentes de información. 2. Conducir la evaluación: - Amenazas / eventos. - Vulnerabilidades. - Probabilidad de ocurrencia. - Impacto. - Riesgo. 3. Comunicación de los resultados.	1. Establecimiento del contexto. 2. Valoración de los riesgos: -Análisis de los riesgos. Identificación y estimación de riesgos. -Evaluación de los riesgos. 3. Tratamiento de los riesgos. 4. Aceptación de los riesgos. 5. Monitoreo y revisión. 6. Comunicación de los riesgos.	1. Establecer el contexto. 2. Valoración del riesgo: - Identificación de los riesgos. - Análisis del riesgo. - Evaluación del riesgo. 3. Tratamiento del riesgo. 4. Comunicación y consulta. 5. Monitoreo y revisión.	1. Establecer el criterio de medición del riesgo. 2. Desarrollar un perfil de activo. 3. Identificar los contenedores de los activos de información. 4. Identificar las áreas de preocupación. 5. Identificar los escenarios de amenaza. 6. Identificar los riesgos. 7. Analizar los riesgos. 8. Seleccionar un enfoque de mitigación.	1. Identificar los componentes del escenario 2. Evaluar la probable frecuencia de pérdida (LEF). 3. Evaluar la probable magnitud de la pérdida (PLM). 4. Evaluar y articular el riesgo.	*Planear (Plan)* 1. Establecer el contexto. 2. Evaluar el riesgo. 3. Desarrollar el plan de tratamiento para los riesgos identificados. 4. Aceptación de los riesgos. *Hacer (Do)* 5. Implementación del plan de tratamiento de riesgos. *Verificar (Check)* 6. Monitoreo continuo y revisión de riesgos. *Actuar (Act)* 7. Mantener y mejorar el proceso de gestión de riesgos de seguridad de la información.

Fuente: Elaboración propia

Con base en esta información se muestran en la figura 6.3 Metodología para la gestión de riesgos de seguridad de la información de los datos clínicos (CADERVIM), las etapas que conforman la metodología para la gestión de riesgos de seguridad propuesta para las instituciones de salud IMSS e ISSSTE de segundo y tercer nivel de atención en el Distrito Federal.

Figura 6. 3 Metodología para la gestión de riesgos de seguridad de la información de los datos clínicos (CADERVIM).



Fuente: Elaboración propia

La metodología CADERVIM ha sido diseñada para apoyar a las instituciones de salud IMSS e ISSSTE para llevar a cabo la gestión de los riesgos de seguridad de la información y de esta forma proteger los datos clínicos tanto en formato físico como electrónico.

La base para implementar esta metodología está formada por (véase Figura 6.4):

Figura 6. 4 Base para implementar la metodología CADERVIM.

Fuente: Elaboración propia

- *Cumplimiento:* que considera todo el conjunto de leyes, regulaciones y normas que para la prestación de los servicios de salud, las instituciones deben cumplir y de forma adicional pueden incluirse estándares de seguridad de la información.

- *Organización:* en este rubro se consideran los objetivos institucionales, la estrategia para llevarlos a cabo y los recursos necesarios (personas, equipos, conocimientos técnicos o administrativos), considerando en todo momento los factores internos y externos que puedan influir para alcanzar lo establecido en la estrategia. Esta información permite conocer la cultura organizacional en aspectos relacionados con la seguridad de la información, las áreas críticas sus procesos y activos, que forman parte de la estructura de gobierno de la institución.

- *Personas:* para llevar a cabo todas las actividades requeridas para el tratamiento de los riesgos de seguridad de la información identificados, es fundamental contar con el apoyo de todo el personal que forma parte de la institución. Dado que el personal es el primer contacto con los datos clínicos en la mayoría de los procesos, es necesario considerar medidas de seguridad como son: estrategias de reclutamiento (verificación de antecedentes, entrevistas y evaluaciones), aspectos relacionados con el empleo (ubicación del área de trabajo, acceso a herramientas, sistemas y datos, capacitación y concienciación), así como al término de la relación laboral (razones de la desvinculación, momento de la salida, roles y responsabilidades, accesos a la información y sistemas). Es de gran importancia en este rubro considerar a los proveedores, los derechohabientes y demás partes interesadas.

- *Procesos:* es necesario conocer los mecanismos formales e informales que son utilizados por la institución, para llevar a cabo las tareas requeridas para la prestación de los servicios de salud, el identificar los procesos de las áreas críticas de la institución permitirá medir, gestionar y controlar el riesgo, la disponibilidad, la integridad y la confidencialidad, además de las responsabilidades en aspectos relacionados con la seguridad de los datos clínicos.

- *Tecnología:* para la prestación de los servicios de salud, las instituciones requieren de herramientas, aplicaciones e infraestructura tecnológica que les permita incrementar la eficiencia de los procesos y dado que en la actualidad para el sector salud la tecnología constituye una parte esencial de la infraestructura y un factor crítico para lograr los objetivos y cumplir con la misión, es por ello que es indispensable contar con inventarios de los recursos tecnológicos que permitan identificar los riesgos de seguridad de la información para establecer controles que mejoren las condiciones en que actualmente se encuentran los datos clínicos.

Adicionalmente a estos elementos base la metodología CADERVIM requiere para su implementación dos pilares fundamentales (véase Figura 6.5):

Figura 6. 5 Pilares y objetivo metodología CADERVIM.

Fuente: Elaboración propia

Uno de ellos es contar con una política de gestión de riesgos de seguridad de la información, la cual servirá de apoyo y respaldo a nivel estratégico, para la implementación de la metodología. Los elementos mínimos que deben considerarse para el diseño de la política son:

- Objetivo.
- Roles y responsabilidades del equipo que llevará a cabo la gestión de los riesgos de la institución.
- Definiciones sobre vocabulario en materia de seguridad de la información y riesgos.
- La metodología de riesgos de seguridad que será utilizada por la institución y hacer referencia al documento donde se detalle en profundidad.
- Los criterios de evaluación de riesgos, impacto, aceptación, probabilidad de ocurrencia y severidad de las vulnerabilidades que serán considerados durante la evaluación de los riesgos.
- Se deberán identificar claramente la conexión entre lo establecido en la política para la gestión de riesgos de seguridad y los procesos de planeación estratégica de la institución.
- Hacer referencia al conjunto de indicadores clave para monitorear el comportamiento de los controles implementados como parte del plan de tratamiento de riesgos.
- Establecer los medios que serán requeridos para comunicar los riesgos a los interesados.

- Definir la periodicidad con la cual se llevarán a cabo las evaluaciones de riesgos de seguridad de la información en la institución.

El segundo pilar requerido es la concientización, indispensable para el éxito de la metodología, es por ello que la primera etapa de la metodología CADERVIM está relacionada con la capacitación del personal para lograr la concienciación sobre temas de seguridad de la información y la gestión de los riesgos en los datos clínicos.

Es indudable que los elementos base, los pilares y la metodología CADERVIM interactuando y retroalimentándose constantemente contribuirán en la mejora de la confidencialidad, la integridad y la disponibilidad de los datos clínicos en las instituciones de salud IMSS e ISSSTE en el Distrito Federal.

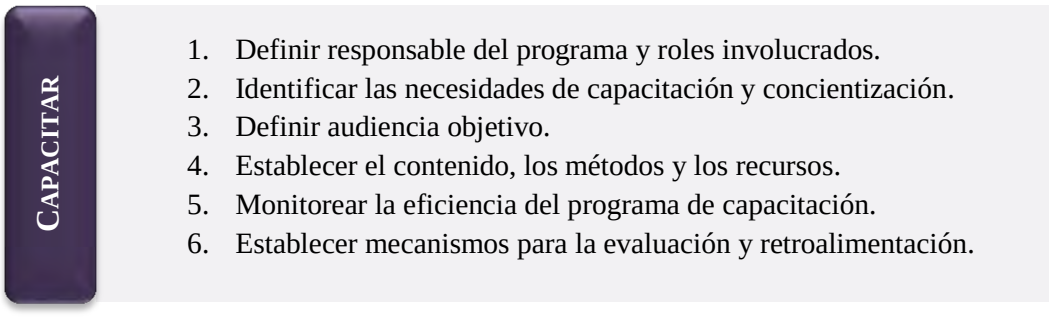
A continuación se presentan cada una de las etapas que conforman la metodología para la gestión de riesgos de seguridad de la información CADERVIM:

6.5.1 CAPACITAR

La metodología CADERVIM inicia con una etapa de capacitación, dada la importancia de educar, formar y concientizar al personal que tiene acceso a los datos clínicos tanto físicos como electrónicos en las instituciones de salud, esto permitirá involucrarlos más a fondo para que comprendan la importancia de proteger la confidencialidad, la integridad y la disponibilidad de los datos clínicos, a los que por su rol dentro de la institución tengan acceso, lo cual facilitará cumplir con las estrategias de seguridad de la información que se hayan establecido, las políticas de seguridad, los procedimientos, las prácticas y que se cuente con los conocimientos que garanticen la adecuada implementación y mantenimiento de los controles estratégicos, tácticos y operativos requeridos para el tratamiento de los riesgos.

Las subetapas que son consideradas para la capacitación se presentan en la figura 6.6 Etapa Capacitar metodología CADERVIM y se describen a continuación:

Figura 6. 6 Etapa Capacitar metodología CADERVIM.



Fuente: Elaboración propia

1. *Definir al responsable del programa y roles involucrados* (directores ejecutivos, personal responsable de los programas de seguridad de la información, dueños de los sistemas y de la información, administradores y personal de soporte de TI, directores de operación y usuarios de sistemas (véase figura 6.7 Definición responsabilidades e involucrados).

Figura 6. 7 Definición de responsabilidades e involucrados.

Rol	Responsabilidades	Nombre	Área a la que pertenece	Contacto
Responsable del programa de capacitación				

Fuente: Elaboración propia

Es importante identificar claramente los roles y basado en ello establecer la capacitación requerida para cada uno, con el objetivo de agrupar roles que requieran capacitación similar y personalizar la capacitación para lograr con ello una mayor eficiencia. Una referencia que puede apoyar al diseño de un programa de capacitación basado en roles se encuentra en la publicación especial del NIST, *Special Publication 800-16 Information Technology Security Training Requirements A Role- and Performance-Based Model*.

2. *Identificar las necesidades de capacitación y concientización*, reunión con las áreas ejecutivas, tácticas y operativas para conocer sus necesidades en temas de seguridad de la información y riesgos. Para llevar a cabo esta actividad pueden utilizarse, algunas técnicas como: entrevistas con los grupos o áreas clave de la institución, encuestas, una evaluación inicial para identificar el nivel de conocimiento que los empleados tienen previo a la capacitación, análisis de los eventos que han afectado a la institución en los últimos años con la finalidad de identificar las brechas existentes y de que forma la capacitación puede contribuir a reducir los incidentes. Como resultado de este rubro se obtendrán las necesidades identificadas, las que actualmente se encuentran cubiertas y la eficiencia de las mismas (véase figura 6.8 Identificar las necesidades de capacitación).

Figura 6. 8 Identificar las necesidades de capacitación.

	Nombre del área	Nombre del titular	Necesidades de capacitación identificadas	Prioridad			Cobertura existente	Eficacia		
				Alta	Media	Baja		Buena	Regular	Mala
Áreas estrategicas										
Áreas tácticas										
Áreas operativas										

Fuente: Elaboración propia

3. *Definir la audiencia objetivo* con la finalidad de diseñar de forma adecuada tanto las sesiones de capacitación como el material que será utilizado como apoyo.

4. *Establecer el contenido, los métodos y los recursos* que serán utilizados para las sesiones que se deriven del programa de capacitación, una vez que se han identificado las necesidades de la institución. Algunos de los temas sugeridos para el desarrollo del plan de capacitación institucional en temas de seguridad de la información para el sector salud son:

   - Importancia de la seguridad de la información en la práctica médica.
   - La seguridad de la información en los datos personales y los datos clínicos.
   - Delitos informáticos.
   - Leyes en México sobre seguridad de la información y delitos informáticos.
   - Leyes en salud y la seguridad de la información.
   - Conociendo las leyes sobre datos personales y su relación con el sector salud.
   - Políticas de seguridad de la información.
   - Responsabilidades sobre la protección de los datos clínicos en la práctica médica.
   - La gestión de riesgos de seguridad de la información en salud.
   - La tecnología en salud y los riesgos de seguridad de la información.
   - La gestión de incidentes de seguridad de la información para la protección de los datos clínicos.
   - El expediente clínico y la seguridad de la información.
   - Roles y responsabilidades sobre la seguridad de la información en salud.
   - Principales amenazas que afectan la seguridad de la información en el sector salud.
   - La clasificación de la información y de los activos en las instituciones de salud.

   Una vez definidos los temas es necesario llevar a cabo la planeación para asignar los tiempos, costos y recursos necesarios (véase figura 6.9 Planeación de los temas de capacitación).

Figura 6. 9 Planeación de los temas de capacitación.

Temas	Duracion	Fecha inicio	Fecha fin	Costo	Responsable	Recursos necesarios	Detalle

Fuente: Elaboración propia

5. *Monitorear la eficiencia del programa de capacitación*. Una vez implementado el programa de capacitación en la institución es necesario monitorear su eficacia, de tal forma que se identifiquen las medidas correctivas y correctivas necesarias que permitan la mejora con el tiempo del programa de capacitación.

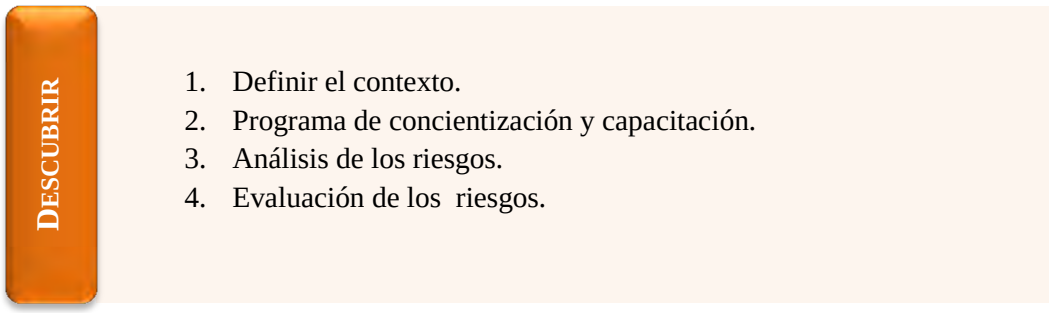
6. *Establecer mecanismos para la evaluación y retroalimentación.* Además deben establecerse mecanismos para la evaluación y retroalimentación del programa de capacitación de seguridad de la información, para ello se puede recurrir a las siguientes técnicas: encuestas, benchmarking, formatos de evaluación, grupos de enfoque, cambios tecnológicos, informes de estado, entrevistas y observaciones independientes.

6.5.2 DESCUBRIR

En esta etapa se obtiene información de la institución sobre su misión, visión, estructura organizacional, procesos y actividades, con la finalidad de identificar el alcance del proceso de gestión de riesgos de seguridad de la información, establecer los activos que serán considerados dentro del alcance y los criterios que serán utilizados durante la evaluación de los riesgos. Además se especifica la forma en que serán analizados y evaluados los riesgos.

Las subetapas que son consideradas para la etapa descubrir se presentan en la figura 6.10 Etapa Descubrir metodología CADERVIM y se describen a continuación:

Figura 6. 10 Etapa Descubrir metodología CADERVIM.



Fuente: Elaboración propia

1. *Definir el contexto.* El objetivo de esta subetapa es conocer más a detalle la institución, como está organizada y la forma de relación existente entre sus diferentes áreas, para llevar a cabo la prestación de los servicios de salud, esta información permitirá identificar el flujo de los datos clínicos, los recursos que son utilizados para su tratamiento, las medidas de seguridad actualmente implementadas y su eficiencia, dando así como resultado el listado de activos, la dependencia con otros recursos y las responsabilidades involucradas para garantizar la confidencialidad, integridad y disponibilidad de los datos clínicos. De manera que una vez que se cuente con esta información, se podrá definir claramente el alcance para el proceso de gestión de riesgos de seguridad de la información y derivado de ello el conjunto de actividades para llevarlo a cabo. Herramientas que pueden contribuir para estas actividades son los mapas de procesos, las entrevistas o reuniones con los responsables de

las diferentes áreas, el análisis FODA (Fortalezas, Oportunidades, Debilidades y Amenazas), los diagramas de flujos de datos y el análisis de dependencia de recursos.
Con la información obtenida a partir de estas y otras herramientas o técnicas se debe completar el siguiente listado (véase figura 6.11 Identificación de procesos y activos).

Figura 6. 11 Identificación procesos y activos.

Tipo de activo	Nombre del activo	Dueño / Área	Clasificación del activo	Requerimientos de seguridad			Importancia	Valor de activo	Controles actuales		
				C	I	D			C	I	D
H			Confidencial	3	2	3	4	12			
S			Reservada	2	1	2	3	8			
R			Pública	1	0	0	2	3			
P			Confidencial	0	2	1	1	4			
S			Reservada	3	3	3	4	13			
O			Pública	2	2	3	3	10			

Fuente: Elaboración propia

Con la información concentrada en este formato, se puede identificar la alineación de los procesos con los objetivos estratégicos de la institución, adicionalmente el área responsable de cada proceso y en su caso la dependencia existente entre ellos, además de la importancia que tiene cada proceso para la operación, el logro de los objetivos y estrategias de la institución, logrando de esta forma determinar claramente los procesos críticos y los activos tanto primarios como de soporte necesarios para llevar a cabo las actividades de cada proceso.
Los criterios que se proponen para evaluar la importancia de un proceso son:

4	**Crítico**	Es el proceso que es fundamental para la operación de la institución, la interrupción de este proceso tendría un impacto catastrófico del cual no podría recuperarse la institución.
3	**Moderado**	Este proceso es necesario para llevar a cabo actividades de la institución, la interrupción de este proceso o servicio puede causar un impacto problemático para la institución.
2	**Bajo**	Este proceso es opcionalmente necesario para llevar a cabo actividades de la institución, la interrupción de este proceso o servicio puede causar un impacto soportable para la institución.
1	**Ninguno**	Proceso que no es tan necesario dentro de la operación, brinda en pequeña parte apoyo a otros procesos, la interrupción del proceso o servicio es imperceptible para la institución.

Una vez identificados los procesos críticos de la institución, se deberá establecer el alcance que tendrá el proceso de gestión de riesgos de seguridad de la información, es recomendable considerando el tamaño de la institución se comience con aquellos procesos y activos críticos que sean utilizados para el tratamiento de los datos clínicos y una vez que

el proceso de gestión de riesgos adquiera madurez ampliar el alcance, hasta lograr la cobertura de otros procesos y activos de la institución.
Es de gran importancia que una vez determinado el alcance se establezca una política para la gestión de riesgos de seguridad de la información, que sea aprobada por el comité de seguridad de la información y personal directivo además de darse a conocer a todo el personal desde niveles estratégicos hasta operativos, con la finalidad de que contribuyan en las actividades derivadas de la implementación de la metodología y como resultado de la misma. La política deberá incluir explícitamente los criterios que serán considerados para la evaluación, aceptación y tratamiento de los riesgos, estos deberán ser revisados y aprobados por el comité de seguridad y los directivos.

Para la metodología CADERVIM propone la definición de los siguientes criterios:

- *Criterio de evaluación de riesgos:* establece la pauta para priorizar los riesgos, para determinar los valores es necesario considerar, el valor estratégico de los procesos, la criticidad de los activos involucrados, los requerimiento legales, regulatorios y contractuales, importancia de la confidencialidad, disponibilidad e integridad en la operación y las expectativas y percepciones de los involucrados, así como las consecuencias en la reputación de la institución.

- *Criterio de impacto:* establece cómo se determinará el impacto que puede causar un evento de seguridad de la información, es decir el grado de daño o costo a la institución generado por el incidente.

- *Criterio de aceptación:* indica la pauta a seguir para aceptar los riesgos e identificar el nivel que la institución está dispuesta a aceptar.

- *Criterio para la probabilidad de ocurrencia:* esta escala indica la probabilidad de ocurrencia de las amenazas, involucra eventos históricos y la posibilidad de que ocurran nuevamente.

- *Criterios para la severidad en vulnerabilidades:* determina la criticidad de la vulnerabilidad, los controles implementados y la facilidad de explotación.

En esta misma etapa deberá quedar claramente establecido y documentado el conjunto de actividades requeridas, la duración de las mismas y los recursos que serán utilizados, definiendo puntualmente para el caso de los recursos humanos los roles y responsabilidades que participarán en el proceso de gestión de riesgos de seguridad, para llevar a cabo esta actividad puede utilizarse la matriz RACI *(Responsible, Accountable, Consulted, and Informed)* esta matriz especifica las actividades y los roles, identificando para cada uno la responsabilidad en términos de quien es el responsable (R), quien debe rendir cuentas (A), quien solo consulta (C) y quien debe ser informado (I).

Para esta matriz puede utilizarse el formato que se presenta en la figura 6.12 Roles y responsabilidades- Matriz RACI:

Figura 6. 12 Roles y responsabilidades- Matriz RACI.

	Funciones			
Actividades	Comité de seguridad	Director de área	Jefe departamento	Dueño información
	R			
	A			
	C			
	I			

Fuente: Elaboración propia

2. *Programa de concientización y capacitación.*

Para llevar a cabo las actividades requeridas por la metodología para la gestión de riesgos de seguridad de la información CADERVIM es necesario apoyarse en el programa de capacitación desarrollado en la etapa Capacitar, logrando de esta forma concientizar al personal de la institución y capacitar al personal que será responsable de llevar a cabo la implementación de la metodología.

3. Análisis de los riesgos.

Una vez identificados los procesos críticos y sus activos serán seleccionados aquellos activos críticos requeridos para el tratamiento de los datos clínicos y se llevará a cabo un análisis más detallado para identificar los requerimientos de seguridad en términos de confidencialidad, integridad y disponibilidad, el dueño del activo, los controles de seguridad que actualmente se tienen implementados para su protección, de tal forma que se identifique un valor para cada activo, dato que permitirá establecer prioridades cuando se lleve a cabo el tratamiento de los riesgos de seguridad.

Para llevar a cabo esta actividad se sugiere el uso del siguiente formato (véase figura 6.13 Valoración de activos críticos):

Figura 6. 13 Valoración activos críticos.

Tipo de activo	Nombre del activo	Dueño / Área	Clasificación del activo	Requerimientos de seguridad			Importancia	Valor de activo	Controles actuales		
				C	I	D			C	I	D
H			Confidencial	3	2	3	4	32			
S			Reservada	2	1	2	3	15			
R			Pública	1	0	0	2	2			
P			Confidencial	0	2	1	1	3			
S			Reservada	3	3	3	4	36			
O			Pública	2	2	3	3	21			

Fuente: Elaboración propia

Para llenar el formato se consideran los siguientes datos:

- *Tipo de activo:* en este rubro serán clasificados los activos con base en la clasificación del estándar ISO 27005, con el objetivo de agruparlos de tal forma que la asignación e implementación de los controles sea más eficiente y efectiva.

H	*Hardware:* en este tipo se incluyen todos los elementos físicos que soportan los procesos. Ejemplo: equipo fijo, medios electrónicos, equipo transportable, equipo de procesamiento de datos, etcétera.
S	*Software*: consiste en todos los programas que contribuyen a la operación o al procesamiento de los datos. Ejemplo: sistemas operativos, software de servicio, paquetería, aplicaciones de la institución, etcétera.
R	*Red:* consiste en todos los dispositivos de telecomunicaciones que son utilizados para la interconexión física y remota de computadoras o elementos de los sistemas de información. Ejemplo: medios y soportes, interfaz de comunicación, etcétera.
P	*Personal:* consiste en todos los grupos de personas involucrados en la operación de los procesos. Ejemplos: tomadores de decisiones, persona de mantenimiento, desarrolladores, etcétera.
S	*Sitio:* todos los lugares incluidos en el alcance y que físicamente son requeridos para operar. Ejemplo: entorno externo, locales, zona, etcétera.
O	*Organización:* describe el marco de la institución, su estructura organizacional. Ejemplo: autoridades, estructura organizacional, organización de proyectos o sistemas, subcontratistas, proveedores y fabricantes, etcétera.

- *Nombre del activo:* en este campo se especifica el nombre con el cual es identificado el activo dentro de la institución.

- *Dueño/Área:* es la persona o rol quien tiene responsabilidad aprobada por la dirección para controlar la producción, desarrollo, mantenimiento, uso y seguridad de activo en cuestión y el área a donde pertenece.

- *Clasificación del activo:* para la clasificación de los activos fue considerado el criterio establecido en la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental (LFTAIPG), confidencial, reservada y pública.

- *Requerimientos de seguridad:* en este apartado se identifican los requerimientos en términos de confidencialidad, integridad y disponibilidad del activo sujeto de análisis considerando los siguientes criterios.

Requerimientos de seguridad de la información

		Confidencialidad	Integridad	Disponibilidad
0	Bajo	Almacena, accede a, transmite, ejecuta, procesa o manipula información con bajos requerimientos de confidencialidad, este es el caso de la información pública.	Almacena, accede a, transmite,ejecuta, procesa o manipula información con bajos requerimientos de integridad, si la exactitud o completitud de la información o el activo se degrada el impacto es menor para la institución.	Almacena, accede a, transmite,ejecuta, procesa o manipula información con bajos requerimientos de disponibilidad, si el activo o la información no esta disponible el impacto es mínimo para la institución.
1	Moderado	Almacena, accede a, transmite, ejecuta, procesa o manipula información con requerimientos de confidencialidad moderados, este es el caso de la información no clasificada pero que requiere un acceso controlado.	Almacena, accede a, transmite,ejecuta, procesa o manipula información con requerimientos de integridad moderados, si la exactitud o completitud de la información o el activo se degrada el impacto es medio para la institución.	Almacena, accede a, transmite,ejecuta, procesa o manipula información con requerimientos de disponibilidad moderado, si el activo o la información no esta disponible el impacto es medio para la institución.
2	Alto	Almacena, accede a, transmite, ejecuta, procesa o manipula información con requerimientos de confidencialidad altos, este es el caso de la información no clasificada con acceso restringido. La divulgación no autorizada podría ocasionar daños a la organización.	Almacena, accede a, transmite, ejecuta, procesa o manipula información con requerimientos de integridad altos, si la exactitud o completitud de la información o el activo se degrada el impacto es alto para la institución.	Almacena, accede a, transmite, ejecuta, procesa o manipula información con requerimientos de disponibilidad altos, si el activo o la información no esta disponible el impacto es alto para la institución.
3	Crítico	Almacena, accede a, transmite, ejecuta, procesa o manipula información con requerimientos de confidencialidad críticos, este es el caso de la información clasificada como reservada o confidencial.	Almacena, accede a, transmite, ejecuta, procesa o manipula información con requerimientos de integridad crítico, si la exactitud o completitud de la información o el activo se degrada el impacto es muy grave para la institución.	Almacena, accede a, transmite, ejecuta, procesa o manipula información con requerimientos de disponibilidad críticos, si el activo o la información no esta disponible el impacto es muy grave para la institución.

- *Importancia:* este valor se obtendrá como resultado del análisis de procesos y activos con base al formato 6.11 Identificación procesos y activos y a los criterios considerados en este apartado.

- *Valor del activo:* el valor del activo será obtenido partir de los valores de los requerimientos de seguridad (confidencialidad, integridad y disponibilidad) y el valor de importancia, mediante la siguiente operación matemática.

$$Valor\ del\ activo = \sum (Requerimientos\ de\ seguridad,\ Importancia)$$

$$Valor\ del\ activo = (C + I + D + Importancia)$$

- *Controles actuales:* en este apartado deberán indicarse y describirse los controles actualmente implementados para proteger la confidencialidad, la integridad y la disponibilidad de los activos, ya que esta información será de utilidad cuando se realice el plan de tratamiento de riesgo y permitirá identificar la eficiencia y eficacia de los controles seleccionados.

4. *Evaluación de los riesgos.*

- *Identificación amenazas y vulnerabilidades:* en este rubro se identifican las amenazas y las vulnerabilidades de cada uno de los activos determinados en la etapa anterior. Una amenaza se define como aquello que puede causar un incidente indeseado, que podría generar un daño para la institución y sus activos, una vulnerabilidad son aquellas debilidades que pueden ser explotadas por una o más amenazas ocasionando eventos no deseados, que pueden resultar en una pérdida, o detrimento o daño de los activos de la institución.
  Los criterios que serán considerados para evaluar las amenazas y vulnerabilidades se presentan a continuación.

Probabilidad ocurrencia de las amenazas

0	**Baja**	El evento es poco probable que ocurra o pudiera ocurrir una vez en un periodo de 3 años. El actor cuenta con escasos conocimientos o habilidades, oportunidad o motivación para explotar la amenaza.
1	**Moderada**	El evento ha ocurrido con anterioridad y existe la probabilidad que ocurra más de una vez en un periodo de 3 años. El actor cuenta con algunos conocimientos, habilidades, oportunidad y motivación para explotar la amenaza.
2	**Alta**	El evento ha ocurrido recientemente y existe la probabilidad de que ocurra por lo menos una vez en un año. El actor tiene altos conocimientos, habilidades, oportunidad y motivación de explotación de la amenaza.
3	**Crítica**	El evento ocurre de forma repetida y es muy probable que siga ocurriendo varias veces durante un semestre. El actor tiene todos los conocimientos, habilidades, oportunidades, motivación de explotación de la amenaza.

Probabilidad ocurrencia de las vulnerabilidades

0	**Baja**	No es probable que pueda ser explotada la vulnerabilidad por la naturaleza de la misma, es de criticidad baja y para descubrirla se requieren altos conocimientos y recursos. No es probable que suceda.
1	**Moderada**	Es relativamente complicado explotar la vulnerabilidad por la naturaleza de la misma, es de criticidad moderada y para descubrirla se requieren ciertos conocimientos y recursos. Es poco probable que suceda.
2	**Alta**	Es relativamente fácil de explotar la vulnerabilidad por la naturaleza de la misma, es de criticidad alta y para descubrirla no se requieren grandes conocimientos ni recursos. Es probable que suceda.
3	**Crítica**	Es fácil de explotar la vulnerabilidad por la naturaleza de la misma, es de criticidad muy alta y para descubrirla no se requieren conocimientos ni recursos. Es altamente probable que suceda.

Algunas de las amenazas que atentan contra la seguridad de la información en los datos clínicos fueron presentadas en el capítulo 3 Sistema de salud en México y de forma adicional el estándar ISO 27005 en sus anexos C y D incluye un listado que puede ser considerado para seleccionar las amenazas y vulnerabilidades que apliquen para los activos identificados.

Cálculo del riesgo: La evaluación del riesgo consistirá en estimar la probabilidad de que las amenazas ocurran y que tan fácilmente puedan ser explotadas, para calcular el riesgo de cada activo se utilizará la siguiente ecuación:

$$Riesgo_{Activo} = Probabilidad\ de\ ocurrencia\ x\ Impacto$$

$$Riesgo_{Activo} = (Prob.\ Amenaza + Prob.\ Vulnerabilidad)\ x\ (C + I + D + Importancia)$$

El riesgo de seguridad para cada activo será calculado mediante la multiplicación de la suma de las probabilidades tanto de la amenaza y la vulnerabilidad por la suma de los valores de los requerimientos de seguridad (confidencialidad, integridad y disponibilidad) más la importancia del activo.
El siguiente formato (véase figura 6.14 Cálculo del riesgo de seguridad para cada activo) puede ser utilizado para concentrar la información de la evaluación de los riesgos de seguridad de la información.

Figura 6. 14 Cálculo del riesgo de seguridad para cada activo.

		PROBABILIDAD DE OCURRENCIA				IMPACTO				
Tipo de activo	Nombre del activo	Requerimientos de seguridad			Importancia	Controles actuales				RIESGO
		C	I	D		Nombre amenaza	Prob. Amenaza	Nombre Vulnerabilidad	Prob. Vulnerabilidad	
H		3			4		3		3	= (A + V) * (C+I+D+Im)
S		2			3		2		2	
R		1			2		1		1	
P		0			1		0		0	
S										
O										

Fuente: Elaboración propia

Una vez calculado el riesgo se realiza la estimación considerando la siguiente matriz y el criterio de estimación (véase figura 6.15 Criterio y matriz para la estimación del riesgo de seguridad).

Figura 6. 15 Criterio y matriz para la estimación del riesgo de seguridad.

Bajo	0 - 24
Medio	24 -48
Alto	49 - 72

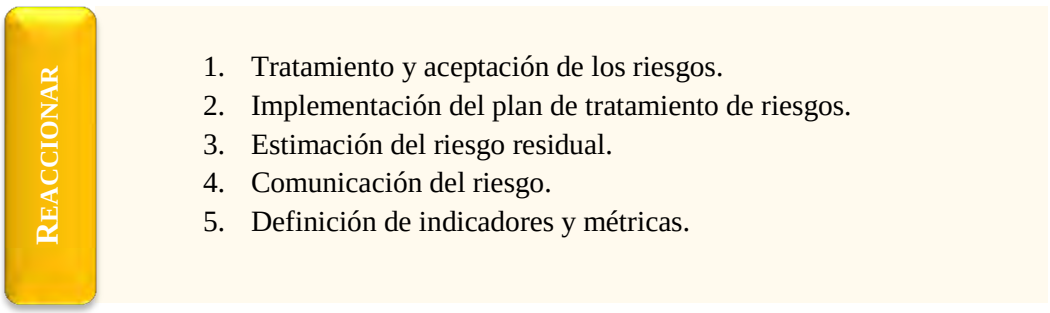
		PROBABILIDAD DE OCURRENCIA						
		0	1	2	3	4	5	6
IMPACTO	0	0	0	0	0	0	0	0
	1	0	1	2	3	4	5	6
	2	0	2	4	6	8	10	12
	3	0	3	6	9	12	15	18
	4	0	4	8	12	16	20	24
	5	0	5	10	15	20	25	30
	6	0	6	12	18	24	30	36
	7	0	7	14	21	28	35	42
	8	0	8	16	24	32	40	48
	9	0	9	18	27	36	45	54
	10	0	10	20	30	40	50	60
	11	0	11	22	33	44	55	66
	12	0	12	24	36	48	60	72

Fuente: Elaboración propia

6.5.3 REACCIONAR

Luego del cálculo del riesgo es importante que la institución defina las acciones y medidas que serán consideradas para el tratamiento de los riesgos de seguridad de la información identificados, estas actividades deben planearse para establecer tiempos, recursos y responsables, de igual forma los resultados obtenidos de proceso de gestión de riesgos deben darse a conocer y contar con métricas para evaluar si las medidas o acciones consideradas fueron eficientes y efectivas, todas estas actividad se llevan a cabo en la etapa reaccionar.
Las subetapas que son consideradas para la etapa reaccionar se presentan en la figura 6.16 Etapa Reaccionar metodología CADERVIM y se describen a continuación:

Figura 6. 16 Etapa Reaccionar metodología CADERVIM.



Fuente: Elaboración propia

1. *Tratamiento y aceptación de los riesgos:* una vez que la institución ha evaluado los riesgos de seguridad de la información, es necesario tomar decisiones sobre cómo serán tratados, dos factores que influyen para la toma de decisiones son: el posible impacto si el riesgo es realizado y que tan frecuente es que esto ocurra, adicionalmente son considerados otros factores como, el deseo de aceptar riesgos (también conocido como tolerancia o apetito de riesgo), la facilidad de implementación del control, los recursos disponibles, las prioridades actuales de la institución y las políticas organizacionales y de gestión.
   Las opciones para el tratamiento del riesgo fueron presentadas en el capítulo 2 Gestión de riesgos de seguridad en el apartado 2.2.4 Tratamiento del riesgo y son: mitigar, aceptar, eliminar y transferir.
   Para llevar a cabo el tratamiento de los riesgos es necesario identificar la forma en que serán tratados, los controles actuales existentes, una evaluación sobre el estado actual de los mismos y los controles que serán propuestos para mejorar la efectividad del control, así como el responsable de su implementación, mantenimiento y mejora. Esta información puede ser recopilada mediante el siguiente formato (véase figura 6.17 Tratamiento de los riesgos de seguridad de la información).

Figura 6. 17 Tratamiento de los riesgos de seguridad de la información.

Tipo de activo	Nombre del activo	RIESGO	Tratamiento del riesgo				Controles actuales	Estado actual	Controles propuestos	Responsable
			Mitigar	Aceptar	Eliminar	Transferir				
H		= (A + V) * (C+I+D+Im)	X							
S				X	X					
R					X					
P						X				
S				X						
O						X				

Fuente: Elaboración propia

Los criterios que serán considerados para la determinar el estado actual de los controles se presentan a continuación:

NE	**No existente**	Se ha identificado como necesario pero no se han tomado medidas para implementarlo. No se cuentan con controles para reducir o mitigar la exposición ante el riesgo.
DO	**Documentado**	Se ha diseñado y planeado el control, se tiene identificadas las medidas y recursos necesarios para implantarlo pero aún no se ha implementado.

IM	**Implementado**	Se ha implementado en la institución el control.
RE	**Registros**	Se cuenta con información que evidencia la implementación y funcionamiento del control.
MO	**Monitoreo**	Se cuenta con medios que permiten determinar y monitorear la eficacia de los controles.
MC	**Mejora continua**	Con los resultados del monitoreo sobre el control, se determinan acciones, con el objetivo de corregir las desviaciones y mejorar la eficiencia.
AU	**Automatizado**	El control requiere de poca o nula intervención del personal ya que esta implementado para funcionar de forma automática por lo que requiere de poca o nula manipulación.

Para la selección de los controles pueden recurrirse a buenas prácticas, marcos de referencia, estándares internacionales como son:

- *ITIL Information Technology Infrastructure Library.*
- *COBIT Control Objectives for Information and related Technology.*
- *NIST Special Publication 800-53 Recommended Security Controls for Federal Information Systems and Organizations.*
- *ISO/IEC 27002 Information technology – Security techniques – Code of practice for information security management*.

2. *Implementación del plan de tratamiento de riesgos:* Por consiguiente una vez que fueron seleccionados los controles que serán aplicados para el tratamiento de los riesgos, se elabora una planeación de las actividades, tiempos y recursos requeridos para implementar los controles en la institución. Para esta actividad se sugiere el uso de herramientas para la gestión de proyectos como son el diagrama de Gantt, que servirá de apoyo para coordinar todas las actividades involucradas en el tratamiento de los riesgos.

3. *Estimación del riesgo residual:* los riesgos residuales son aquellos que permanecen después de implementarse los controles, estos riesgos proporcionan información a los tomadores de decisión para que en evaluaciones de riesgos posteriores, se identifiquen las áreas en las cuales se requieran controles mayores para mitigar aún más los niveles de riesgos y sean llevados a el nivel aceptado por la institución. Para aceptar un riesgo residual la institución debe tomar en cuenta: el cumplimiento regulatorio, su política institucional, la clasificación del activo, los niveles aceptables de riesgo, el costo y eficacia de la implementación. El

cálculo del riesgo residual puede realizarse mediante el cociente entre el valor del riesgo de seguridad una vez que fue implementado el control y el riesgo antes de la implementación del control.

4. *Comunicación del riesgo:* el proceso de gestión de riesgos de seguridad de la información requiere de la retroalimentación y cooperación de todos los niveles de la institución, es por ello que se debe establecer un plan de comunicación que identifique a los actores clave, los tomadores de decisión y la forma en la cual se presentarán los resultados del proceso de gestión de riesgos de seguridad de la información. El plan deberá incluir medios para que la información que sea comunicada siempre este actualizada y sea utilizada para fortalecer la conciencia en materia de seguridad de la información en las instituciones de salud.

   La retroalimentación es un elemento fundamental dentro del plan de comunicación algunas estrategias que pueden ser utilizadas son reuniones con los actores y tomadores de decisión, presentando reportes que contengan recursos visuales como gráficos, cuadros y visiones generales resumidas, además de considerar la existencia de mecanismos para recibir sugerencias, sesiones de lluvia de ideas, etcétera.

5. *Definición de indicadores y métricas:* medir la eficiencia y efectividad de los controles implementados para el tratamiento de los riesgos es vital para el proceso de gestión de riesgos de seguridad de la información. Las mediciones permiten realizar un diseño apropiado, una implementación precisa según las especificaciones y llevar a cabo actividades efectivas para la gestión de los riesgos, incluyendo el establecimiento de metas, la definición de procesos de seguimiento, evaluaciones comparadas (benchmarking) y el establecimiento de prioridades.

   Las mediciones deben contar con una referencia hacia objetivos y metas establecidas por la institución, en definitiva las métricas tienen un propósito único, apoyar las decisiones, el objetivo de medir la efectividad y eficiencia de los controles seleccionados es para proporcionar información sobre la cual se pueda basar la toma de decisiones en materia de seguridad de la información. Las preguntas que deben ser consideradas para el diseño de las métricas son: ¿quién necesita saber?, ¿qué necesita saber? y ¿cuándo necesita saberlo?, es importante que se cuente con métricas que proporcionen información sobre los riesgos de seguridad a cada nivel de la institución, es decir, contar con métricas estratégicas, tácticas y operativas. Otras consideraciones que deben tomarse en cuenta al desarrollar el conjunto de métricas para medir los controles implementados se presentan a continuación:

   - *Predictivas:* puedan proporcionar información de utilidad anticipada.

   - *Manejables:* que los datos que se obtengan como resultado, se puedan condensar, almacenar, ordenar, correlacionar, asimilar y comprender de forma oportuna.

   - *Oportunas:* la información debe tenerse al alcance cuando sea necesaria.

- *Significativas:* los datos obtenidos deben ser comprensibles para el receptor de esta información y proporcionarle una base para tomar las decisiones correspondientes.

- *Inequívocas:* debe ser clara la información que se obtenga como resultado.

- *Confiables:* de gran importancia que los datos obtenidos puedan ser creíbles, ya que de ellos se derivarán decisiones.

- *Realizables:* que la forma de medir pueda llevarse a cabo sin complicaciones o dificultades que impidan la obtención de los resultados.

Para la definición de las métricas puede utilizarse el formato que se muestra en la figura 6.18 Métricas:

Figura 6. 18 Métricas.

Tipo de métrica	Descripción	Objetivo	Cálculo	Frecuencia	Responsable
Estratégicas					
Tácticas					
Operativas					

Fuente: Elaboración propia

Para el diseño de las métricas pueden considerar las siguientes referencias:

- *NIST Special Publication 800-55 Performance Measurement Guide for Information Security.*
- *ISO/IEC 27004 Information technology -- Security techniques -- Information security management -- Measurement*

6.5.4 VIGILAR

1. Monitoreo continuo y revisión de riesgos.

1. Monitoreo continuo y revisión de riesgos:

El proceso de gestión de riesgos de seguridad de la información requiere de un monitoreo congruente y confiable para determinar la eficacia del mismo. Los responsables de los controles deben establecer medidas para monitorear su funcionamiento y a su vez el responsable de la gestión de riesgos de seguridad de la información de la institución debe llevar el control sobre el comportamiento de los riesgos identificados al paso del tiempo.

Llevar a cabo un control de los cambios y de los incidentes de seguridad de la información, puede ayudar a que la institución identifique nuevos riesgos, esta información servirá de entrada para la siguiente evaluación de riesgos de la institución.

Para medir el éxito del proceso de gestión de riesgos de seguridad es necesario definir objetivos cuantificables, monitorear el comportamiento de las métricas más apropiadas y analizar los resultados periódicamente con el objetivo de identificar a tiempo las áreas de oportunidad y definir las acciones preventivas o correctivas.

Para la revisión de los riesgos es recomendable llevar a cabo auditorías tanto internas como externas, los resultados de éstas deben ser dados a conocer a todos los actores involucrados en el proceso de gestión de riesgos de seguridad de la información, para que se tomen las medidas que correspondan.

6.5.5 MEJORAR

1. Mantenimiento y mejoras al proceso de gestión de riesgos de seguridad de la información.

1. *Mantenimiento y mejora al proceso de gestión de riesgos de seguridad de la información.*
   Considerando que la gestión de riesgos es un proceso continuo, se sugiere que se hagan actualizaciones a la evaluación de los riesgos y a los procesos de gestión de riesgos de forma incremental. De manera que el monitoreo regular de los controles de seguridad implementados asegurará su funcionamiento correcto y efectivo, tomando en cuenta, que con el tiempo existe una tendencia al deterioro del rendimiento de los mecanismos. Todas estas actividades deben ser realizadas de forma regular y programada.
   Las actividades de mantenimiento deben incluir: revisiones técnicas de registros, de cumplimiento así como la actualización de políticas y procedimientos.

La metodología para la gestión de riesgos de seguridad de la información CADERVIM tiene por objetivo ser una guía para que las instituciones de salud gestionen los riesgos de seguridad de los datos clínicos, lo que ayudará a mejorar la confidencialidad, integridad y disponibilidad de los mismos durante su tratamiento.

Todos los formatos que fueron presentados pueden consultarse en el Anexo D.

6.6 CALIDAD

La metodología CADEVIM fue diseñada tomando como base metodologías para la gestión de riesgos de seguridad de la información de entidades reconocidas y estándares internacionales, información que fue analizada seleccionando lo mejor de éstas y tomando en cuenta la situación organizacional y las áreas de oportunidad del sector salud en materia de seguridad de la información.

La metodología permitirá a las instituciones de salud mejorar la calidad en el tratamiento de los datos clínicos y mejorar la gestión de sus activos.

A través de la implementación de la metodología CADERVIM se podrá:

- Mejorar los niveles de cumplimiento sobre las leyes aplicables, ya que en su primera etapa la metodología CADERVIM considera la identificación y valoración de la normatividad que deba ser considerada, lo que facilitará las actividades para su cumplimiento.

- Se contará con un listado de roles y responsabilidades que como mínimo serán actualizada cada 6 meses.

- Las instituciones incorporarán un plan anual de capacitación basado en los roles que mejorará la efectividad y eficiencia del aprendizaje lo que contribuirá a mejorar los niveles de concienciación del personal.

- Se tendrá un listado con los procesos y activos asociados a cada proceso, lo que contribuirá a mejorar la implementación del MAAGTIC-SI, facilitando con ello que la implementación pueda lograrse al 100%.

- Se determinará la clasificación de información que permitirá que el 100% de los activos utilizados para el tratamiento de los datos clínicos cuenten con una clasificación y facilitará la selección de los controles para su protección.

- Se llevarán a cabo por lo menos dos evaluaciones de riesgo al año, lo cual permitirá identificar nuevas amenazas y seleccionar formas más efectivas para el tratamiento de los riesgos.

- Serán consideradas en el desarrollo de sistemas de información validaciones para mejorar al 90% la consistencia en los datos clínicos que son ingresados a los sistemas.

- Se contará con un conjunto de métricas e indicadores que permitirán evaluar el 100% de los controles seleccionados.

- Las instituciones contarán con una base de conocimientos que incluyan las lecciones aprendidas evitando así la reincidencia en un 80% de los incidentes que se generen.

- Se llevarán a cabo actividades de monitoreo que permitirán identificar actividades que atenten contra la seguridad de la información de los datos clínicos mejorando en un 90% el control sobre la infraestructura de las instituciones.

CONCLUSIONES

Una vez que se han analizado los resultados de la presente investigación se concluye que el sector salud en México, enfrenta grandes retos por vencer en temas relacionados con la seguridad de la información, que en gran parte se deben a la falta de conciencia por parte del personal sobre la responsabilidad de proteger la confidencialidad, la integridad y la disponibilidad de los datos clínicos, aunado a la resistencia que persiste en el sector en cambiar sus procedimientos y formas de trabajo para incorporar medidas para la protección de la información. Es importante hacer mención que la presencia de nuevos recursos tecnológicos para la prestación de los servicios de salud conlleva no sólo la innovación en aspectos tecnológicos y mejora de servicios, implica a su vez nuevas amenazas que de no ser consideradas a tiempo, pondrían en riesgo la información que estas instituciones tienen en su poder y que utilizan en las actividades diarias, es por ello que el sector salud debe tomar en cuenta la evolución de las técnicas de ataque, las nuevas amenazas y la situación en la que actualmente son tratados los datos clínicos y con estos elementos definir una estrategia interinstitucional para incorporar medidas para protección de la seguridad de la información que estén claramente alineadas a sus objetivos institucionales y fomenten una cultura sobre estos temas en todo el personal, este trabajo previo contribuirá a facilitar la incorporación del expediente clínico electrónico, iniciativa que se mantiene desde el sexenio anterior y que no ha podido ser implementada en su totalidad por diversos factores que han complicado la labor.

La consideración de proteger los datos clínicos, no sólo requiere de esfuerzos por parte del sector salud, además es fundamental que el marco legal sea modificado para incluir la definición puntual de los datos clínicos y los datos genéticos, que hasta la fecha forman parte de los datos personales sensibles, es por ello que es necesario establecer leyes que exijan a las instituciones públicas que ofrecen servicios de salud a la población, una protección más rigurosa para los datos clínicos de los pacientes y que de la misma forma en que a los particulares se les exige y en algunos casos se auditan las medidas implementadas para la protección de los datos personales, de igual forma el sector público de salud sea supervisado para evitar el mal uso de los datos clínicos o incidentes donde se lucre con esta información.

Como resultado del trabajo de campo se pudo observar la gran resistencia que existe por parte del sector salud, en particular de las instituciones IMSS e ISSSTE, para que esta situación sea analizada y solucionada, esto se concluye al percibirse hermetismo o negativas rotundas por parte del personal de las instituciones, al solicitar su apoyo para dar respuesta al instrumento, situación que complicó la aplicación del mismo. Y que si bien existen recursos para la transparencia y acceso a la información pública, aún con ello las instituciones analizadas, no proporcionaron información sobre

estos temas, prueba de esto fue las solicitudes mediante el sistema INFOMEX de las cuales hasta la fecha no se han obtenido respuesta alguna.

Además al visitar las instalaciones de los hospitales, se observó en la mayoría de los casos, que los controles para proteger los expedientes clínicos son deficientes, los recursos tecnológico siguen siendo insuficientes, en algunos casos obsoletos y los tiempos de espera para la atención afectan la calidad de los servicios de salud.

El implementar controles para proteger la seguridad de la información permitirá a las instituciones reducir los incidentes de seguridad, que con base en la investigación realizada, van desde robos de identidad, mal uso de los recursos, robo de medicamentos, hasta desfalcos financieros, lo cual es una clara muestra de la deficiencia en los controles que actualmente están implementados.

Los principales retos que enfrenta el sector salud identificados a partir de la investigación realizada son, la información está dispersa y fácilmente puede verse afectada la confidencialidad, la integridad y la disponibilidad de la misma, es necesario estandarizar procedimientos para que todas las entidades que pertenezcan a la misma institución protejan la información de la misma forma, deben contar con mecanismos para actuar de forma proactiva ante incidentes de seguridad de la información, ya que las instituciones entrevistadas evidenciaron la falta de una metodología para gestionar los riesgos de seguridad de la información y uno de los retos más importantes identificados durante el trabajo de campo, está relacionado con el personal y la necesidad de concientizarlo y capacitarlo en estos temas.

Es por ello que como resultado de la investigación y evaluando las necesidades de las instituciones IMSS e ISSSTE se propone una metodología para gestionar los riesgos de seguridad de la información para la protección de los datos clínicos, lo cual contribuirá a mejorar los controles actualmente implementados. Es importante que los profesionales en seguridad de la información e informática vean en el sector salud, una oportunidad para aplicar sus conocimientos y contribuyan para resolver una problemática que más allá de la tecnología tiene mucho que ver con un problema organizacional y de resistencia al cambio.

Esta investigación busca ser una puerta que abra el camino a nuevas líneas de investigación y profesionales interesados en el tema, es por ello que para contribuir a la difusión, fue presentado este tema en el congreso de seguridad en cómputo 2013 de la Subdirección de Seguridad de la Información de la UNAM (SSI/UNAM-CERT), con la ponencia “Retos en materia de seguridad de la información para el Sector Salud en México”[12] donde se obtuvo una buena respuesta por parte del público asistente, en su mayoría especialistas de seguridad quienes reflexionaron sobre la importancia de proteger los datos clínicos y las consecuencias de no hacerlo.

[12] http://tic.unam.mx/seguridad_sector_salud.html

GLOSARIO

A

activo
Cualquier cosa que tenga valor para la organización. · 10, 53, 130, 140, 141, 142, 143, 144, 145, 148, 200, 201

amenaza
Causa potencial de un incidente no deseado, que pudiera resultar en el daño a un sistema o a la organización. · 9, 10, 22, 38, 39, 44, 48, 49, 51, 53, 71, 72, 73, 74, 75, 129, 130, 143, 145

análisis de riesgo
Uso sistemático de la información para identificar la fuente de riesgo y de estimar el riesgo. · 38

ataque
Tentativas de destruir, de exponer, de alterar, o de inhabilitar un sistema de información y/o información dentro de ella o de violar la política de seguridad. · 10, 32, 72, 154

C

comunicación del riesgo
Proceso continuo o iterativo para la comunicación de riesgo que una organización conduce para proporcionar y para obtener información y mantener un diálogo con las partes interesadas tanto internos como externos con respecto a la gestión del riesgo. · 53, 82, 92, 98, 149

confidencialidad
La propiedad que la información no está hecha disponible ni está divulgada a individuos desautorizados, entidades, o para procesos. · 6, 7, 10, 19, 24, 30, 32, 33, 36, 39, 56, 71, 72, 74, 77, 78, 81, 89, 90, 98, 103, 106, 117, 119, 122, 123, 125, 127, 129, 132, 134, 137, 139, 140, 142, 143, 145, 152, 154, 155, 161, 168, 175, 196

control
Formas de gestión del riesgo, incluyendo, políticas, procedimientos, directrices, prácticas, y estructuras organizacionales que pueden ser de naturaleza administrativa, técnica, gestión o legal. · 8, 19, 20, 21, 29, 30, 35, 51, 52, 58, 72, 74, 78, 79, 94, 116, 118, 124, 147, 148, 149, 151, 153, 168, 187, 190, 192, 194, 196, 197

D

datos
Son resultados de observaciones obtenidas a partir, de mediciones aplicadas a hechos concretos o valores asignados de forma explícita a un objeto o acontecimiento. · 5, 6, 1, 2, 3, 4, 6, 9, 11, 13, 15, 17, 18, 22, 23, 24, 26, 27, 28, 29, 30, 31, 32, 33, 34, 45, 56, 58, 59, 63, 64, 69, 71, 72, 74, 75, 76, 77, 78, 79, 80, 81, 83, 84, 85, 86, 89, 90, 94, 95, 98, 106, 107, 109, 110, 113, 114, 115, 116, 117, 119, 120, 121, 122, 123, 124, 125, 126, 127, 131, 132, 134, 136, 137, 138, 140, 141, 144, 149, 150, 152, 153, 154, 155, 161, 167, 168, 169, 170, 171, 172, 174, 175, 176, 177, 182, 187, 192, 193, 194, 195, 196, 197, 206, 207

disponibilidad
La información que se puede acceder cuando lo requiera el proceso de negocio ahora y en el futuro. · 8, 18, 170

E

evaluación de riesgo
Proceso de comparar el riesgo estimado contra criterios de riesgo para determinar la significación del riesgo · 44

I

impacto
El resultado de un incidente indeseado. · 32, 38, 39, 40, 44, 47, 48, 51, 53, 58, 73, 75, 91, 98, 120, 121, 122, 123, 127, 129, 133, 138, 139, 147, 161

información

Datos seleccionados, han sido analizados, bajo un contexto personal o colectivo, en un momento determinado, adquieren un sentido. · 5, 6, 7, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 13, 14, 17, 19, 20, 21, 22, 24, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 43, 44, 45, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 63, 65, 66, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 89, 90, 91, 92, 93, 94, 95, 96, 97, 98, 104, 105, 106, 107, 109, 110, 111, 112, 113, 114, 115, 116, 117, 118, 119, 120, 121, 122, 123, 124, 125, 126, 127, 128, 129, 130, 131, 132, 133, 134, 135, 136, 137, 138, 139, 140, 141, 143, 144, 145, 146, 147, 148, 149, 150, 151, 152, 153, 154, 155, 161, 167, 168, 169, 170, 171, 172, 173, 175, 176, 177, 182, 183, 185, 186, 187, 188, 190, 191, 192, 193, 194, 195, 196, 197, 200, 201, 204, 205, 207

informática

Hace referencia al manejo de la información, que incluye desde su computación, sistematización, creación, almacenamiento y transmisión · 5, 3, 5, 31, 32, 37, 74, 78, 92, 98, 155, 161, 177, 187, 192, 204

integridad

La propiedad de salvaguardar la exactitud de la información. · 6, 7, 10, 19, 29, 32, 33, 36, 39, 56, 57, 72, 73, 74, 77, 78, 81, 89, 90, 98, 106, 117, 122, 123, 125, 127, 129, 132, 134, 137, 139, 140, 142, 143, 145, 152, 154, 155, 161, 168, 170

M

métrica

Un estándar de medición utilizado en la gestión de actividades relacionadas con la seguridad. · 202

mitigación

La administración de un riesgo mediante el uso de controles y contramedidas. · 116, 130

R

riesgo residual

El riesgo restante posterior al tratamiento del riesgo. · 41, 148, 149

S

seguridad

Se refiere a los resultados obtenidos al implementar y mantener medidas de protección, que permitan a una entidad cumplir con su misión y funciones críticas, no obstante los riesgos existentes en el uso de los sistemas de información. · 1, 5, 6, 7, 1, 2, 3, 5, 6, 7, 8, 10, 11, 13, 17, 19, 20, 21, 22, 27, 29, 30, 31, 32, 33, 34, 36, 37, 38, 39, 41, 43, 44, 45, 48, 49, 50, 51, 53, 54, 55, 56, 57, 58, 59, 61, 63, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 89, 90, 91, 92, 93, 94, 95, 96, 97, 98, 105, 106, 109, 112, 113, 114, 115, 116, 117, 118, 119, 120, 122, 123, 124, 125, 126, 127, 128, 129, 130, 131, 132, 133, 134, 135, 136, 137, 138, 139, 140, 142, 143, 144, 145, 146, 147, 149, 151, 152, 153, 154, 155, 161, 167, 168, 169, 170, 172, 175, 176, 177, 182, 183, 185, 186, 187, 188, 190, 191, 192, 193, 194, 195, 196, 197, 200, 201, 205

seguridad de la Información

La preservación de la confidencialidad, integridad y disponibilidad de la información. · 22, 70, 71, 76, 118, 120, 121, 126, 155, 204, 205, 207

T

tolerancia al riesgo

El nivel del riesgo que la gestión está dispuesta a aceptar y contra cuál se conduce una evaluación de riesgos. · 44

tratamiento del riesgo

Proceso de selección e implementación de los controles para modificar el riesgo. · 41, 42, 44, 147

V

valoración del riesgo

El proceso de ceder el riesgo a otra organización, por lo general mediante la compra de una póliza de seguro o la subcontratación de un servicio. · 130

vulnerabilidad

Una debilidad de un activo o un grupo de activos que puede ser explotado por una amenaza. · 9, 10, 38, 44, 57, 64, 74, 139, 143, 145, 197

ANEXOS

A. Instrumento de medición.

B. Oficio de presentación del estudio.

C. Estudios informacionales.

D. Formatos metodología CADERVIM.

E. Oficio de nombramiento de jurado de tesis.

A. INSTRUMENTO DE MEDICIÓN

CUESTIONARIO: GESTIÓN DE RIEGOS DE SEGURIDAD DE LA INFORMACIÓN EN LOS DATOS CLÍNICOS

FECHA DE APLICACIÓN SEPTIEMBRE – OCTUBRE 2013

Esta investigación tiene fines estrictamente académicos, el presente cuestionario es parte sustancial de un estudio para una tesis de maestría acerca de la seguridad de la información en los datos clínicos. Quisiera solicitar su colaboración para contestar las siguientes preguntas.

INSTRUCCIONES:	Lea cuidadosamente las preguntas, ya que existen algunas en las que sólo se puede responder una opción y otras con varias opciones. El cuestionario está dirigido para directores o jefes de departamento encargados de las oficinas de tecnologías de información, archivo clínico. De antemano: ¡MUCHAS GRACIAS POR SU COLABORACIÓN!
CONFIDENCIALIDAD:	Sus respuestas serán anónimas, absolutamente confidenciales y serán analizadas con fines estrictamente académicos. Además como usted puede ver, en ningún momento se le pide su nombre.

PREGUNTAS:

1. Seleccione la institución de seguridad social a la que pertenece:
   ☐IMSS ☐ISSSTE

2. Indique el número aproximado de derechohabientes que reciben el servicio de salud en la institución de seguridad social a la que pertenece:
   _____

3. Del siguiente listado seleccione las especialidades o subespecialidades que son atendidas en la institución donde labora, en caso de dar atención a otras especifique cuáles son:

   ☐Medicina interna
   ☐Cirugía
   ☐Ginecobstetricia
   ☐Pediatría
   ☐Dermatología
   ☐Neurología
   ☐Neumología
   ☐Oncología
   ☐Cardiología
   ☐Ginecología
   ☐Geriatría
   ☐Traumatología y ortopedia
   ☐Dermatología
   ☐Hematología
   ☐Otras: _____

4. Número aproximado de computadoras de escritorio disponibles para la prestación del servicio de salud en las diferentes especialidades.
   ☐0-50 ☐51- 100 ☐101-150 ☐151-200 ☐más de 200

5. Número aproximado de computadoras portátiles disponibles para la prestación del servicio de salud en las diferentes especialidades.
   ☐0-50 ☐51- 100 ☐101-150 ☐151-200 ☐más de 200

6. Número aproximado de impresoras disponibles para la prestación del servicio de salud en las diferentes especialidades.
   ☐0-10 ☐11- 20 ☐21-30 ☐31-40 ☐más de 40

7. La institución cuenta con infraestructura que permita al personal interno el uso de Internet.
☐SI ☐NO

8. Indique el número aproximado de personas que laboran en la institución:
_____

9. ¿Cuál es el número de personas responsables de las tecnologías de información y comunicaciones (TIC) de la institución?
_____

10. ¿Cuál es el número de personas de TIC, destinado para temas relacionados con la seguridad de la información?
_____

11. ¿Se tienen identificados y documentados los procesos utilizados en la operación de la institución?
☐SI ☐NO

12. ¿Se cuenta con algún listado de recursos críticos en materia de TIC (Tecnologías de Información y Comunicaciones), que sean fundamentales para la operación diaria?
☐SI ☐NO

13. ¿Existe alguna metodología evaluar los riesgos de seguridad de la información?
☐SI ☐NO

14. Del siguiente listado marque las principales amenazas (aquello que pretende causar algún daño) que usted considere afectan la confidencialidad, la integridad y la disponibilidad de los datos clínicos de la institución a la que pertenece:

☐Suplantación por empleados	☐Desconocimiento de actividades por parte de los empleados	☐Errores de los usuarios.
☐Suplantación por proveedores de servicio	☐Fallas en las conexiones o servicios de TI	☐Escases de personal.
☐Suplantación por externos	☐Incorporación de virus, programas maliciosos.	☐Acceso a información privilegiada por personal no autorizado
☐Uso no autorizado de programas y aplicaciones de información de salud	☐Envío erróneo o accidental de información	☐Daños intencionales por personal interno.
☐Introducción de software dañino o perjudicial	☐Fallas generadas por desastres naturales	☐Daños intencionales por personal externo.
☐Mal uso de los recursos de los sistemas	☐Fallas en los sistemas de información de salud	☐Terrorismo
☐Infiltración de las comunicaciones	☐Uso indebido de los recursos de TI.	☐Uso de programas sin licencia para su uso
☐Intercepción de las comunicaciones	☐Errores en el mantenimiento de los equipos de TI.	☐Desconocimiento de leyes en materia de seguridad de la información

15. ¿Existe algún procedimiento sobre cómo se identifican las amenazas y debilidades en materia de seguridad de la información?
☐SI ☐NO

16. ¿Cuál es el enfoque empleado para la evaluación de riesgos en materia de seguridad de la información?
☐Cualitativo (Alto-Medio-Bajo) ☐Cuantitativo (Numérico)

17. Para la valoración de los riesgos de seguridad, ¿Cuentan con matrices de probabilidad de ocurrencia e impacto?
☐SI ☐NO

18. ¿Cuáles de las siguientes opciones para tratar el riesgo conoce? *Puede seleccionar más de una opción.*
☐Reducción ☐Aceptación ☐Evitación ☐Transferencia

19. ¿Se llevan a cabo campañas de concientización para el personal sobre los riesgos de seguridad de la información y sobre las medidas implementadas para su tratamiento?
☐SI ☐NO

20. ¿Cada cuánto tiempo son revisadas las medidas implementados para dar tratamiento a los riesgos de seguridad de la información identificados?
☐Cada 6 meses ☐Cada año ☐Cada dos años ☐Más de dos años ☐No se revisan

21. ¿Cuenta la institución con un manual de políticas de seguridad informática?
☐SI ☐NO

22. ¿El manual de políticas de seguridad informática se encuentra aprobado por el director de la institución?
☐SI ☐NO

23. ¿Se llevan a cabo de forma periódica campañas para la difusión de las políticas de seguridad informática?
☐SI ☐NO

24. ¿La institución cuenta con algún comité para abordar temas relacionados con la seguridad de la información?
☐SI ☐NO

25. ¿Se cuentan con procedimientos especiales en materia de seguridad de la información para personal externo (proveedores)?
☐SI ☐NO

26. Seleccione los inventarios de recursos con los que cuente la institución (*Puede seleccionar más de una opción*):
☐Información ☐Recursos físicos ☐Personal
☐Software ☐Servicios ☐Intangibles

27. ¿La institución cuenta con una clasificación para los diferentes tipos de información?
☐SI ☐NO

28. ¿Se cuentan con distintivos para manejar o etiquetar la información considerando su clasificación?
☐SI ☐NO

29. ¿Se cuenta con algún registro para controlar los accesos a los sistemas de información?
☐SI ☐NO

30. ¿Son considerados los roles al otorgar los privilegios necesarios para el acceso a los sistemas o información?
☐SI ☐NO

31. ¿El personal cuenta con contraseñas para ingresar a los equipos de cómputo y/o sistemas de información?
☐SI ☐NO

32. ¿Se cuentan con mecanismos para controlar el acceso a la red local y/o Internet?
☐SI ☐NO

33. ¿Se cuentan con mecanismos para controlar el acceso a la red local y/o Internet de los dispositivos móviles (smartphones, tablets)?
☐SI ☐NO

34. Del siguiente listado seleccione las normas, leyes o estándares relacionados con la seguridad de la información que conoce y/o que estén implementados en la institución:

Norma-Estándar-Ley	Conoce	Implementada/o
Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental	☐	☐
Ley General de Salud	☐	☐

Reglamento de la Ley General de Salud en Materia de Prestación de Servicios de Atención Médica	☐	☐
NOM-040-SSA2-2004, Norma Oficial de Información en Salud	☐	☐
NOM-004-SSA3-2012, Norma Oficial Del expediente clínico	☐	☐
NOM-024-SSA3-2010 Norma sobre los productos de Sistemas de Expediente Clínico Electrónico	☐	☐
ISO 27001	☐	☐
ISO 27002	☐	☐
ISO 27799	☐	☐
ISO 27005	☐	☐
ITIL	☐	☐

35. ¿Se cuentan con roles y responsabilidades del personal de la institución claramente definidos?
☐SI ☐NO

36. ¿Se realizan de forma periódica programas de capacitación para el personal sobre el uso de los sistemas o sobre la clasificación de información?
☐SI ☐NO

37. ¿Se cuentan con planes para la continuidad del negocio (Plan de Continuidad del Negocio-PCN, Plan de Recuperación de Desastres-PRD)?
☐SI ☐NO

38. ¿Se realizan pruebas a los planes para la continuidad del negocio (PCN-PRD)?
☐SI ☐NO

39. Seleccione los mecanismos para la seguridad de la información que son considerados al desarrollar sistemas de información (*Puede seleccionar más de una opción)*:
☐Validaciones de datos (entrada-salida)
☐Pruebas
☐Cifrado
☐Control de vulnerabilidades
☐Control de versiones

40. ¿Se cuentan con mecanismos para protección contra programas malicioso (virus, gusanos)?
☐SI ☐NO

41. ¿Se llevan a cabo respaldo de la información de equipos de cómputo y de los sistemas de información?
☐SI ☐NO

42. Seleccione los mecanismos físicos utilizados por la institución para protección de la seguridad de la información *(Puede seleccionar más de una opción)*:

☐Puertas en archiveros
☐Cámaras de video vigilancia
☐Escáner corporal
☐Sensores
☐ Controles biométricos en zonas restringidas
☐Bitácoras de registro
☐Custodio (policía)

43. ¿Se cuentan con servicios de apoyo contra fallas eléctricas u otras interrupciones?
☐SI ☐NO

44. ¿Existe algún programa de mantenimiento para los equipos de TI de la institución?
☐SI ☐NO

45. ¿Existen medidas para evitar la fuga de información, o salida de equipos sin autorización?
☐SI ☐NO

46. ¿Existe algún procedimiento para el reporte de incidentes de seguridad de la información?
☐SI ☐NO

47. ¿Existe alguna base de conocimiento sobre los incidentes de seguridad de la información reportados y atendidos?
☐SI ☐NO

AGRADECEMOS SU PARTICIPACIÓN

B. OFICIO DE PRESENTACIÓN DEL ESTUDIO

VNIVERSIDAD NACIONAL AVTÓNOMA DE MEXICO

Facultad de Contaduría y Administración
División de Estudios de Posgrado
Coordinación de la Maestría en Administración

Oficio: FCA/DEP/MAO/089/09/2013

Asunto: Carta de presentación

A QUIEN CORRESPONDA:

Por medio de la presente, hago de su conocimiento que la alumna **Miriam Josefina Padilla Espinosa**, de la Maestría en Administración de la Tecnología y con número de cuenta 301068893, se encuentra realizando una investigación sobre seguridad de la información, a fin de obtener el grado académico correspondiente.

Por lo anterior, solicito a usted su amable disposición para permitirle a la alumna Padilla, aplicar el cuestionario denominado "Gestión de riesgos de seguridad de la información en los datos clínicos", dirigido al personal de los distintos niveles de la organización.

La aplicación de estos cuestionarios podrá realizarse en la forma y momento que usted considere más convenientes y en base a sus reglamentos internos.

Asimismo, hago hincapié en que el objetivo de la investigación y los resultados que se obtengan tienen una finalidad estrictamente académica, por lo que éstos serán manejados de manera confidencial.

Agradezco de antemano la atención que sirva dar a esta solicitud y quedo a sus órdenes para cualquier aclaración al respecto.

Atentamente
"POR MI RAZA HABLARÁ EL ESPÍRITU"
Ciudad Universitaria, D.F., a 23 de septiembre de 2013

EL COORDINADOR

F.C.A. 23 SEP 2013 DIV. DE ESTUDIOS DE POSGRADO

DR. ADRIÁN MÉNDEZ SALVATORIO

Circuito Exterior s/n, Ciudad Universitaria
Delegación Coyoacán, C.P. 04510
Cubículos 17 y 18 del edificio de posgrado de la FCA
Teléfono: 56-22-84-54
Correo electrónico: mao@fca.unam.mx

C. ESTUDIO INFORMACIONAL

1. Introducción
2. Justificación
3. Objetivos
   3.1 Objetivo General
   3.2 Objetivos Específicos
4. Conceptos básicos
   4.1 Estado del arte
   4.2 Gestión de riesgos
   4.3 Seguridad de la información
   4.4 Datos clínicos
5. Desarrollo
   5.1 Fuentes de información consideradas
   5.2 Fuentes de información descartadas
   5.3 Operadores
   5.4 Estrategias de búsqueda
   5.5 Cuadro de estrategias
   5.6 Cuadro bibliométrico
   5.7 Resultados de la búsqueda sobre gestión de riesgos
      5.7.1 Procedimiento
      5.7.2 Análisis de los resultados obtenidos
   5.8 Resultados de la búsqueda sobre seguridad de la información
      5.8.1 Procedimiento
      5.8.2 Análisis de los resultados obtenidos
   5.9 Resultados de la búsqueda sobre gestión de riesgos y seguridad de la información
      5.9.1 Procedimiento
      5.9.2Análisis de los resultados obtenidos
   5.10 Resultados de la búsqueda sobre datos clínicos y seguridad de la información
      5.10.1 Procedimiento
      5.10.2 Análisis de los resultados obtenidos
6 Hallazgos y conclusiones

LA GESTIÓN DE RIESGOS DE SEGURIDAD DEL SECTOR SALUD EN MÉXICO

1. INTRODUCCIÓN

El contenido de este documento muestra los resultados obtenidos para la identificación del estado del arte sobre la gestión de riesgos de seguridad en los datos clínicos, realizado entre octubre y noviembre de 2012.

El estado del arte sobre el tema descrito es generado con la finalidad de conocer la cantidad de información disponible sobre el tema, así como la identificación de corrientes, autores principales, todo ello con el fin de fundamentar de forma adecuada el marco teórico del tema de investigación de tesis.

Los resultados obtenidos fueron generados a partir de una revisión documental, así como una breve de la información encontrada, además mediante el uso de indicadores bibliométricos fue posible refinar las estrategias de búsqueda con el objeto de identificar información que fuera relevante para el tema tratado.

La exploración documental fue realizada en bases de datos que indexan contenidos relacionados con las ciencias sociales, ingeniería y salud, también se recurrió a la consulta de bases de datos restringidas, utilizando el acceso otorgado por la UNAM y buscadores comerciales.

El presente estudio informacional presenta la justificación del mismo, los objetivos de la investigación, los conceptos básicos del tema tratado y el desarrollo de las estrategias de búsqueda utilizadas, así como la descripción de las fuentes de consulta utilizadas y las que fueron descartadas.

Se indican las estrategias de búsqueda, se presenta el cuadro bibliométrico y con base en los resultados obtenidos se genera el reporte sobre los hallazgos y conclusiones.

2. JUSTIFICACIÓN

Considerando que los datos clínicos de los pacientes en los centros que brindan atención médica no sólo incluye datos personales que deben ser protegidos según lo establece la Constitución Política de los Estados Unidos Mexicanos en su artículo 16 y la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, sino además de ello incluye información sobre el estado de salud y tratamiento de cada uno de los pacientes, los cuales son considerados como datos sensibles que deben ser protegidos para evitar el mal uso de esta información que violen el derecho a la privacidad de los pacientes.
Por ello es fundamental que los centros que brindan atención médica, hospitales, clínicas y centros de salud identifiquen los riesgos a los cuales están expuestos los datos clínicos, así como definir medidas para cumplir con los objetivos de seguridad de la información como son, la confidencialidad, la integridad, la autenticación, el control de acceso, el no repudio y la disponibilidad.
La adopción en algunos hospitales, clínicas y centros de salud de tecnologías de la información contribuye sin duda a mejorar la prestación del servicio a los usuarios, sin embargo el uso de estos recursos también implica contar con una sólida cultura en materia de seguridad de la información, considerando que los bancos de datos ya no sólo estarán en formatos físicos como pueden ser los expedientes que generalmente se almacenan en el archivo clínico de la dependencia, ya que hoy en día algunos hospitales cuentan con sistemas que les permiten el acceso y edición de expedientes electrónicos. Lo cual sin duda representa un gran riesgo considerando que algunos de los usuarios que acceden a estos sistemas no cuentan conocimientos de los posibles riesgos que pudieran afectar o comprometer la información, lo cual representa un riesgo latente.

Bajo este escenario es fundamental que todo el personal que manipula la información este consiente de las principales amenazas que afectan la seguridad de la información de los datos clínicos, lo cual permitirá una vez considerando el grado de severidad y de ocurrencia identificar los posibles riesgos y una vez identificados definir las estrategias a seguir para su tratamiento, todo esto realizado a través de una metodología para la gestión de riesgos de seguridad de la información.

3. OBJETIVOS

3.1 Objetivo General

Identificar el estado del arte de la gestión de riesgos y la relación con la seguridad de la información de los datos clínicos en la base de datos del *Institute for Scientific Information (ISI)*.

3.2 Objetivos Específicos

a) Realizar el estudio informacional sobre la gestión de riesgos de seguridad en la información clínica.
b) Analizar los resultados obtenidos para identificar áreas de oportunidad.
c) Identificar autores y teorías principales sobre la gestión de riesgos y la seguridad de la información.
d) Visualizar como es la distribución de la generación de conocimiento sobre el tema en todo el mundo.

4. CONCEPTOS BÁSICOS

4.1 Estado del arte

El estado del arte se define como el recorrido que se realiza para conocer y sistematizar la producción científica en una determinada área de conocimiento, con el objetivo de conocer lo que se produjo respecto a determinado tema y que permita la recuperación de conceptos, teorías, metodologías, autores, perspectivas desde las cuales se interrogará al objeto de investigación que se está construyendo *(Souza, 2005)*.

4.2 Gestión de riesgos

La gestión de riesgos de seguridad es una parte fundamental dentro de la gestión estratégica de cualquier empresa y está definido como el proceso mediante el cual las empresas tratan los riesgos relacionados con sus actividades, con el fin de obtener un beneficio sostenido, el riesgo puede ser definido como la combinación de un suceso y las consecuencias que implica *(FERMA, 2003)*.

La gestión de riesgos de seguridad brinda protección y adiciona valor a la empresa, las instituciones y a sus interesados mediante el apoyo a los objetivos definidos, lo cual es logrado a través de:

- Provee una estructura que permite que las actividades futuras sean desarrolladas de forma consistente y controlada.
- Mejora la toma de decisiones, el proceso de planificación y establecimiento de prioridades ya que brinda una visión integrada y estructurada de la entidad, así como volatilidad, oportunidades y amenazas del proyecto.

- Permite una asignación más eficiente del capital y de los recursos dentro de la organización.
- Reduce la volatilidad en las áreas que no están relacionadas con el core de la entidad.
- Desarrolla y apoya a los empleados y la base de conocimiento de la entidad.
- Optimiza la eficiencia operacional.

4.3 Seguridad de la información

La seguridad de la información con base en la definición del NIST *National Institute of Standards and Technology (NIST, 2011)* se considera como la protección de la información y de los sistemas de información de accesos no autorizados, uso, divulgación, alteración, modificación o destrucción con el fin de proporcionar:

a) *Integridad:* lo que significar protección contra la información incorrecta, modificación o destrucción de la misma, incluye el no repudio y la autenticación.
b) *Confidencialidad:* considera que la información este restringida y que solo los usuarios autorizados puedan tener acceso a ésta, incluye medio para protección de la privacidad personal y de la información confidencial
c) *Disponibilidad:* significa garantizar el acceso oportuno y confiable para el uso de la información.

La ley Federal de Seguridad Privada en México establece que la seguridad de la información consiste en la preservación, integridad y la disponibilidad de la información del titular, a través de sistemas de administración de seguridad, de bases de datos, de redes locales, corporativas y globales, sistemas de cómputo, transacciones electrónicas, así como el respaldo y la recuperación de dicha información ya sea en formato documental, electrónico y multimedia *(LFSP, 2011)*.

4.4 Datos clínicos

En las disposiciones sanitarias actuales no se encuentra definido el término de datos clínicos, aunque puede obtenerse una definición a partir de lo establecido en el artículo 32 de la Ley General de Salud, en el cual se define como la atención médica al conjunto de servicios que se proporcionan al individuo, con la finalidad de proteger, promover y restaurar su salud, la cual podrá apoyarse de medios electrónicos con base en las normas oficiales que sean expedidas por la Secretaría de Salud, lo cual da origen a la *Norma Oficial del Expediente Clínico NOM-168-SSA-1-1998 ahora NOM-004-SSA3-2012 del Expediente Clínico*, con base en esta información los datos clínicos pueden definirse como el conjunto de información sobre el origen, evolución y estado actual del binomio salud-enfermedad de una persona, identificada o identificable..

5. DESARROLLO

5.1 Fuentes de información consideradas

La figura 1 presenta las fuentes de información y una breve descripción de las mismas, fuentes que fueron consideradas en la búsqueda y que mejores resultados ofrecieron, por su relevancia con el tema de investigación.

Figura 1: Tabla de fuentes de información consideradas en la búsqueda

Nombre de la Base de datos	Descripción
1. IEEE Xplore digital library	Base de datos especializada en las áreas de ingeniería eléctrica, computación y electrónica, permite acceder al texto completo de las publicaciones científicas y técnicas elaboradas por el *Institute of Electrical and Electronics Engineers* (IEEE) y sus socios editoriales, contiene más de dos millones de artículos de más de 12,000 publicaciones que incluyen: revistas, actas de congresos, y las normas técnicas, con contenidos seleccionados que se remontan a 1893. **Tipo de acceso:** restringido (acceso mediante la BIDI Biblioteca Digital de la UNAM) **Sitio web de acceso:** http://www.dgbiblio.unam.mx/index.php/catalogos
2. Web of Knowledge	Herramienta especializada en el área de las ciencias que ofrece acceso a referencias bibliográficas, citas a trabajos publicados y resúmenes, información del autor, etc. Su actualización es semanal y ofrece información de más de 5,800 revistas científicas. **Tipo de acceso:** restringido (acceso mediante la BIDI Biblioteca Digital de la UNAM) **Sitio web de acceso:** http://www.dgbiblio.unam.mx/index.php/catalogos
3. Health business full text	Provee el acceso en línea al texto completo de más de 130 publicaciones sobre administración de la salud, y aspectos no clínicos de la administración de instituciones de cuidados de la salud. Con la cobertura en los siguientes temas: administración de hospitales, representación de hospitales, mercadotecnia, recursos humanos, tecnología computacional, seguros. **Tipo de acceso:** restringido (acceso mediante la BIDI Biblioteca Digital de la UNAM) **Sitio web de acceso:** http://www.dgbiblio.unam.mx/index.php/catalogos
4. EBSCO Academic	Contiene miles de títulos de publicaciones periódicas en texto completo, y publicaciones arbitradas, de múltiples disciplinas académicas, Además, ofrece índices y resúmenes de más de 11,600 publicaciones especializadas y un total de más de 12,200

Figura 1: Tabla de fuentes de información consideradas en la búsqueda (Continuación)

	publicaciones diversas, entre las que se incluyen monografías, informes y conferencias. **Tipo de acceso:** restringido (acceso mediante la BIDI Biblioteca Digital de la UNAM) **Sitio web de acceso:** http://www.dgbiblio.unam.mx/index.php/catalogos
5. JSTOR	Recurso de información que ofrece acceso en línea a los archivos retrospectivos, tal como fueron publicados en su versión original, de más de 1,000 títulos de revistas y publicaciones académicas y de investigación de los ámbitos de las ciencias sociales, las humanidades y las diversas ramas de la ciencia, así como monografías y otros materiales valiosos para el trabajo académico. **Tipo de acceso:** restringido (acceso mediante la BIDI Biblioteca Digital de la UNAM) **Sitio web de acceso:** http://www.dgbiblio.unam.mx/index.php/catalogos
6. Safety science and risk	*Science and risk*, publicada en asociación con la Universidad del Sur de California y la Universidad de *Waterloo, Safet*, ofrece citas y resúmenes de la información completa y oportuna sobre el área de la salud pública, seguridad e higiene industrial. **Tipo de acceso:** restringido (acceso mediante la BIDI Biblioteca Digital de la UNAM) **Sitio web de acceso:** http://www.dgbiblio.unam.mx/index.php/catalogos
7. Dialnet	Plataforma de recursos y servicios documentales su objetivo es brindar acceso a literatura científica hispana a través de Internet **Sitio web de acceso:** http://dialnet.unirioja.es/
8. UC Library	Buscador de la Universidad de California que ofrece búsquedas en las bibliotecas de UC y en las bibliotecas del mundo, su motor de búsqueda se denomina Melvyl. **Tipo de acceso:** Libre **Sitio web de acceso:** http://melvyl.worldcat.org/
9. Google académico	Es un buscador de Google especializado en artículos de revistas científicas, enfocado en el mundo académico, y soportado por una base de datos disponible libremente en Internet que almacena un amplio conjunto de trabajos de investigación científica de distintas

Figura 1: Tabla de fuentes de información consideradas en la búsqueda (Continuación)

	disciplinas y en distintos formatos de publicación. **Tipo de acceso:** libre **Sitio web de acceso:** http://scholar.google.com.mx

Nota: Elaboración propia

5.2 Fuentes de información descartadas

Una vez realizadas las búsquedas con las estrategias identificadas y al analizar los resultados obtenidos las siguientes fuentes no brindaron resultados satisfactorios, por lo cual fueron descartadas. La información de las fuentes descartadas se presenta en la figura 2.

Figura 2: Tabla de fuentes de información descartadas.

10. MIT Library	Este sitio brinda un catálogo de recursos de las Bibliotecas del MIT (*Massachusetts Institute of Technology*), se cuentan con diversos materiales como son 2.6 millones de volúmenes impresos, 20,000 revistas periódicas, CD´s, recursos en línea, etcétera. Tipo de acceso: **Libre** Sitio web de acceso: **http://library.mit.edu**
11. Redalyc	Hemeroteca científica en línea de acceso libre, reúne revistas científicas de América Latina y el Caribe, España y Portugal. **Tipo de acceso:** Libre **Sitio web de acceso:** http://redalyc.uaemex.mx

Nota: Elaboración propia

5.3 Operadores

Los operadores utilizados para realizar las búsquedas se presentan en la figura 3.

Figura 3: Tabla de Operadores utilizados en las búsquedas.

Operador	Descripción
“ “	Los documentos deben contener la frase exactamente como se definió entre las comillas.
?	Signo de interrogación de cierre. Se usa como un comodín de una sola letra.
AND	Debe incluir la palabra en todos los resultados.
OR	Los documentos deben incluir por lo menos una palabra de las que se tienen como alternativas.
Acento	Si se incluye sólo arrojará los resultados en donde la palabra objetivo se encuentre acentuada, en los buscadores comerciales si se omite arrojará resultados que incluyan palabras acentuadas.

Figura 3: Tabla de Operadores utilizados en las búsquedas. (Continuación)

Mayúsculas-Minúsculas	Son indistintas al realizar las búsquedas
Ordenamiento	En el caso de los buscadores comerciales se considera relevante el orden en que se colocan las palabras a buscar.
Fecha	En algunos buscadores se puede configurar esta opción para modificar el rango de búsqueda considerando la fecha.

Nota: Elaboración propia

5.4 Estrategias de búsqueda

Dado que las bases de datos consultadas en algunas ocasiones no arrojaron resultados utilizando el idioma español se realizó la búsqueda en el idioma inglés, en la figura 4 se específica la estrategia utilizada según el idioma y la base de datos.

Las bases de datos consultadas fueron:

1. IEEE Xplore digital library
2. Web of Knowledge
3. Health business full text
4. EBSCO Academic
5. JSTOR
6. Safety science and risk
7. Dialnet
8. UC Library
9. Google académico
10. MIT Library
11. Redalyc

5.5 Cuadro de estrategias

Figura 4 Cuadro de estrategias de búsqueda

	ESTRATEGIAS	BASES DE DATOS											DESCRIPCIÓN
		1	2	3	4	5	6	7	8	9	10	11	
a	"gestion de riesgos" OR "administración de riesgos"			X	X			X	X	X		X	Estrategia que se define con el objeto de identificar toda la información disponible sobre la gestión o administración de riesgos.
	"risk management"	X	X			X	X				X		
b	"seguridad de la información" and ("gestion de riesgos" OR "administración de riesgos")			X	X			X	X	X		X	Esta estrategia tiene como objetivo identificar la información disponible sobre la administración o gestión de riesgos enfocada a la seguridad de la información.
	"information security" and ("risk management")	X	X			X	X				X		
c	mexico and "seguridad de la información" and ("gestion de riesgos" OR "administración de riesgos")			X	X			X	X	X		X	Esta estrategia busca la identificación de información existente sobre la gestión de riesgos de seguridad de la información relacionada con México.
	mexico and "information security" and ("risk management")	X	X			X	X				X		
d	proteccion AND "datos personales" AND "México"			X	X			X	X	X		X	Mediante esta estrategia se pretende identificar toda la información disponible sobre la protección de datos personales en México.
	protection AND "personal data" AND "Mexico"	X	X			X	X				X		
e	"administración de riesgos" and "datos personales" and mexico			X	X			X	X	X		X	Esta estrategia busca identificar la información disponible sobre la administración de riesgos y los datos personales.
	"risk management" and "personal data" and mexico	X	X			X	X				X		
f	datos personales confidencialidad mexico OR "seguridad de la información" OR "política de salud" AND "sistema de salud en México"			X	X			X	X	X		X	Mediante esta estrategia se busca identificar información sobre los datos personales, políticas de salud, el sistema de salud en México.
	Privacy Policy mexico OR "information security" OR "health policy" AND "health system in Mexico"	X	X			X	X				X		
g	"seguridad de la información"			X	X			X	X	X		X	Estrategia para obtener toda la información disponible sobre la seguridad de la información.
	"information security"	X	X			X	X				X		
h	"seguridad de la información" AND M?exico			X	X			X	X	X		X	Estrategia para obtener toda la información disponible sobre la seguridad de la información en México.
	"information security" and mexico	X	X			X	X				X		
i	sistema de salud en México			X	X			X	X	X		X	Estrategia para obtener toda la información disponible sobre el sistema de salud en México.
	health system in Mexico	X	X			X	X				X		
j	"administración de riesgos" and "seguridad de la información"			X	X			X	X	X		X	Estrategia para obtener la información sobre administración de riesgos vinculada a la seguridad de la información.
	"risk management" and "information security"	X	X			X	X				X		
k	"seguridad de la información" and "expedientes medicos"			X	X			X	X	X		X	Esta estrategia busca obtener la información disponible sobre la seguridad de la información vinculada con los expedientes médicos.
	"information security" and "medical records"	X	X			X	X				X		
l	seguridad de la información and "expedientes medicos" and "mexico"			X	X			X	X	X		X	Esta estrategia busca obtener la información disponible sobre la seguridad de la información vinculada con los expedientes médicos en México.
	information security and "medical records" and "mexico"	X	X			X	X				X		
m	proteccion AND "datos personales"			X	X			X	X	X		X	Esta estrategia pretender obtener toda la información disponible sobre los datos personales y la protección de los mismos.
	protection AND "personal data"												
n	"datos clinicos" AND "seguridad de la información"			X	X			X	X	X		X	Esta estrategia tiene por objetivo identificar información que vincule la seguridad de la información con el área de salud específicamente con los datos clínicos.
	"clinical data" AND "information security"	X	X			X	X				X		

5.6 Cuadro bibliométrico

A continuación se presentan en la figura 5, los resultados obtenidos sobre la producción de documentos científicos relacionados con los temas de gestión de riesgos, seguridad de la información y datos clínicos, se consideraron las bases de datos y estrategias definidas en el apartado anterior.

Figura 1 Cuadro bibliométrico.

Base de datos	a	b	c	d	e	f	g	h	i	j	k	l	m	n
1. IEEE Xplore digital library	20,795	2,084	70	68	4	0	33,130	761	0	2,084	499	0	1,849	112
2. Web of Knowledge	1,438	23	0	1	0	993	750	3	44	110	22	4	12	4
3. Health business fulltext	18,825	395	0	30	1	0	1,469	45	1	110	172	6	0	49
4. EBSCO Academic	*80*	*2*	*0*	*38*	*0*	*31*	*1,671*	*6*	*31*	*448*	*219*	*448*	*120*	*60*
5. JSTOR	*11,389*	*44*	*7*	*204*	*34*	*603*	*131*	*17*	*7614*	*44*	*17*	*270*	*996*	*6*
6. Safety science and risk	4,843	18	27	0	0	0	122	0	106	18	1,607	0	21	7
7. Dialnet	53	8	1	27	0	0	1,392	30	104	16	0	0	9	13
8. UC Library	4,013	29	19	2,233	3	1,492	749	413	137	21	1	34	2,645	26
9. Google académico	11,500	516	170	6,490	71	33	6,630	1,540	658	223	14	1	11,800	1,440
10. MIT Library	2,680	32	0	0	0	0	767	3	71	32	2	0	0	0
11. Redalyc	2	0	0	0	0	0	4	0	0	0	0	0	0	0

Nota: Elaboración propia

Del cuadro bibliométrico se marcan en color **azul** aquellas bases de datos que brindaron información de mayor utilidad, con mayor enfoque sobre el tema y donde la mayoría de las estrategias definidas arrojaron información útil, los resultados marcados en color **verde** indican que los resultados obtenidos de estas bases son útiles pero en algunos casos no tienen tanta relevancia o relación con el tema abordado en la investigación, el caso de los resultados en color **naranja** indica que las bases fueron descartadas porque no arrojaron resultados útiles y en la mayoría de los casos no se encontraba información sobre el tema de interés.

Para el análisis de los índices bibliométricos se consideró la base de datos **Web of Knowledge** con las estrategias **a**, **g**, **j** y **n**, a y g que fueron seleccionadas considerando que servirán de referencia para la elaboración del marco teórico sobre gestión de riesgos y seguridad de la información, la estrategia j fue seleccionada ya que sus resultados brindan información que relaciona la gestión de riesgos con la seguridad de la información y por último la estrategia n fue considerada ya que relacionada los el concepto de seguridad de la información con los datos clínicos en especial esta estrategia presenta pocos resultados y analizando la información que proporciona fue la más aproximada con el tema a investigar.

5.7 Resultados de la búsqueda sobre gestión de riesgos

5.7.1 Procedimiento

Los datos analizados fueron obtenidos de la base de dados del Institute for *Scientific Information (ISI)* mediante el recurso electrónico *Web of Knowledge* y de forma específica en la base de datos Social Science Citation Index, el acceso a este recurso fue realizado desde la Universidad Nacional Autónoma de México.

La búsqueda se realizó por tema, utilizando la palabra clave "risk management" y el operador "", en idioma inglés ya que no se obtenían resultados en español. El periodo en años que fue considerado es de 2008 a 2012.

Fueron seleccionadas para el análisis las siguientes referencias.

- Article
- Proceedings paper
- Book chapter

De los resultados obtenidos se realizó un filtrado por áreas para enfocar al tema de interés, los cuales con presentados a continuación.

- *Management.*
- *Business*
- *Health Care Sciences Services*
- *Health Policy Services*
- *Medical Informatics*

Se incluyeron áreas de gestión y negocios para identificar orígenes, teorías y metodologías de la gestión de riesgos y se incluyeron áreas médicas e informáticas para obtener alguna información que pudiera vincular la administración de riesgos con la salud o la seguridad informática.

La consulta realizada en la base de datos se muestra a continuación:

Topic=("risk management")

Refined by: Document Types=(ARTICLE OR PROCEEDINGS PAPER OR BOOK CHAPTER) AND Web of Science Categories=(MANAGEMENT OR HEALTH CARE SCIENCES SERVICES OR MEDICAL INFORMATICS OR BUSINESS OR HEALTH POLICY SERVICES) AND Publication Years=(2008 OR 2010 OR 2009 OR 2011 OR 2012)

Timespan=All Years. Databases=SCI-EXPANDED, SSCI, A&HCI, CPCI-S, CPCI-SSH.

Lemmatization=On

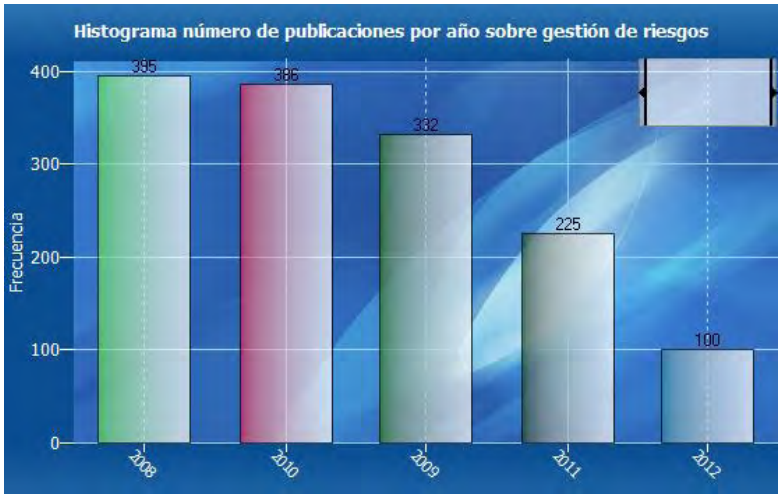
Los resultados obtenidos mediante esta búsqueda indican **1,438** registros los cuales al ser analizados presentan la siguiente información.

5.7.2 Análisis de los resultados obtenidos

A continuación se presenta el análisis de los resultados obtenidos considerando los siguientes puntos.

- **Publicaciones por año**

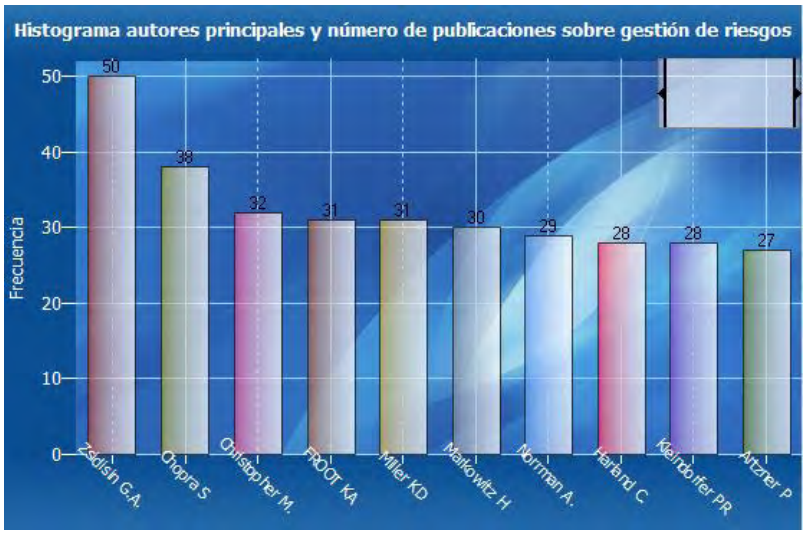
Figura 6 Histograma del número de publicaciones por año



De la gráfica se puede observar que 2008 y 2010 fueron los años con mayor número de publicaciones relacionadas con la gestión de riesgos.

- **Diez autores principales**

Figura 7 Histograma de los 10 autores con el mayor número de publicaciones de 2008 al 2012



De la gráfica se puede observar que Zsidisin G.A. es el autor con mayor número de publicaciones sobre gestión de riesgos en el periodo de 2008 y 2012.

- **Distribución de las publicaciones por país**

El siguiente cuadro presenta la distribución de las publicaciones por país y considerando que por lo menos se tengan 3 publicaciones en el periodo de 2008 a 20012.

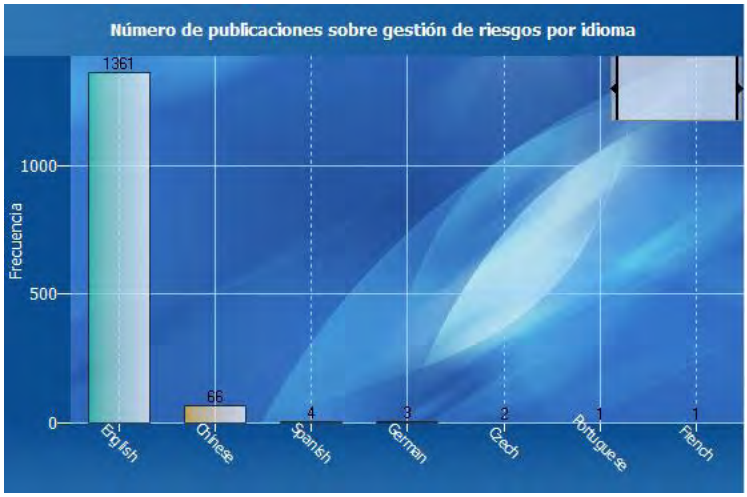
Figura 8: Distribución de las publicaciones por país con al menos 3 publicaciones entre 2005 y 2012

País	Número de publicaciones	País	Número de publicaciones
China.	676	Wales.	10
USA.	130	Finland.	10
England.	94	Norway.	9
Australia.	51	Singapore.	8
Canada.	45	Sweden.	8
Germany.	39	Portugal.	7
Romania.	35	Malaysia.	7
Taiwan.	34	Denmark.	7
Netherlands.	33	Belgium.	6
Italy.	26	Greece.	6
Switzerland.	20	U Arab Emirates.	6
France.	19	Pakistan.	5
Spain.	18	New Zealand.	5
Turkey.	13	Slovakia.	5
India.	13	Poland.	4
South Africa.	13	Serbia.	4
Lithuania.	12	Czech Republic.	4
Brazil.	11	Ireland.	4
Iran.	11	Israel.	3
Scotland.	11	North Ireland.	3
Japan.	11	Croatia.	3
South Korea.	11	Cyprus.	3
Austria.	10		

Del presente cuadro se observa que los seis países que han generado más publicaciones sobre gestión de riesgos entre el 2008 y el 2012 son China, USA, Inglaterra, Australia, Canadá y Alemania.

- **Distribución por idioma**

Figura 9: Distribución del número de publicaciones por idioma



De la gráfica se observa que el idioma predominante en las publicaciones es el inglés, seguido con menor número de publicaciones el chino.

- **Diez revistas con el mayor número de publicaciones**

Figura 10: Diez revistas con el mayor número de publicaciones entre el 2008-2012

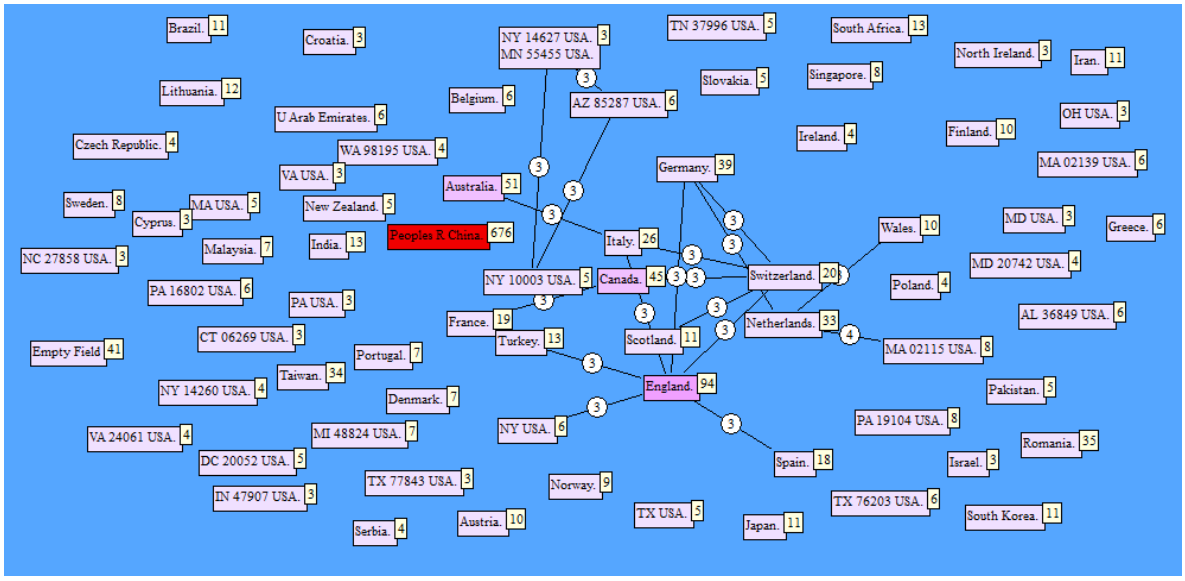
Publicación	Número de publicaciones
1. European journal of operational research	52
2. EBM 2010: international conference on engineering and business management, Vols 1-8	47
3. Proceedings of 2008 international conference on risk and reliability management, Vols I and II	40
4. Proceedings of the 1st international conference on sustainable construction & risk management, Vols I and II	36
5. Disaster prevention and management	30
6. Proceedings of the 2nd international conference on risk management & engineering management, Vols 1 and 2	28
7. African journal of business management	24
8. Chinese perspective on risk analysis and crisis response	22
9. Proceedings of the 3rd international conference on risk management & global e-business, vols I and II	21
10. International Journal of Project Management	20

- **Mapa de publicaciones por país**

A continuación se muestra el mapa de publicaciones por país sobre gestión de riesgos en el periodo del 2008 al 2012.

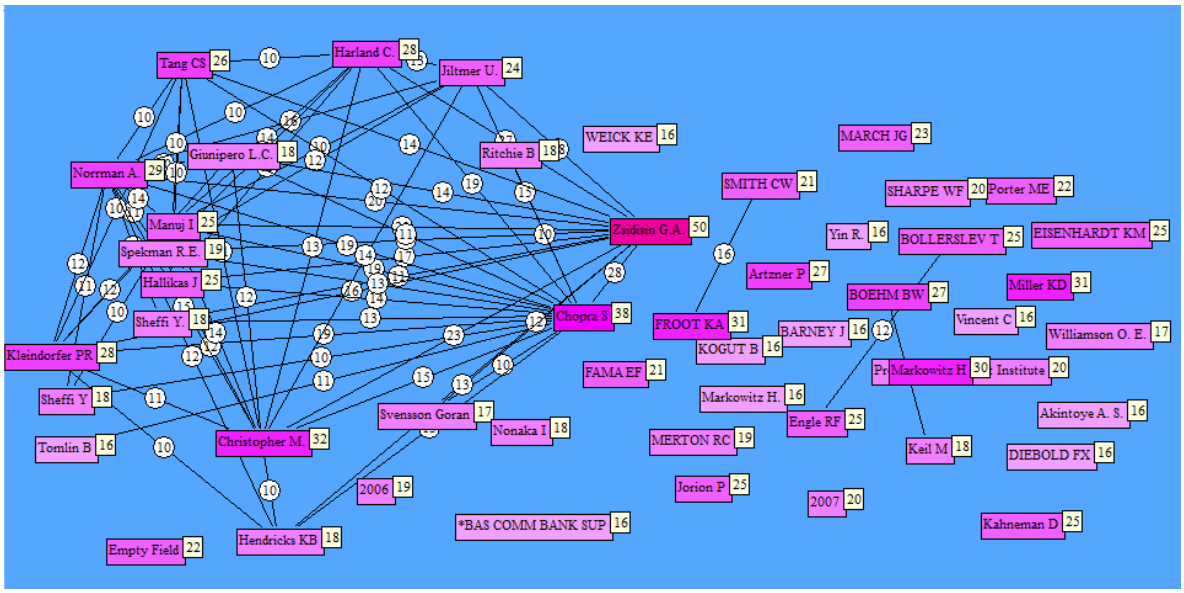
Del mapa puede observarse el dominio por parte de China con el mayor número de publicaciones seguido por USA, Canadá, Inglaterra y Australia.

Figura 11 Mapa de publicaciones sobre gestión de riesgos 2008-2012



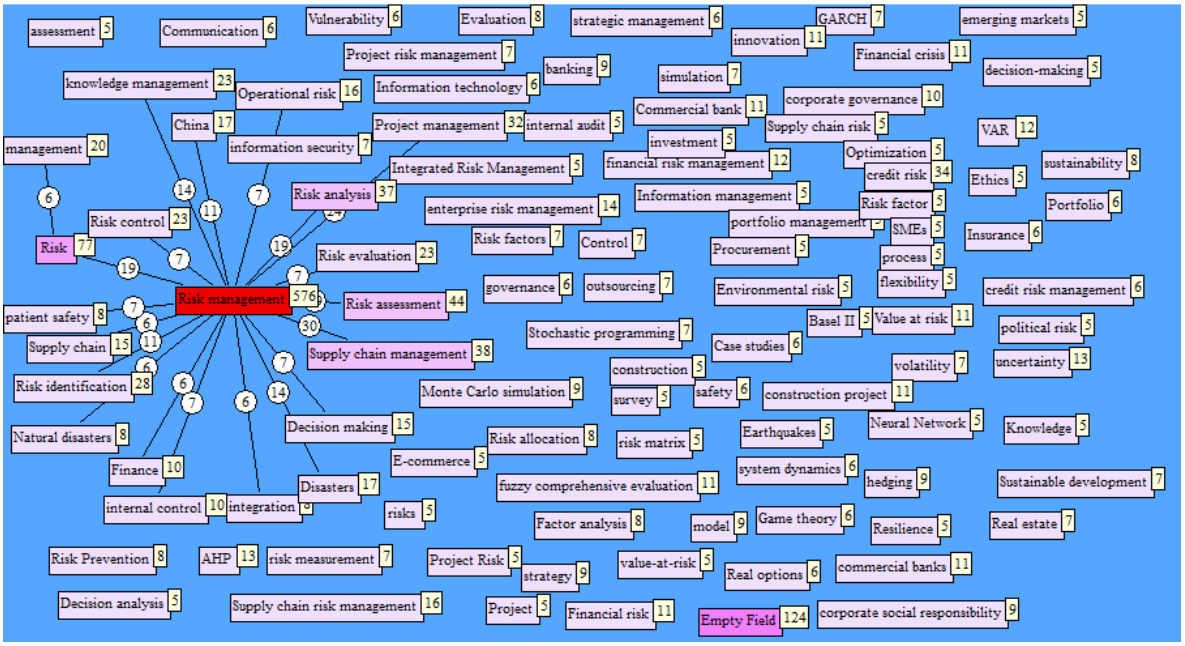
- **Mapa de autores más citados**

Figura 12 Mapa de autores más citados sobre gestión de riesgos en el periodo de 2008 a 2012.



- **Palabras clave más utilizadas**

Figura 13 Palabras clave más utilizadas sobre gestión de riesgos entre el periodo de 2008-2012



5.8 Resultados de la búsqueda sobre seguridad de la información

5.8.1 Procedimiento

Los datos analizados fueron obtenidos de la base de dados del *Institute for Scientific Information (ISI)* mediante el recurso electrónico *Web of Knowledge* y de forma específica en la base de datos Social Science Citation Index, el acceso a este recurso fue realizado desde la Universidad Nacional Autónoma de México.

La búsqueda se realizó por tema, utilizando la palabra clave "information security" y el operador "", en idioma inglés ya que no se obtenían resultados en español. El periodo en años que fue considerado es de 2008 a 2012.

Fueron seleccionadas para el análisis las siguientes referencias.

- *Article*
- *Proceedings paper*

De los resultados obtenidos se realizó un filtrado por áreas para enfocar al tema de interés, los cuales con presentados a continuación.

- *Management.*
- *Business*
- *Health Policy Services*
- *Health Care Science Services*
- *Computer Science Information Systems*
- *Medical Informatics*
- *Public Administration*
- *Law*
- *Medicine Legal*

Fueron consideradas las áreas de negocios y gestión para identificar publicaciones que estén relacionadas con la seguridad de la información y la administración, así como áreas de salud y legal.

La consulta a la base de datos se muestra a continuación:

Topic=("information security")

Refined by: Document Types=(PROCEEDINGS PAPER OR BOOK CHAPTER OR ARTICLE) AND Web of Science Categories=(COMPUTER SCIENCE INFORMATION SYSTEMS OR MANAGEMENT OR PUBLIC ADMINISTRATION OR LAW OR BUSINESS OR MEDICINE LEGAL OR HEALTH POLICY SERVICES OR MEDICAL INFORMATICS OR HEALTH CARE SCIENCES SERVICES) AND Publication Years=(2010 OR 2008 OR 2009 OR 2012 OR 2011)

Timespan=All Years. Databases=SCI-EXPANDED, SSCI, A&HCI, CPCI-S, CPCI-SSH.

Lemmatization=On

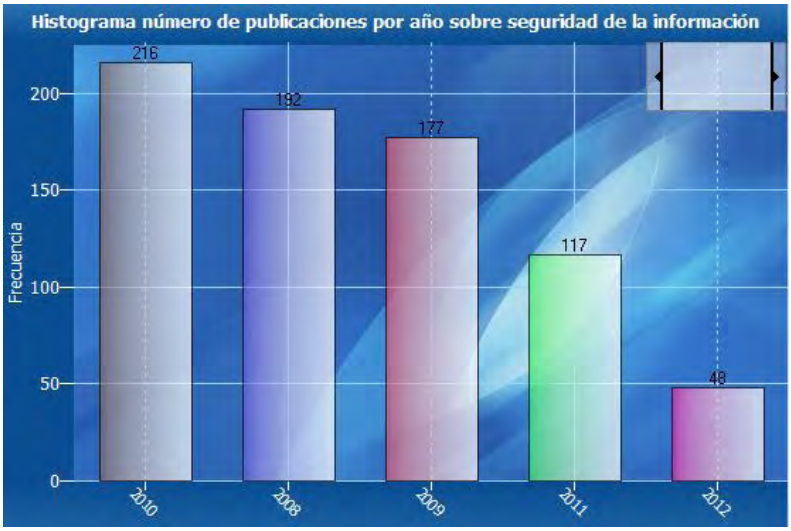
Los resultados obtenidos mediante esta búsqueda indican **750** registros los cuales al ser analizados presentan la siguiente información.

5.8.2 Análisis de los resultados obtenidos

A continuación se presenta el análisis de los resultados obtenidos considerando los siguientes puntos.

- **Publicaciones por año**

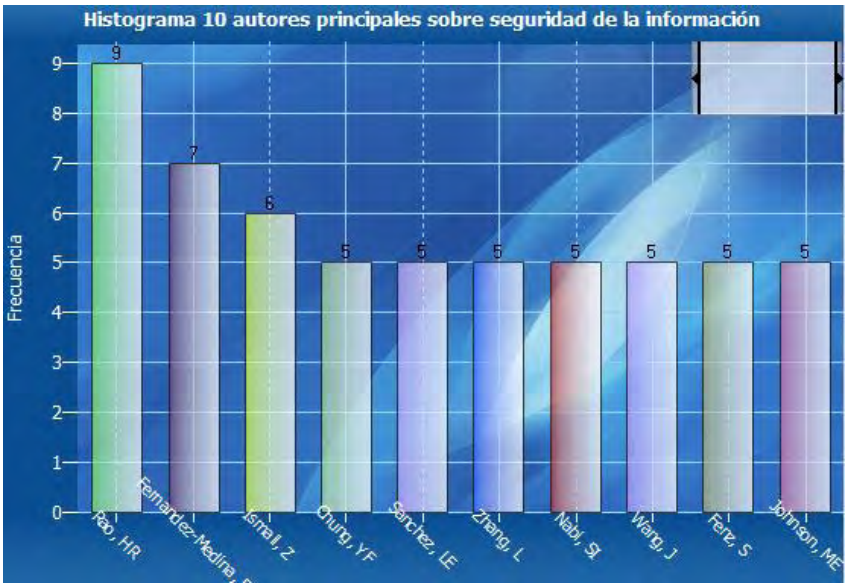
Figura 14 Histograma del número de publicaciones por año



De los resultados obtenidos se identifica que el año 2010 y 2008 se generaron un número mayor de publicaciones sobre seguridad de la información.

- **Diez autores principales**

Figura 15 Histograma de los 10 autores con el mayor número de publicaciones de 2008 al 2012



- **Distribución de las publicaciones por país**

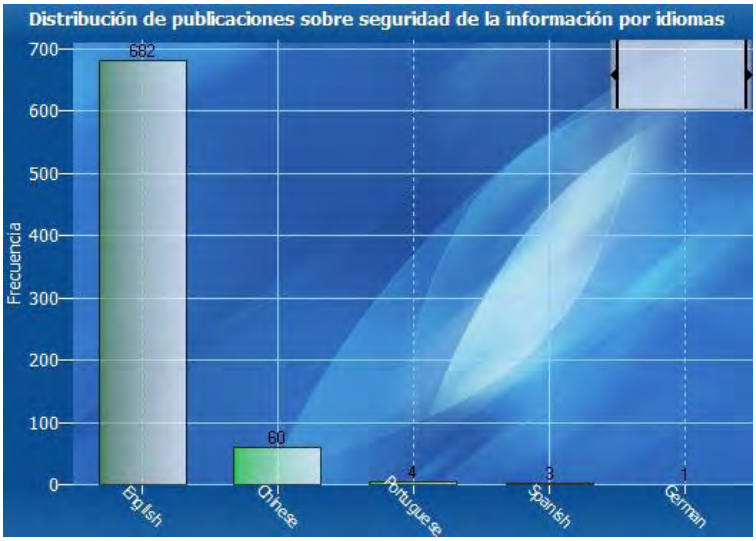
El siguiente cuadro presenta la distribución de las publicaciones por país y considerando que por lo menos se tengan 3 publicaciones en el periodo de 2008 a 20012.

Figura 16 Distribución de las publicaciones por país con al menos 3 publicaciones entre 2008 y 2012

País	Número de publicaciones	País	Número de publicaciones
China.	239	Austria.	8
USA.	62	Iran.	7
Taiwan.	42	Brazil.	7
South Korea.	38	Netherlands.	7
India.	24	Saudi Arabia.	7
Australia.	24	Singapore.	6
England.	21	Norway.	6
Spain.	21	Italy.	5
Germany.	18	Pakistan.	4
Canada.	17	Belgium.	4
Japan.	17	France.	4
South Africa.	16	Wales.	3
Sweden.	16	Denmark.	3
Greece.	12	Thailand.	3
Finland.	12	Bulgaria.	3
Malaysia.	12	Switzerland.	3
Romania.	10	Czech Republic.	3
Portugal.	9		

- **Distribución por idioma**

Figura 17 Distribución del número de publicaciones por idioma



- **Diez revistas con el mayor número de publicaciones**

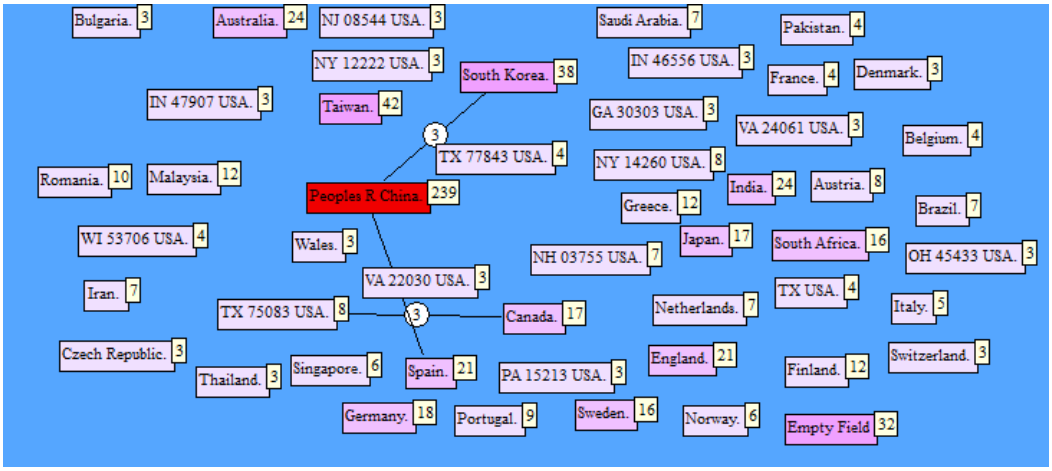
Figura 18: Diez revistas con el mayor número de publicaciones sobre seguridad de la información entre el 2008-2012

Publicación	Número de publicaciones
1. National teaching seminar on cryptography and information security (2010nts-cis), proceedings	50
2. Computers & security	25
3. Decision support systems	14
4. Proceedings of the 9th european conference on information warfare and security	11
5. Journal of medical systems	8
6. IEICE transactions on information and systems	8
7. 3RD international conference on information warfare and security proceedings	8
8. IEEE Latin America transactions	7
9. Mis quarterly	7
10. Proceedings of the 8TH European conference on information warfare and security	7

- **Mapa de publicaciones por país**

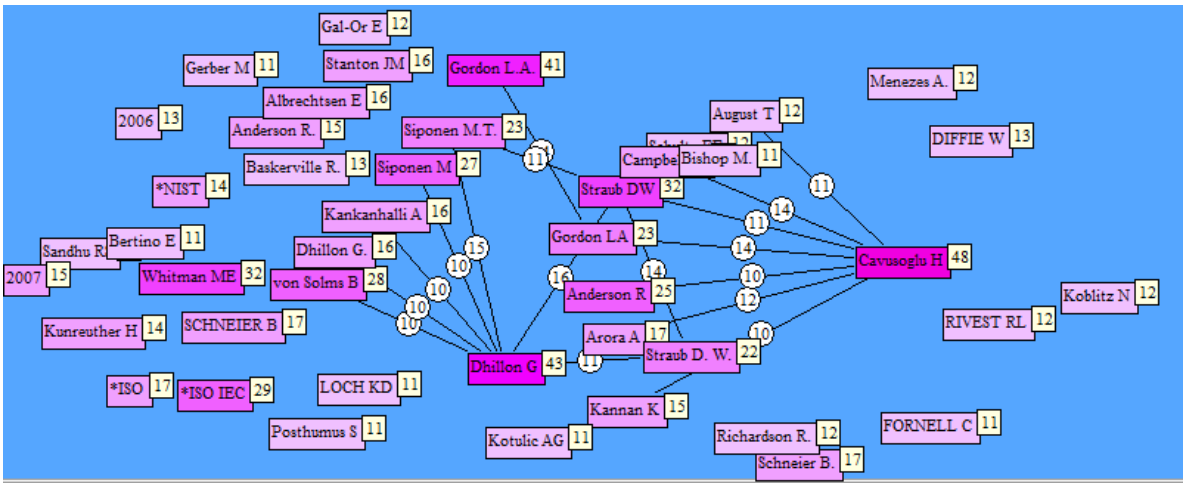
A continuación se muestra el mapa de publicaciones por país sobre seguridad de la información en el periodo del 2008 al 2012, donde se observa que los países con mayor número de publicaciones son China, USA, Alemania, España, Inglaterra, Corea del Sur, Japón, India, Taiwan y Australia.

Figura 19: Mapa de publicaciones sobre seguridad de la información 2008-2012



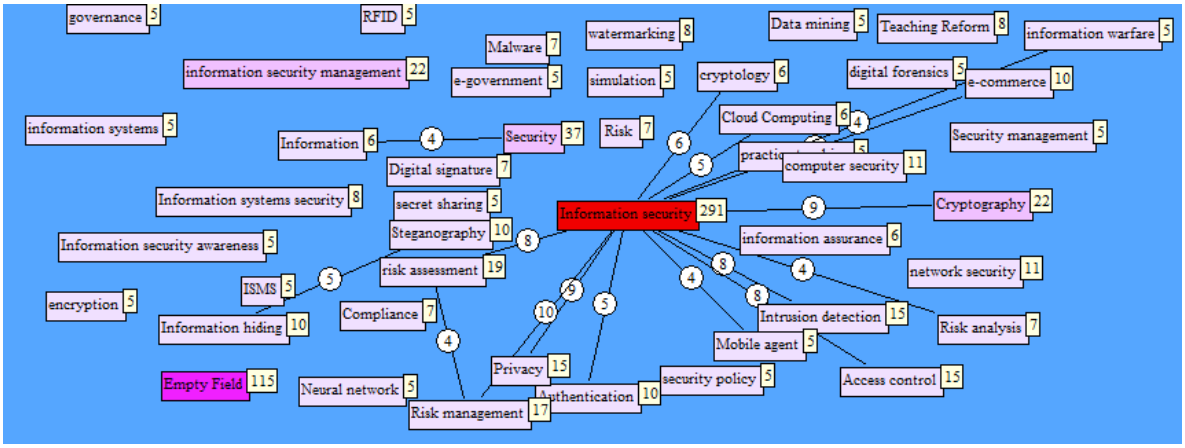
- **Mapa de autores más citados**

Figura 20 Mapa de autores citados sobre seguridad de información en el periodo de 2008-2012



- **Palabras clave más utilizadas**

Figura 1 Palabras clave más utilizadas sobre seguridad de la información en el periodo de 2008 a 2012



5.9 Resultados de la búsqueda sobre gestión de riesgos y seguridad de la información

5.9.1 Procedimiento

Los datos analizados fueron obtenidos de la base de dados del *Institute for Scientific Information (ISI)* mediante el recurso electrónico *Web of Knowledge* y de forma específica en la base de datos Social Science Citation Index, el acceso a este recurso fue realizado desde la Universidad Nacional Autónoma de México.

La búsqueda se realizó por tema, utilizando la palabra clave "risk management", "information security", utilizando los operadores "" y AND para relacionar los temas y con ello reducir la cantidad de información que pudiera generar la búsqueda de gestión de riesgos y que estuviera enfocado a la parte de seguridad de la información, en idioma inglés ya que no se obtenían resultados en español. Dado que los resultados fueron pocos no se realizó un filtrado de años.

Fueron seleccionadas para el análisis las siguientes referencias.

- Article
- Proceedings paper

De los resultados obtenidos se realizó un filtrado por áreas para enfocar al tema de interés, los cuales con presentados a continuación.

- *Computer Science Information Systems*
- *Computer Science Theory Methods*
- *Computer science interdisciplinary applications*
- *Automation control systems*
- *Medical Informatics*
- *Business*
- *Public Administration*
- *Management*

Fueron consideradas la informática y la médica tratando de buscar información específica sobre la relación de los datos clínicos y su protección.

La consulta a la base de datos se muestra a continuación:

Topic=("risk management " AND "information security")

Refined by: Document Types=(PROCEEDINGS PAPER OR ARTICLE) AND Publication Years=(2008 OR 2007 OR 2009 OR 2006 OR 2010 OR 2012 OR 2005 OR 2011) AND Web of Science Categories=(COMPUTER SCIENCE INFORMATION SYSTEMS OR COMPUTER SCIENCE THEORY METHODS OR COMPUTER SCIENCE INTERDISCIPLINARY APPLICATIONS OR AUTOMATION CONTROL SYSTEMS OR MANAGEMENT OR MEDICAL INFORMATICS OR PUBLIC ADMINISTRATION OR BUSINESS)

Timespan=All Years. Databases=SCI-EXPANDED, SSCI, A&HCI, CPCI-S, CPCI-SSH.
Lemmatization=On

Los resultados obtenidos mediante esta búsqueda indican **110** registros los cuales al ser analizados presentan la siguiente información.

5.9.2Análisis de los resultados obtenidos

A continuación se presenta el análisis de los resultados obtenidos considerando los siguientes puntos.

- **Publicaciones por año**

Figura 2 Histograma del número de publicaciones sobre seguridad de la información y gestión de riesgos por año.

- **Diez autores principales**

Figura 23 Histograma de los 10 autores con el mayor número de publicaciones.

- **Distribución de las publicaciones por país**

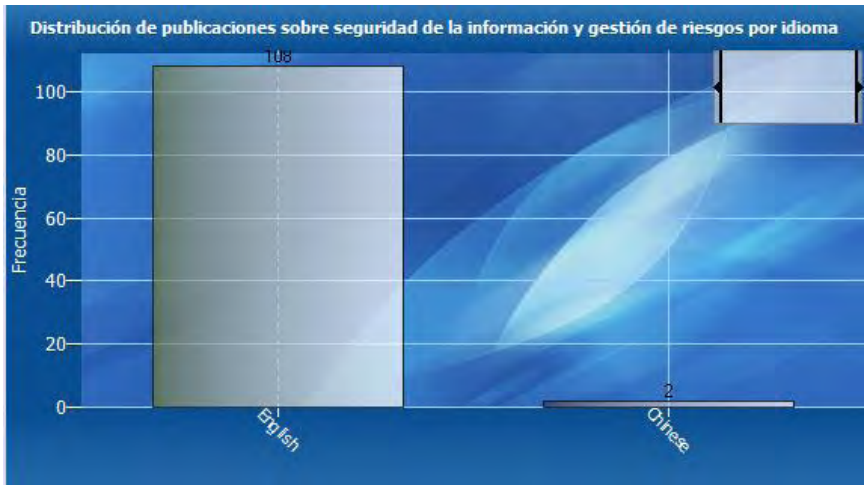
El siguiente cuadro presenta la distribución de las publicaciones por país y considerando que por lo menos se tengan 2 publicaciones.

Figura 24: Distribución de las publicaciones por país con al menos 3 publicaciones

País	Número de publicaciones
China.	12
South Africa.	9
Taiwan.	6
USA	6
Poland.	6
Switzerland.	5
Australia.	5
Austria.	4
Canada.	4
England.	4
Romania.	3
Greece.	3
México	**2**

- **Distribución por idioma**

Figura 25 Distribución del número de publicaciones por idioma



- **Diez revistas con el mayor número de publicaciones**

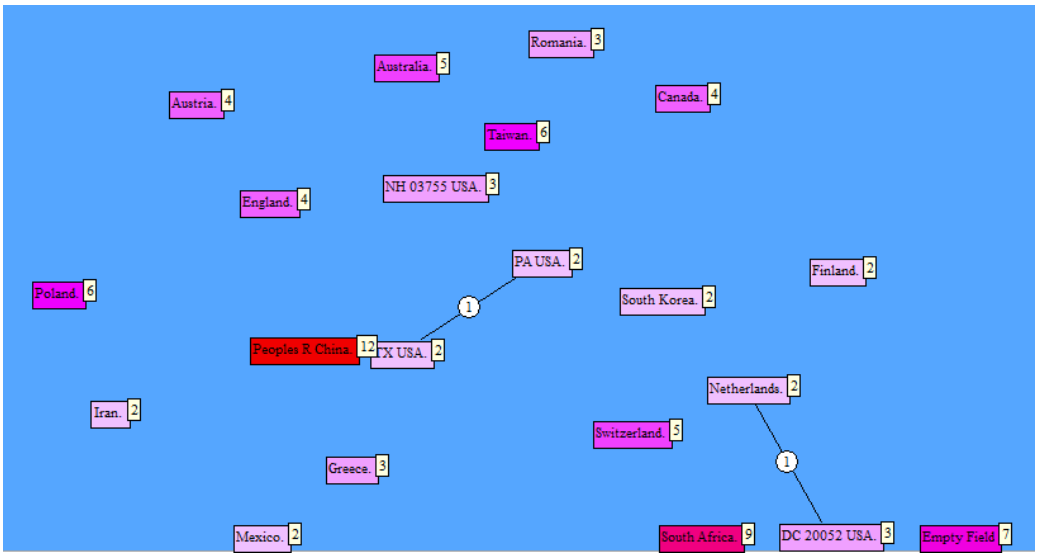
Figura 26 Diez revistas con el mayor número de publicaciones.

Publicación	Número de publicaciones
Computers & security	8
IEEE security & privacy	3
Industrial management & data systems	3
Proceedings of the 9th european conference on information warfare and security	3
Mis quarterly	2
Global security, safety, and sustainability	2
Journal of management information systems	2
World congress on engineering 2008, vols I-II	2
3rd international conference on information warfare and security, proceedings	2
SSecurity management, integrity, and internal control in information systems	2

- **Mapa de publicaciones por país**

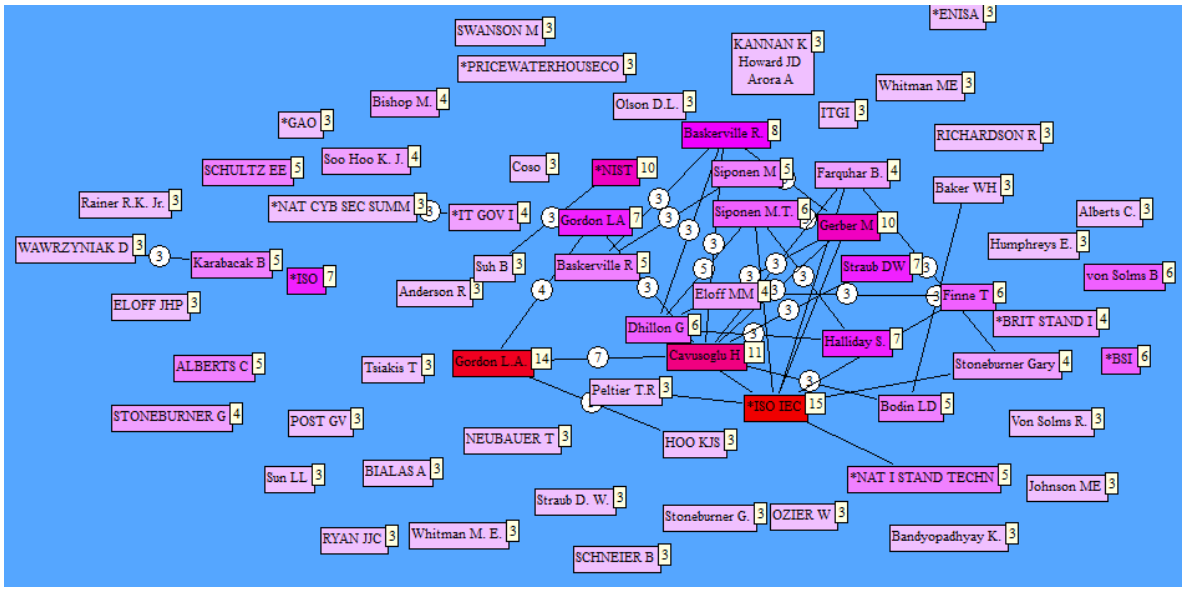
A continuación se muestra el mapa de publicaciones por país sobre gestión de riesgos y seguridad de la información.

Figura 27 Mapa de publicaciones sobre gestión de riesgos y seguridad de la información.



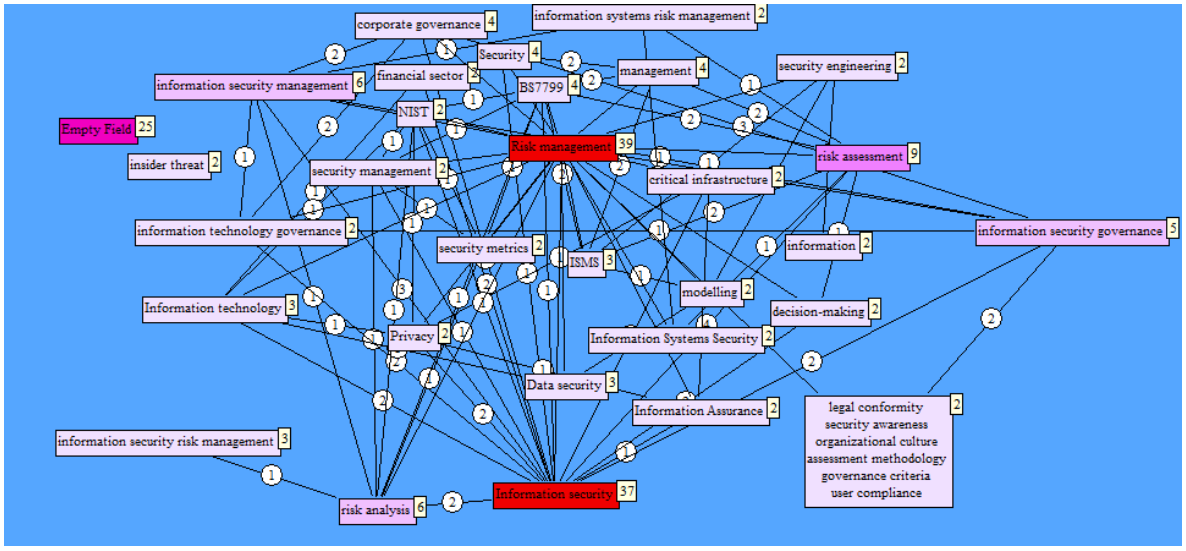
- **Mapa de autores más citados**

Figura 28 Mapa de autores más citados sobre gestión de riesgos y seguridad de la información.



- **Palabras clave más utilizadas**

Figura 29 Palabras clave más utilizadas sobre gestión de riesgos y seguridad de la información.



5.10 Resultados de la búsqueda sobre datos clínicos y seguridad de la información

5.10.1 Procedimiento

Los datos analizados fueron obtenidos de la base de dados del *Institute for Scientific Information (ISI)* mediante el recurso electrónico *Web of Knowledge* y de forma específica en la base de datos Social Science Citation Index, el acceso a este recurso fue realizado desde la Universidad Nacional Autónoma de México.

La búsqueda se realizó por tema, utilizando la palabra clave "clinical data", "information security", utilizando los operadores "" y AND para relacionar los temas y con ello reducir la cantidad de información que pudiera generar la búsqueda de datos clínicos y que estuviera enfocado a la parte de seguridad de la información en idioma inglés ya que no se obtenían resultados en español. Dado que los resultados fueron pocos no se realizó un filtrado de años.

Fueron seleccionadas para el análisis las siguientes referencias.

- Proceedings paper
- Article

De los resultados obtenidos se realizó un filtrado por áreas para enfocar al tema de interés, los cuales con presentados a continuación.

- Computer Science Information Systems
- Medical Informatics
- Telecomunications
- Automation control systems

Fueron consideradas la informática y la médica tratando de buscar información específica sobre la relación de los datos clínicos y la seguridad de la información.

La consulta a la base de datos se muestra a continuación:

Topic=("clinical data" AND "information security",)

Refined by: Document Types=(PROCEEDINGS PAPER OR ARTICLE) AND Web of Science Categories=(COMPUTER SCIENCE INFORMATION SYSTEMS OR MEDICAL INFORMATICS OR TELECOMMUNICATIONS OR AUTOMATION CONTROL SYSTEMS)

Timespan=All Years. Databases=SCI-EXPANDED, SSCI, A&HCI, CPCI-S, CPCI-SSH. Lemmatization=On

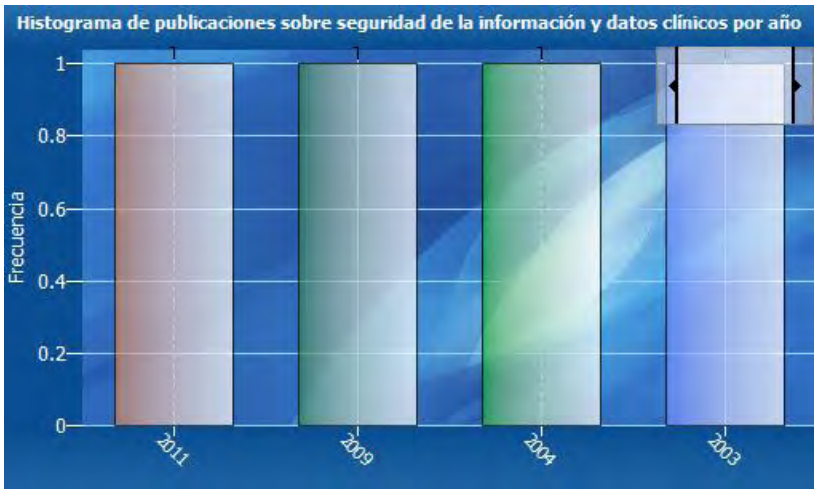
Los resultados obtenidos mediante esta búsqueda indican **4** registros los cuales al ser analizados presentan la siguiente información.

5.10.2 Análisis de los resultados obtenidos

A continuación se presenta el análisis de los resultados obtenidos considerando los siguientes puntos.

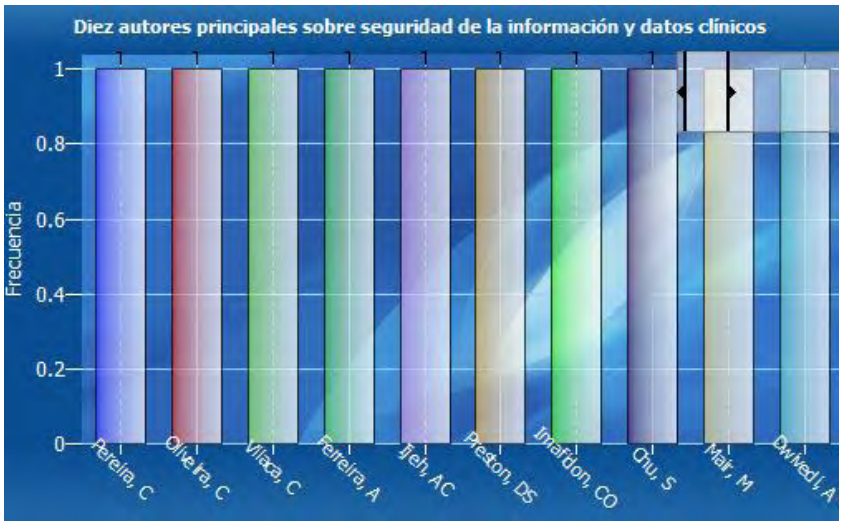
- **Publicaciones por año**

Figura 30: Histograma del número de publicaciones sobre seguridad de la información y datos clínicos por año.



- **Diez autores principales**

Figura 31 Histograma de los 10 autores principales con el mayor número de publicaciones sobre seguridad de la información y datos clínicos.



- **Distribución de las publicaciones por país**

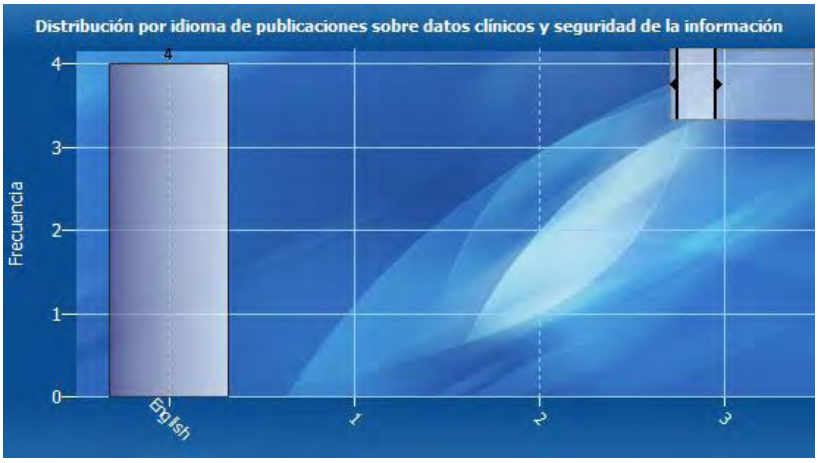
El siguiente cuadro presenta la distribución de las publicaciones por país sobre seguridad de la información y datos clínicos.

Figura 32 Distribución de las publicaciones por país con al menos 3 publicaciones.

País	Número de publicaciones
England	2
Portugal	1
New Zealand	1

- **Distribución por idioma**

Figura 33 Distribución del número de publicaciones por idioma sobre seguridad de la información y datos clínicos.



- **Revistas con el mayor número de publicaciones**

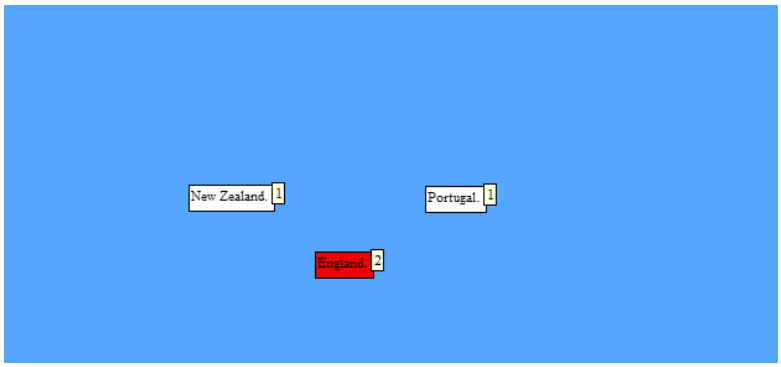
Figura 34 Revistas con el mayor número de publicaciones sobre seguridad de la información y datos clínicos.

Publicación	Número de publicaciones
Healthinf 2011: proceedings of the international conference on health informatics	1
Global security, safety, and sustainability, proceedings	1
International conference on computing, communications and control technologies, vol 6, post-conference issue, proceedings	1
ITAB 2003: 4th international IEEE embs special topic conference on information technology applications in biomedicine, conference proceedings: new solutions for new challenges	1

- **Mapa de publicaciones por país**

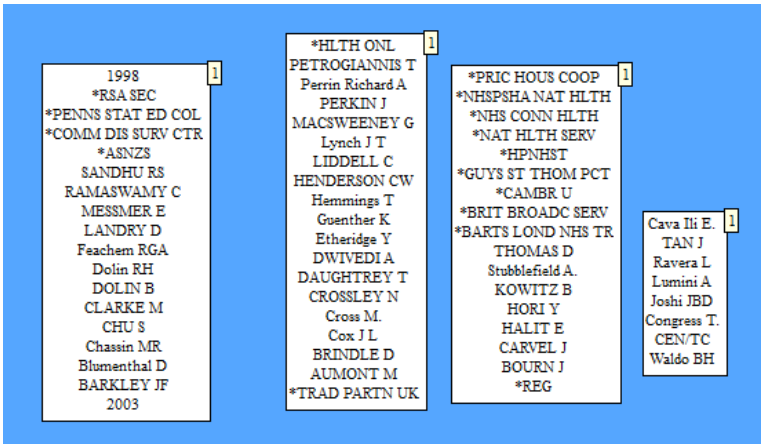
  A continuación se muestra el mapa de publicaciones por país sobre datos clínicos y seguridad de la información.

Figura 35 Mapa de publicaciones sobre datos clínicos y seguridad de la información.



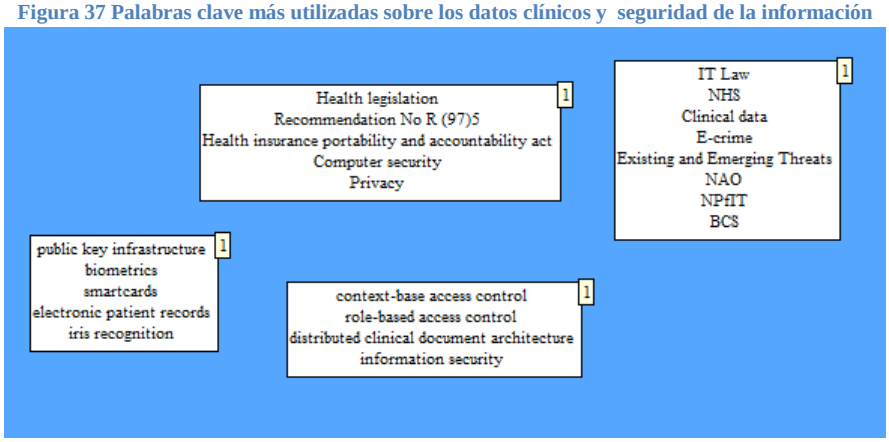
- **Mapa de autores más citados**

Figura 36 Mapa de autores citados sobre los datos clínicos y seguridad de la información.



- **Palabras clave más utilizadas**

Figura 37 Palabras clave más utilizadas sobre los datos clínicos y seguridad de la información



6. HALLAZGOS Y CONCLUSIONES

Como resultado de las búsquedas realizadas se determinan las siguientes conclusiones.

- Se identifica el **capta** que está conformado por los siguientes artículos:
    1. *Protection of clinical data Comparison of European with American Legislation and Respective Technological Applicability*
    2. *The Significance of Security in Transmitting Clinical Data.*
    3. *Secured access control of distributed healthcare data sources.*
    4. *Towards a practical healthcare information security model for healthcare institutions.*

  El capta por estrategia de búsqueda se presenta en la siguiente tabla:

Estrategia de búsqueda	Capta
"risk management"	1,438
"information security"	750
"risk management" AND "information security"	110
"clinical data" AND"information security"	4

- El **ruido** en los resultados de la búsqueda se observa en al cuadro bibliométrico en las estrategias donde se buscaban los términos de gestión de riesgos donde el número mayor de registros fue de 11,500 y seguridad de la información con 2,084.

- El **silencio** se identificó durante la búsqueda que había poca información, solo 4 registros, sobre la seguridad de la información relacionada directamente con los datos clínicos y ningún resultado relacionando directamente, ambos términos con la gestión de riesgos.

- La **serendipia** que fue identificada durante la búsqueda incluyen los siguientes artículos:

    1. *Una prospectiva de la salud en México (Algunos aspectos del marco sociojurídico).*
    2. *La descentralización de la salud en México: avances y retrocesos.*
    3. *A standards-based security model for health information systems.*
    4. *La seguridad, confidencialidad y disponibilidad de la información clínica.*
    5. *Sistema de Salud en México.*
    6. *The Role of Standards in Medical InformationSecurity: An Opportunity for Improvement.*
    7. *Tratamiento jurídico de los datos clínicos en México (información y límites de acceso).*

- Para el tema de *gestión de riesgos* se observa que el año 2008 y 2010 fueron los años con mayor actividad en la generación de publicaciones sobre el tema, como autor predominante se encuentra Zsidisin G.A. quien con un número de 50 publicaciones se posiciona en el primer lugar. Los cinco países que más generado publicaciones del 2008 al 2012 son China, USA, Inglaterra, Australia y Canadá, dentro de esta búsqueda de publicaciones por país no aparece México. La diferencia entre el número de publicaciones entre China y USA es considerable ya que el primero generó 676 mientras que USA solo 130, lo que indica que China es el país que más ha generado información sobre gestión de riesgos. El idioma predominante en las publicaciones generadas es el inglés seguido por el

chino. Las palabras claves que más se relacionan con el tema de gestión de riesgos son el análisis de riesgos, la evaluación de riesgos, riesgos, control de riesgos, gestión del conocimiento, administración de la cadena de suministro, administración, finanzas, seguridad de la información, vulnerabilidad, riesgo operacional, entre otras.

- Sobre el tema de *seguridad de la información* se identificó que los años con mayor actividad fueron el 2008, 2009 y 2010 en los cuales se generaron el mayor número de publicaciones, los cinco países que generaron más publicaciones entre el 2008 y 2012, sobre el tema fueron China, USA, Taiwán, Corea del Sur y la India. Los autores que más destacan por el número de publicaciones es Rao, HR y Fernández Medina. El idioma predominante es el inglés seguido del chino y las palabras clave más utilizadas que se relacionan con la seguridad de la información son, seguridad, detección de intrusiones, seguridad de la computación, gestión de la seguridad de la información, criptografía, control de acceso, seguridad de la red, autenticación, privacidad, gestión de riesgos, esteganografía, seguridad de sistemas de información, entre otras.

- En el caso de los temas *gestión de riesgos y seguridad de la información* se identificó que el año 2008 es donde se han generado el mayor número de publicaciones sobre el tema, los autores principales son Fenz, S, Ekelthart y A, Simms, el país que domina en el número de publicaciones es China seguido de Sudáfrica, Taiwán, USA y Polonia, cabe destacar que en este tema México aparece con dos publicaciones entre el 2008 y el 2012, el idioma predominante es el inglés seguido por el chino y las palabras clave relacionadas con la gestión de riesgos y la seguridad de la información que han sido más utilizadas destacan, gestión de la seguridad de la información, gestión de riesgos de seguridad de la información, gobierno de seguridad de la información, evaluación de riesgos, gestión, seguridad, NIST, administración de la seguridad, gobierno corporativo, métricas de seguridad, seguridad de los datos, seguridad de sistemas de información, tecnologías de la información, no se observan entre los resultados alguna palabra que relacione a los datos médicos o aspectos relacionados con la salud.

- Sobre el tema de *datos clínicos vinculados a la seguridad de la información*, se observa que hay pocas publicaciones que relacionen estos temas, se observa se han generado únicamente 4 publicaciones las cuales pertenecen a los años 2003, 2004, 2009 y 2011, lo cual indica que es un tema que poco estudiado, los cinco autores principales sobre el tema son Pereira, C, Oliveira, C, Villaca, C, Ferreira, A y Ijeh,AC. El país con mayor número de publicaciones es Inglaterra seguido de Portugal y Nueva Zelanda, el idioma predominante es el inglés y las palabras clave más utilizadas que se relacionan con los datos clínicos y seguridad de la información son privacidad, seguridad de la computación, legislación de salud, leyes de IT, datos clínicos, e-crimen, control de acceso basado en roles, seguridad de la información, biométricos, infraestructura de llave pública, tarjetas inteligentes, registro de pacientes electrónico y reconocimiento de iris.

En conclusión se observa que los resultados sobre el tema de seguridad de la información, gestión de riesgos y datos clínicos en conjunto presentan pocos resultados lo que indica que es un tema que no se ha explotado en México, lo cual brinda una ventaja para ser utilizado como tema de investigación de tesis.

D. FORMATOS METODOLOGÍA CADERVIM

CAPACITAR

Definir responsabilidades e involucrados.

Rol	Responsabilidades	Nombre	Área a la que pertenece	Contacto
Responsable del programa de capacitación				

Identificar las necesidades de capacitación.

	Nombre del área	Nombre del titular	Necesidades de capacitación identificadas	Prioridad			Cobertura existente	Eficacia		
				Alta	Media	Baja		Buena	Regular	Mala
Áreas estratégicas										
Áreas tácticas										
Áreas operativas										

Planeación de los temas de capacitación

Temas	Duración	Fecha inicio	Fecha fin	Costo	Responsable	Recursos necesarios	Detalle

DESCUBRIR

Definir el contexto

Id Objetivo estratégico	Objetivo estratégico	Id proceso	Nombre	Importancia	Área responsable	Activos		Dependencia otros procesos	
						Primarios	Soporte	Primaria	Secundaria
A		A1		Crítico				B1	D2, C1
		A2		Moderado				A1	B1
		A3		Bajo				C1	
B		B1		Ninguno				B2	C1
		B2		Crítico				A3	A2
C		C1		Moderado				A1	

Roles y responsabilidades- Matriz RACI

Actividades	Funciones: Comité de seguridad	Director de área	Jefe departamento	Dueño información
	R			
	A			
	C			
	I			

Valoración de activos críticos

Tipo de activo	Nombre del activo	Dueño / Área	Clasificación del activo	Requerimientos de seguridad			Importancia	Valor de activo	Controles actuales		
				C	I	D			C	I	D
H			Confidencial	3	2	3	4				
S			Reservada	2	1	2	3				
R			Pública	1	0	0	2				
P				0	2	1	1				
S				3	3	3	4				
O				2	2	3	3				

Cálculo del riesgo de seguridad para cada activo.

		PROBABILIDAD DE OCURRENCIA				IMPACTO				
Tipo de activo	Nombre del activo	Requerimientos de seguridad			Importancia	Controles actuales				RIESGO
		C	I	D		Nombre amenaza	Prob. Amenaza	Nombre Vulnerabilidad	Prob. Vulnerabilidad	
H		3			4		3		3	= (A + V) * (C+I+D+Im)
S		2			3		2		2	
R		1			2		1		1	
P		0			1		0		0	
S										
O										

Tratamiento del riesgo de seguridad de la información.

Tipo de activo	Nombre del activo	RIESGO	Tratamiento del riesgo				Controles actuales	Estado actual	Controles propuestos	Responsable
			Mitigar	Aceptar	Eliminar	Transferir				
H		= (A + V) * (C+I+D+Im)	X							
S				X	X					
R					X					
P						X				
S				X						
O						X				

Métricas

Tipo de métrica	Descripción	Objetivo	Cálculo	Frecuencia	Responsable
Estratégicas					
Tácticas					
Operativas					

E. OFICIO DE NOMBRAMIENTO DE JURADO DE TESIS

VNIVERSIDAD NACIONAL AVTONOMA DE MEXICO

Relación de Entrega de Carta de Presentación y Tesis para Sinodales de Examen de Grado de Maestría.

Maestría en Administración
Alumna: Miriam Josefina Padilla Espinosa

Tesis: "La gestión de riesgos de seguridad del Sector Salud en México"

	Nombre del Sinodal	Fecha	Firma de Recibido
1	M.A. Lourdes Mata Romero	7/abril/14	
2	Dr. Raúl Ojeda Villagómez	9/Abril/14	
3	M.A. Rita Aurora Fabregat Tinajero	10/Abril/14	
4	M.A. Celia Luz González Fernández	8/Abril/14	
5	M.A. Uriel Calvo Palmerín	5/ABR/14	

Una vez obtenidos los votos respectivos y firmada la presente relación, favor de entregarlos al cubículo 5 ó 6.

BIBLIOGRAFÍA

1. Addy, Rob. (2007). *Effective IT Service Management: To ITIL and Beyond!* : Springer.
2. AMIPCI. (2011). Estudio AMIPCI de Redes Sociales 2011. Ed. Asociación Mexicana de Internet (AMIPCI). Recuperado 21/02, 2013, de http://www.slideshare.net/gpbolde/estudio-amipci-de-redes-sociales-2011
3. AMIPCI. (2012). Estudio de Protección de Datos Personales entre Usuarios y Empresas. Ed. Asociación Mexicana de Internet (AMIPCI). Recuperado 21/02, 2013, de http://www.amipci.org.mx/?P=editomultimediafile&Multimedia=254&Type=1
4. ASF. (2014a). Informe del Resultado de la Fiscalización Superior de la Cuenta Pública 2012 . Recuperado de: http://www.asf.gob.mx/Trans/Informes/IR2012i/Paginas/Master_Ejecutivo.htm
5. ASF. (2014b). Instituto de Seguridad y Servicios Sociales de los Trabajadores del Estado. Aprovechamiento de Infraestructura y Servicios de las TICs. Recuperado de: http://www.asf.gob.mx/Trans/Informes/IR2012i/Documentos/Auditorias/2012_1187_a.pdf
6. ASF. (2014c). Instituto Mexicano del Seguro Social. Aprovechamiento de Infraestructura y Servicios de las TICs . Recuperado de: http://www.asf.gob.mx/Trans/Informes/IR2012i/Documentos/Auditorias/2012_1178_a.pdf
7. Banco Mundial, BM. (2013). Gasto en salud, total (% del PIB).
8. Bernstein, Peter L. (1996). *Against the gods: The remarkable story of risk*: Wiley New York.
9. Bertolín, Javier Areitio. (2008). *Seguridad de la Información redes, informática y sistemas de información*: Editorial Paraninfo.
10. BSI. (2002). BS 7799-2:2002 *Information security management systems- specification with guidance for use* (pp.).
11. BSI (Cartographer). (2006a). BS 7799-3:2006 *Information security management systems – Part 3: Guidelines for information security risk management*. Recuperado de http://www.iso.staratel.com/ISO17799/Doc/BS7799.3.1999/BS%207799-3-2006.pdf
12. BSI. (2006b). BS 25999-1:2006 *Business Continuity Management. Code of Practice*.
13. Senate Bill No. 1386 (2003).
14. CNSS, Committee on National Security Systems. (2010). *National Information Assurance* (IA) Glossary. Recuperado 22/02, 2013, de http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf
15. Cornella, Alfons. (2000). La información no es necesariamente conocimiento (pp.). Infonomia.com: la empresa es información.COSO. (2004). Enterprise Risk Management — Integrated Framework. de http://www.coso.org/erm-integratedframework.htm
16. COSO. (2009). *Guidance on Monitoring Internal Control Systems*.
17. Constitución Política de los Estados Unidos Méxicanos, 2013 C.F.R. (1917).
18. Código Penal Federal., 2013 C.F.R. (1931).

19. CSAE, Consejo Superior de Administración Electrónica (2012). MAGERIT - versión 3 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información - Libro III Guías Técnicas. Madrid.
20. Christopher Alberts, Audrey Dorofee, James Stevens, & Woody, Carol. (2003). *Introduction to OCTAVE Approach* C. M. S. E. Institute (Ed.) Recuperado de http://www.itgovernanceusa.com/files/Octave.pdf
21. Daltabuit, Enrique, Hernández, Leobardo, Mallen, Guillermo, & Vázquez, J. (2007). La seguridad de la información. *México: Noriega Editores*.
22. DGIS, Dirección General de Información en Salud. (2011). Manual del Expediente Clínico Electrónico.
23. EY. (2012). XIV Encuesta Global de Seguridad de la Información: Ernst & Young.
24. FERMA. (2003). Estándares de gerencia de riesgos.
25. FUNSALUD, Fundación Mexicana para la Salud. (2012). Universalidad de los Servicios de Salud. Propuesta de *FUNSALUD* FUNSALUD, A. Fundación Mexicana para la Salud (Ed.) Recuperado de http://funsalud.org.mx/eventos_2012/Universalidad%20de%20los%20servicios%20de%20salud/UNIVERSALIDAD%20DE%20LOS%20SERVICIOS_DEF.pdf
26. Gabuardi, Carlos A. El Marco Jurídico de la Información en Materia de Salud en México.
27. Gammack, John, Hobbs, Valerie, & Pigott, Diarmuid. (2011). *The book of informatics*: Cengage Learning.
28. Gómez-Dantés, Octavio, Sesma, Sergio, Becerril, Victor M, Knaul, Felicia M, Arreola, Héctor, & Frenk, Julio. (2011). Sistema de salud de México. salud pública de méxico, 53(suplemento 2).
29. González Guzmán, R Moreno Altamirano, L, & Castro Albarrán, JM. (2010). La salud pública y el trabajo en comunidad (M. G. Hill Ed. Primera Edición ed.).
30. Gorn, S. Informatics (computer and information science): Its ideology, methodology, and sociology). *The study of information: Interdisciplinary messages*.
31. IEC/ISO. (2009). IEC/ ISO 31010 *Risk management -- Risk assessment techniques*.
32. IFAI. (2009). Guía para la elaboración de un documento de seguridad. México.
33. IMSS. (2013). Informe al Ejecutivo Federal y al Congreso de la Unión sobre la situación financiera y los riesgos del Instituto Mexicano del Seguro Social 2012-2013. de http://www.imss.gob.mx/estadisticas/Documents/20122013/InformeCompleto.pdf
34. INEGI. (2011a). Derechohabiencia y uso de servicios de salud- Población protegida por los servicios de salud, 2000 a 2011. de http://www3.inegi.org.mx/sistemas/sisept/default.aspx?t=msoc01&s=est&c=22594
35. INEGI. (2011b). Población derechohabiente en el ISSSTE según tipo de derechohabiencia por entidad federativa, 2011. de http://www3.inegi.org.mx/sistemas/sisept/default.aspx?t=msoc05&s=est&c=27726
36. INEGI. (2012). Población derechohabiente en el IMSS según tipo de derechohabiencia por entidad federativa, 2011. de http://www3.inegi.org.mx/sistemas/sisept/default.aspx?t=msoc04&s=est&c=27724
37. ISACA. (2005). *COBIT 5 Control Objectives for Information and Related Technology*.
38. ISF. (2003). *Information Security Forum: The Standard of Good Practice for Information Security*.
39. ISM3 Consortium. (2007). *ISM3 Information Security Management Maturity Model.*
40. ISO. (2008a). ISO 9001:2008 Sistemas de gestión de la calidad — Requisitos
41. ISO. (2008b). ISO 27799:2008 *Health informatics —Information security management in health using ISO/IEC 27002*
42. ISO. (2009). ISO 31000 *Risk management — Principles and guidelines*.

43. ISO/IEC. (2000). ISO/IEC 13335-4 I*nformation technology — Guidelines for the management of IT Security — Part 4:Selection of safeguards.*
44. ISO/IEC. (2005). ISO 27002:2005-*Information technology — Security techniques — Code of practice for information security management.*
45. ISO/IEC. (2008). ISO 27005:2008-*Information technology - Security techniques - Information security risk management.*
46. ISSSTE. (2011). Informe de Rendición de Cuentas de la Administración Pública Federal 2006 – 2012 del ISSSTE. de http://www2.issste.gob.mx:8080/images/downloads/transparencia/rendicion-de-cuentas/Compilado_Informes_Rendicion_Cuentas_ISSSTE.pdf
47. ISSSTE. (2013). Informe financiero y actuarial 2012. de http://www2.issste.gob.mx:8080/images/downloads/instituto/quienes-somos/ifa_2012.pdf
48. ITEI, Instituto de Transparencia e Información Pública de Jalisco. (2010). Consideraciones sobre hábeas data y su regulación en distintos ámbitos. http://www.itei.org.mx/v3/documentos/estudios/estudio_habeas_data_6abr10.pdf
49. Leal, Héctor Vázquez, Campos, Raúl Martínez, Domínguez, Carlos Blázquez, & Sheissa, Roberto Castañeda. Un expediente clínico electrónico universal para México: características, retos y beneficios.
50. Ley Federal del Derecho de Autor., 2013 C.F.R. (1996).
51. Ley Federal de Protección de Datos Personales en Posesión de los Particulares., 2013 C.F.R. (2010).
52. Ley Federal de Seguridad Privada (2011).
53. Ley Federal de Telecomunicaciones., 2013 C.F.R. (1995).
54. Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, 2013 C.F.R. (2002).
55. Ley General de Salud, 2013 C.F.R. (1984).
56. López B., Jaquelina, & Quezada R., Cintia. (2006). Fundamentos de Seguridad Informática (F. d. I. UNAM Ed.). México.
57. Ley de la Propiedad Industrial., 2013 C.F.R. (1991).
58. Malhotra, Naresh K, Martínez, José Francisco Javier Dávila, & Rosales, Magda Elizabeth Treviño. (2004). Investigación de mercados: Pearson Educación.
59. McAfeeLabs. (2012). 2013 Threats Predictions.
60. NIST, *National Institute of Standards and Technology. (1998). Special Publication 800-16 Information Technology Security Training Requirements.* . Recuperado 30/01, 2014, de http://csrc.nist.gov/publications/nistpubs/800-16/800-16.pdf
61. NIST, *National Institute of Standards and Technology. (2002). Risk Management Guide for Information Technology Systems Special Publication 800-39* Recuperado 23/02, 2013, de http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf
62. NIST, *National Institute of Standards and Technology. (2011). Glossary of Key Information Security Terms*. Recuperado 22/02, 2013, de http://csrc.nist.gov/publications/nistir/ir7298-rev1/nistir-7298-revision1.pdf
63. NIST, *National Institute of Standards and Technology. (2012). Risk Management Guide for Information Technology Systems Special Publication 800-30 r1*. Recuperado 23/02, 2013, de http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf
64. Directrices sobre protección de la privacidad y flujos transfronterizos de datos personales. (1980).
65. Principios rectores para la reglamentación de los ficheros computarizados de datos personales. (1990).

66. Piña Libien, Hiram Raúl. (2006). Los delitos informáticos previstos y sancionados en el ordenamiento jurídico mexicano. http://www.ordenjuridico.gob.mx/Congreso/2doCongresoNac/pdf/PinaLibien.pdf
67. Piñar, José Luis , & Ornelas, Lina. (2013). La protección de datos personales en México (T. L. B. México Ed.).
68. Poder Ejecutivo Federal, PEF. (2013a). Plan nacional de desarrollo 2013-2018: México.
69. Poder Ejecutivo Federal, PEF. (2013b). Programa Sectorial de Salud 2013-2018: México.
70. RAE, Real Academia Española. (Ed.) (2010) Diccionario de la Lengua Española. Madrir.
71. Ramírez Ramírez, Agustín. (2006). Tratamiento jurídico de los datos clínicos en México (información y límites de acceso). Paper presented at the Estudios en homenaje a Marcia Muñoz de Alba Medrano. Bioderecho, tecnología, salud y derecho genómico.
72. Rivas, TLA. (2006). Como hacer una tesis de maestría. Editorial "Taller Abierto SCL" 2ª edición. México.
73. Salvador Rosas, Griselda. (2007). La proteccion de los datos personales en expedientes clinicos, un derecho fundamental de todo individuo. (Licenciado en Derecho Licenciatura), UNAM. Recuperado de http://132.248.9.195/pd2007/0618485/Index.html
74. Sampieri, Roberto, Collado, Carlos Fernández, & Lucio, Pilar Baptista. (2008). Metodología de la investigación. Editorial Mc Graw *Hill, 1*, 998.
75. Sánchez-González, JM, & Ramírez-Barba, EJ. El expediente clínico en México.
76. SANS, SysAdmin *Audit Networking and Security Institute (2012). An Introduction to Information System Risk Management 2013*(23/02). http://www.sans.org/reading_room/whitepapers/auditing/introduction-information-system-risk-management_1204
77. SEI, Software Engineering Institute. (2010). *CMMI for Development*, Version 1.3.
78. Souza, María Silvina. (2005). El estado del arte. *Ficha de cátedra. Disponible en*.
79. Norma Oficial Mexicana NOM-168-SSA1-1998, Del Expediente Clínico (1998).
80. SSA, Secretaría de Salud. (2013). Guía de intercambio de información en salud para un Sistema de Gestión de la Seguridad de la Información en salud. México.
81. Tellez, Julio. (2004). Derecho informático. México: Ed: McGraw–Hill.
82. Thomas, Peltier R. (2000). *Information security risk analysis. Rothstein Associates Inc, 200.*
83. *Gramm–Leach–Bliley Act* (1999).
84. *Health Insurance Portability and Accountability* (1996).
85. WEF. (2013a). *The Global Information Technology Report 2013: The World Economic Forum.*
86. WEF. (2013b). *Unlocking the value of Personal Data: de collection to Usage: The World Economic Forum*.