Facultad de Ingeniería

Escuela de Ingeniería Civil Biomédica

# Diseño de una metodología para la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en ISO/IEC 27001 en la Unidad de Emergencia Adulto del Hospital Carlos Van Buren.

Por

**Vanessa Gissel Bello Garcés**

Trabajo de Titulación para optar al Título de

Ingeniero Civil Biomédico

**Prof. Guía: M. Sc. Antonio Rienzo.**

Julio 2015

# Dedicatoria

Dedicado a mi familia, por su apoyo incondicional durante todo el proceso.

"Toda organización requiere hacer gestión de cómo proteger eficaz y eficientemente la información".

Principio de la gestión de la seguridad.

# Agradecimientos

Agradecer primeramente a mi Dios todopoderoso por su fidelidad y fortaleza para llevar a cabo mis metas y anhelos. A mis padres y hermana por su apoyo incondicional y oraciones constantes, a mi José por acompañarme durante todo este proceso y a mis amigas por su aliento.

Además, agradecer a mi profesor guía por su ayuda prestada en el desarrollo de este trabajo de título, por su tiempo y disposición. También a mi profesor corrector por sus sugerencias.

## Resumen

Palabras claves: Seguridad de la información, SGSI, activos de información, riesgo.

***Resumen:*** *A diario las instituciones de todo tipo están amenazadas por riesgos que ponen en peligro la integridad de la información y con ello la viabilidad de sus negocios y servicios. Riesgos que provienen no solo desde el exterior de las instituciones, sino que también desde el interior. Para poder trabajar en un entorno como este de forma segura, las instituciones pueden asegurar sus datos e información de valor con la ayuda de un Sistema de Gestión de Seguridad de la Información SGSI. La norma ISO/IEC 27001 entrega directrices, lineamientos y requerimientos necesarios para la implementación de un SGSI.*

*En el caso del siguiente trabajo de título, se diseñó una metodología para la implementación de un SGSI, basado en la norma ISO/IEC 27001, en la Unidad de Emergencia Adulto (UEA) del Hospital Carlos Van Buren (HCVB). Para ello, se estudió la norma en cuestión, la cual utiliza el modelo PDCA (PHVA en español) aplicado a todos los procesos del SGSI. Se analizaron las 4 etapas que contiene este SGSI y se identificaron las actividades en cada una de ellas. Se buscó información relativa al Ministerio de Salud (MINSAL), quién se comprometió a gestionar la seguridad de la información como un proceso continuo en el tiempo, el cual se consolida el año 2014 en el nivel central, con las etapas de Implementación y Evaluación del Sistema. Además, el MINSAL realizó un diagnóstico a nivel nacional a todos los Servicios de Salud para conocer su nivel de seguridad de la información.*

*Entre los resultados obtenidos se destaca la metodología para implementar las 4 fases del ciclo continuo siguiendo los requerimientos de la ISO/IEC 27001 en conjunto con los requerimientos de seguridad de la UEA. Estas cuatro fases son: PLANEAR, en la cual se establece el SGSI; HACER, en la cual se implementa y opera el SGSI; VERIFICAR, en la cual se monitorea y revisa el SGSI y finalmente la fase ACTUAR, en la que se debe mantener y mejorar el SGSI.*

*Existen aspectos claves en la implementación del SGSI, como el compromiso y apoyo por parte de la Dirección de la institución; definición de un política de seguridad y normas, definir un alcance apropiado y limitado; concientización y formación del personal; evaluación de riesgos; compromiso de mejora continua por parte de la Dirección y todo el personal involucrado; organización y comunicación; gestión adecuada de la continuidad de negocio, de los incidentes de seguridad, del cumplimiento legal; mediciones de eficacia del SGSI, sus controles y objetivos de control; y de la integración del SGSI en la organización.*

*Si bien es una metodología que pretende entregar los procedimientos que se deben seguir en la implementación del SGSI en la UEA del HCVB, es necesario considerar el alcance a procesos dentro de la misma institución, sobre todo procesos clínicos que requieran gestionar sus activos de información.*

# Tabla de Contenidos

# Diseño de una metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la norma ISO/IEC 27001 en la Unidad de Emergencia Adulto del Hospital Carlos Van Buren

Vanessa Gissel Bello Garcés
*Escuela de Ingeniería Civil Biomédica, Universidad de Valparaíso, Chile*

***Palabras claves:*** *Seguridad de la información, SGSI, activo de información, riesgo, ISO/IEC 27001, UEA*

## 1. Introducción

La información, junto a los procesos y sistemas que hacen uso de ella, son un importante activo para cualquier institución. Si pensamos en la realidad de un hospital, la información que posee es variada y abundante, pero a su vez no toda posee la misma importancia, ya que si comparamos la información administrativa con la que tiene relación con los pacientes (por ejemplo: datos, atención de salud, etc.), esta última es más crítica y requiere de un manejo especial.

La seguridad de la información permite la protección de potenciales amenazas y riesgos que podrían tener y enfrentar las instituciones. La seguridad recalca su importancia en al ámbito de la protección de la confidencialidad, integridad y disponibilidad de la información. Es por ello que las instituciones deben velar por la seguridad de sus activos de información.

Actualmente, las instituciones de todo tipo se ven enfrentadas a constantes riesgos que ponen en peligro la protección de la confidencialidad, integridad y disponibilidad de la información. Riegos que provienen de distintas fuentes, ya sean externas o internas a la institución, y que pueden provocar daños al punto de poner en peligro la continuidad del negocio o servicio.

A medida que la tecnología experimenta una evolución, las amenazas a la seguridad se han vuelto más presentes y sofisticadas. Los parámetros de seguridad establecidos hace un par de años atrás ya no son lo suficientemente eficientes para el actual desarrollo tecnológico. Cabe señalar que la seguridad de la información no sólo abarca al ámbito informático, ya sea con firewalls o antivirus, sino que también está enfocado a la gestión de la seguridad tomando como principales actores a la Dirección y a los usuarios de la información. Ante este escenario, es importante que cada institución tome medidas para mitigar los riesgos y vulnerabilidades que se enfrentan a diario.

La identificación de estos activos de información es imprescindible para determinar qué es lo que se debe proteger. No toda la información posee la misma importancia, es por ello que se debe priorizar. Además, esto permite tener un mejor conocimiento de lo que es más crítico o presenta una mayor vulnerabilidad.

Al verse afectada la seguridad de la información, se ve afectado el funcionamiento normal, causando serios problemas a la institución y su servicio. Si colocamos un ejemplo pensando en la Unidad de Emergencia Adulto (UEA) del Hospital Carlos Van Buren (HCVB), como el filtro o pérdida de información de la atención de un paciente, esto implicaría no tener un diagnóstico correcto o completo, retraso en la atención y posiblemente la llegada de esta información a manos incorrectas. Sumado a esto, al existir leyes que regulan y protegen la privacidad de la información personal, el derecho de los pacientes a recibir una atención de calidad, entre otros, causaría problemas legales y de confianza hacia el hospital.

Es por ello que los hospitales y toda institución requieren hacer gestión de cómo proteger eficaz y eficientemente la información. Para lograr esto, es necesario implementar un Sistema de Gestión de Seguridad de las Información (SGSI). Este sistema ayuda a establecer políticas y procedimientos adecuados a lo que una institución requiere en relación a los objetivos que tienen definidos. La norma ISO/IEC 27001 adopta un modelo por procesos para establecer, implementar, operar, monitorear, mantener y mejorar un SGSI. El diseño e implementación de un SGSI es influenciado por las necesidades y objetivos, requerimientos de seguridad, los procesos empleados y el tamaño y estructura de la institución.

El Ministerio de Salud (MINSAL) en marzo del 2014, realizó un diagnóstico acerca de la seguridad de la información, en base a los requerimientos de la ISO/IEC 27001, a todos los Servicios de Salud del país. El Servicio de Salud Valparaíso San Antonio (SSVSA) al observar el resultado no favorable de este diagnóstico en la institución, consideró pertinente conocer el nivel de seguridad de la información en los hospitales del Servicio, en los cuales se repitió el resultado desfavorable. Analizando esta situación, se consideró como estrategia implementar un SGSI a nivel institucional, y también en los hospitales, en donde existe información aún más crítica.

Como punto de inicio, se desea implementar un SGSI en la Unidad de Emergencia Adulto del Hospital Carlos Van Buren, ya que es un escenario potencial adverso. Por ello, este trabajo de Título entregará una metodología basada en las directrices que entrega la ISO/IEC 27001 para ayudar en la futura implementación de un SGSI en la Unidad.

### *1.1. Objetivo general*

Diseñar una metodología para la implementación de un SGSI basado en la norma ISO/IEC 27001 en la Unidad de Emergencia Adulto del Hospital Carlos Van Buren.

### *1.2. Objetivos específicos:*

(1) Analizar los lineamientos que enmarcan la seguridad de la información y un SGSI según ISO/IEC 27001, aclarando los requerimientos y contextualizándolos en la Unidad de Emergencia Adulto del hospital.

(2) Elaborar una metodología para la implementación de un SGSI, según el modelo PHVA adoptado por la norma ISO/IEC 27001, en la Unidad de Emergencia Adulto.

En este trabajo se diseñará una metodología según el modelo del proceso Planear-Hacer-Verificar-Actuar (PHVA) de mejoramiento continuo aplicado a todos los procesos del SGSI, como lo indica la ISO/IEC 27001, para su implementación en la UEA del HCVB. Esto se abordará en seis (06) capítulos:

(1) Introducción, indicando el objetivo general y los objetivos específicos para el desarrollo de esta metodología de implementación.
(2) Análisis de la problemática, que incluye el estado del arte, problemática global y problemática específica contextualizando los riesgos de la información en las instituciones, la implementación de ISO/IEC 27001 en el mundo y en Chile, y luego planteando las justificaciones para realizar este trabajo.
(3) Diseño de la propuesta, considerando un estudio del marco teórico, el diseño como tal de la propuesta y su implementación.
(4) Resultados, se expresan los productos de cada uno de los objetivos específicos planteados que entre sí completan el cómo implementar un SGSI y su importancia en el manejo de la seguridad de la información.
(5) Discusiones, corresponde al análisis de los resultados conseguidos y observaciones surgidas en las etapas precedentes.
(6) Conclusiones, finalizando con los impactos asociados y la manera cómo influye en los involucrados el objetivo de introducir una cultura de seguridad y la de implementar un SGSI.

## 2. Análisis de la problemática

### *2.1. Estado del arte: Implementación de SGSI basado en ISO/IEC 27001*

En un principio se mostrará el número de certificaciones ISO/IEC 27001, con el propósito de contextualizar la implementación de esta norma en distintas instituciones a nivel mundial y posteriormente a nivel nacional. Se revisará esta información considerando el hecho de que las instituciones que se han certificado con esta norma poseen un SGSI y también poseen mecanismos para la seguridad de la información. Luego se comentarán tesis similares a lo que se propone en este trabajo, buenas prácticas y lo que la UEA tiene actualmente con respecto a la seguridad de la información.

#### *2.1.1. Certificaciones ISO/IEC 27001 en el mundo*

ISO, sigla de la expresión inglesa International Organization of Standardization (Organización Internacional de Estandarización) es una organización de miembros no gubernamental independiente y el mayor desarrollador mundial de las normas internacionales voluntarias. Estas normas internacionales entregan las especificaciones del estado del arte para los productos, servicios y buenas prácticas, contribuyendo a hacer que la industria sea más eficiente y eficaz (ISO, 2014).

IEC, sigla de la expresión inglesa International Electrotechnical Commission (Comisión Electrotécnica Internacional) es una organización mundial que publica normas internacionales globalmente pertinentes para todas las tecnologías eléctricas, electrónicas y demás relaciones (IEC, 2014).

La ISO cada año, a finales del mes de diciembre, publica los resultados de encuestas de certificación. Este estudio anual muestra el número de certificados emitidos a las normas de sistemas de gestión en el último año. La última encuesta publicada corresponde a la del año 2013.

Las normas expuestas en esta encuesta son las siguientes:

(1) ISO 9001: Determina los requisitos para un Sistema de Gestión de la Calidad (SGC).
(2) ISO 14001: Sistema de Gestión Ambiental.
(3) ISO 50001: Sistema de Gestión de Energía.

(4) ISO 27001: Sistema de Gestión de Seguridad de la Información.
(5) ISO 22000: Sistema de Gestión de Seguridad Alimentaria.
(6) ISO/TS 16949: Especificación técnica para el desarrollo de un SGC.
(7) ISO 13485: SGC para fabricantes de equipos médicos y servicios relacionados.



Un resumen de las estadísticas se muestra en la siguiente tabla:

**Tabla 1.** Estadísticas de certificados ISO al año 2013 (ISO Survey, 2013)

| Standard | N° de certificados en 2013 | N° de certificados en 2012 | Evolución | Evolución en porcentaje |
|---|---|---|---|---|
| **ISO 9001** | **1.129.446** | **1.096.987** | **32.459** | **3%** |
| **ISO 14001** | 301.647 | 284.654 | 16.993 | 6% |
| **ISO 50001** | 4.826 | 2.236 | 2.590 | 116% |
| **ISO 27001** | 22.293 | 19.620 | 2.673 | 14% |
| **ISO 22000** | 26.847 | 23.278 | 3.569 | 15% |
| **ISO/TS 16949** | 53.723 | 50.071 | 3.652 | 7% |
| **ISO 13485** | 25.666 | 22.317 | 3.349 | 15% |
| **TOTAL** | 1.564.448 | 1.499.163 | 65.285 | 4 % |

Los resultados expuestos anteriormente, poseen fluctuaciones en el número de certificados de un año a otro debido a los siguientes motivos:

- La variabilidad en el número de certificados reportados cada año por los organismos de certificación individuales.
- Participación inconsistente de algunos organismos de certificación que contribuyan a la encuesta de un año pero no la próxima.
- La participación de nuevos organismos de certificación (ISO Survey, 2013).

El estándar ISO/IEC 27001 ha sido preparado para proporcionar un modelo para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un SGSI. Permite que una organización de cualquier tipo sea certificada, lo cual significa que una entidad de certificación independiente ha confirmado que la seguridad de la información se ha implementado en dicha organización. No está basada principalmente en la seguridad informática, sino más bien en la seguridad de aquellos documentos considerados activos de información que al estar en situación de riesgo provocarían un gran impacto en la organización.

En la tabla 1 se observa que a finales de diciembre del año 2013, al menos existieron 22.293 certificados ISO/IEC 27001:2005, lo que indica un crecimiento del 14% (2.673) con respecto al año anterior.

Desde el año 2007 hasta el 2013, el crecimiento anual en el mundo con respecto a las certificaciones de la norma en cuestión ha sido favorable. El mayor crecimiento se produjo en el año 2009 llegando a un 40%. Desde el 2011 al 2013, si bien el crecimiento no ha sido tan radical como el ocurrido el año 2008 al 2009, se ha mantenido constante, demostrando que los distintos países han tomado en consideración la importancia de su certificación (ver figura 1).

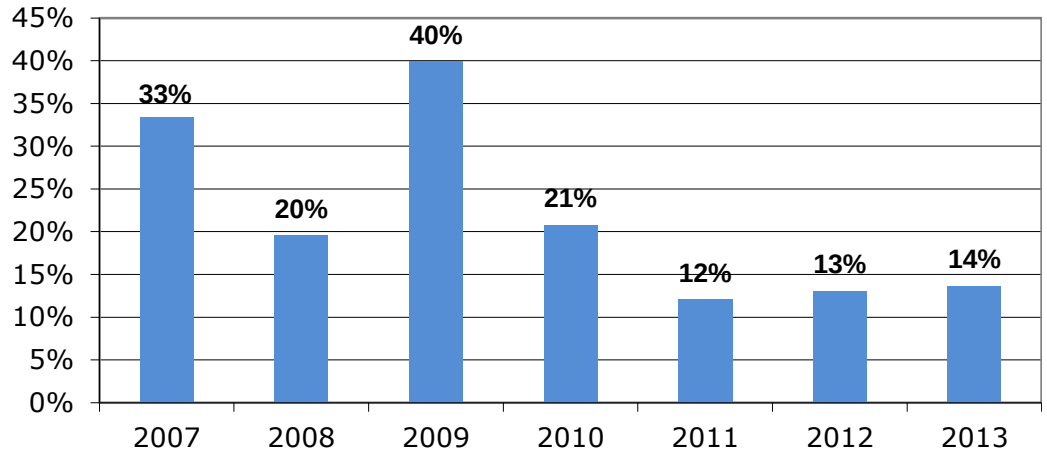



**Figura 1**. Crecimiento mundial anual en porcentaje, ISO 27001 (ISO 27001 Survey Data, 2013)

En relación a las certificaciones realizadas durante el año 2013a nivel mundial, se puede nombrar en primer lugar el continente africano, en donde destacan los siguientes países: Sudáfrica, Egipto, Nigeria y Marruecos entre otros. En lo que respecta a Asia Central y Sur, destaca mayoritariamente India, ya que alcanza el 94% del total de certificaciones. Para mayor detalle en cuanto a número de certificaciones por país ver Anexo 2.

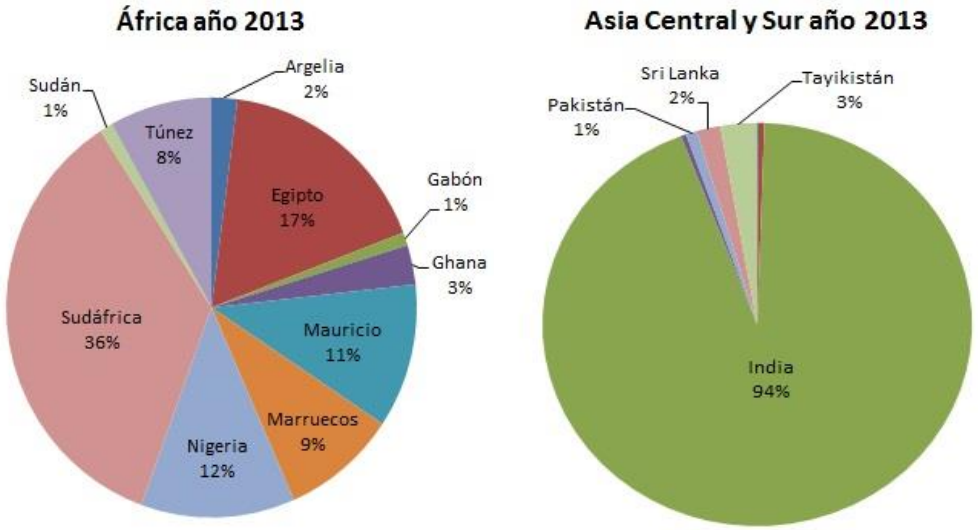



**Figura 2.** Porcentaje certificaciones ISO 27001 en África y Asia central y Sur el año 2013 (ISO 27001 Survey Data, 2013)

En cuanto a Europa, este continente lidera en el número de certificaciones ISO/IEC 27001 en el año 2013 a nivel mundial. Entre los países europeos con mayor número de certificaciones destacan: Reino Unido, Rumania, Italia, España y Alemania. Para mayor detalle del número de certificaciones por país revisar Anexo 3.

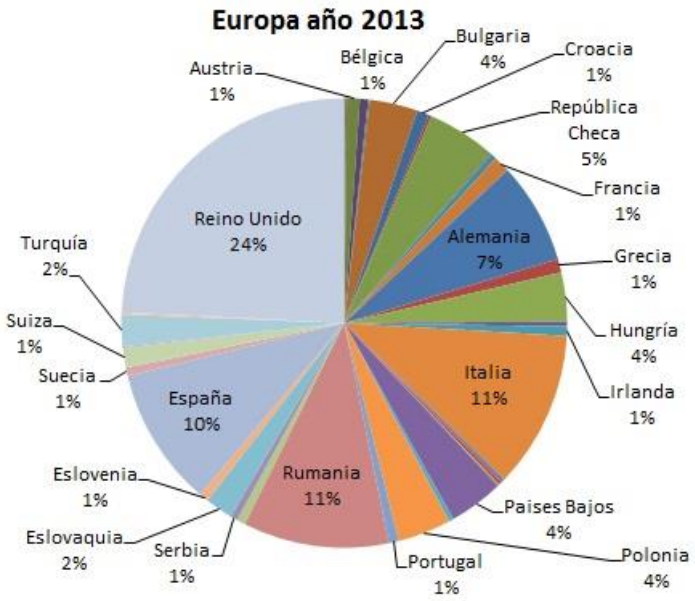



**Figura 3.**Porcentaje certificaciones ISO 27001 en Europa el año 2013 (ISO 27001 Survey Data, 2013)

Al igual que Europa, Asia Oriental lidera en el número de certificaciones ISO/IEC 27001. En relación a Asia Oriental y El Pacífico, se destacan los siguientes países: mayoritariamente Japón, China, Taipéi (China), entre otros. Para acceder a mayor información respecto al número de certificaciones ISO/IEC 27001 de cada país en cuestión revisar Anexo 4.

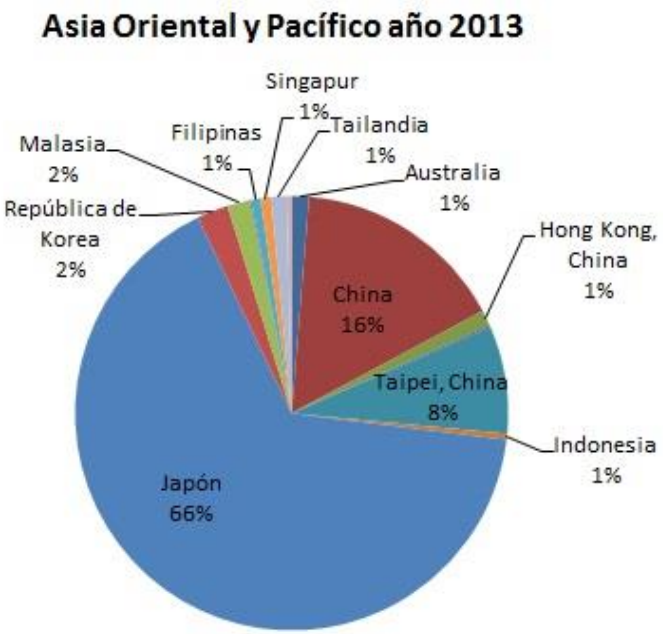



**Figura 4.**Porcentaje certificaciones ISO 27001 en Asia Oriental y Pacífico el año 2013 (ISO 27001 Survey Data, 2013)

En Medio Oriente, los países con certificación ISO/IEC 27001 son el número más bajo en comparación con el resto de las zonas nombradas en los párrafos anteriores. Dentro de lo que es Medio Oriente destacan los siguientes países: Israel, Emiratos Árabes Unidos y Arabia Saudita.

Con respecto a Norteamérica, EE.UU. lidera esa zona alcanzando el 80% del total de certificados del año 2013 en el continente, también se destaca México y Canadá, aunque en menor porcentaje. Para mayor detalle del número de certificaciones de los países de cada sector revisar Anexo 5.

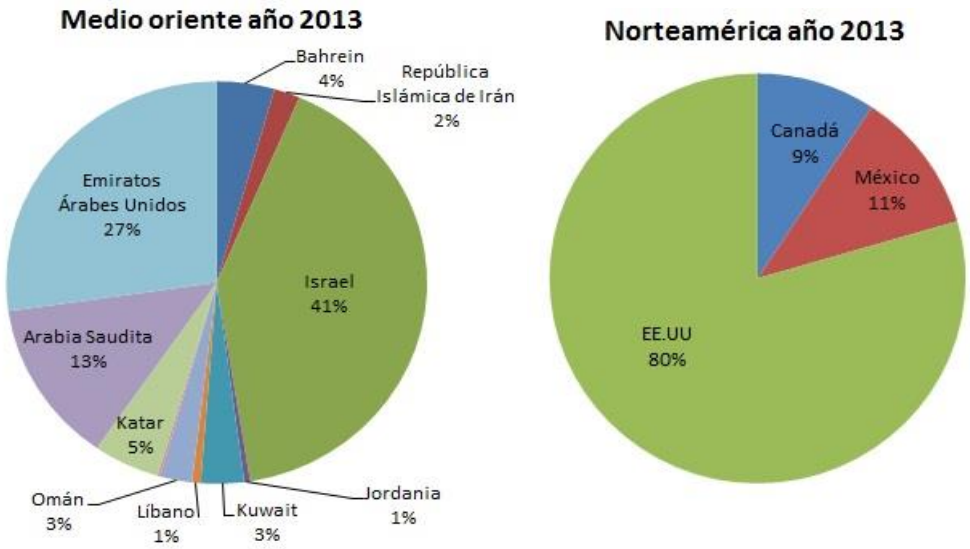



**Figura 5.** Porcentaje certificaciones ISO 27001 en el Medio Oriente y Norteamérica el año 2013 (ISO 27001 Survey Data, 2013)

Como se nombró anteriormente Asia Oriental y Europa lideran en el número de certificados ISO 27001, a diferencia del Medio oriente, región con menor número a nivel mundial.

*2.1.2. Certificaciones ISO/IEC 27001 en América Central y Sur*

Con respecto al crecimiento que ha tenido la incorporación y certificación de la norma ISO/IEC 27001 en los países de América Central y América del Sur desde finales del 2006 a finales del 2013, se presenta la Tabla 2, en donde se evidencia el crecimiento constante que ha existido.

| **Año** | **2006** | **2007** | **2008** | **2009** | **2010** | **2011** | **2012** | **2013** |
|---|---|---|---|---|---|---|---|---|
| **País** | **18** | **38** | **72** | **100** | **117** | **150** | **203** | **272** |
| Argentina | 1 | 1 | 6 | 4 | 8 | 24 | 33 | 40 |
| Barbados | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 |
| Bolivia | 0 | 0 | 0 | 1 | 1 | 3 | 1 | 1 |
| Brasil | 10 | 25 | 40 | 48 | 41 | 50 | 53 | 82 |
| Chile | 2 | 3 | 7 | 10 | 13 | 18 | 23 | 24 |
| Colombia | 3 | 8 | 11 | 14 | 23 | 27 | 58 | 82 |
| Costa Rica | 0 | 0 | 2 | 5 | 6 | 7 | 7 | 10 |
| Cuba | 0 | 0 | 1 | 1 | 2 | 0 | 0 | 0 |
| República Dominicana | 0 | 0 | 0 | 1 | 1 | 2 | 3 | 4 |
| Ecuador | 0 | 0 | 0 | 1 | 1 | 1 | 3 | 5 |
| El Salvador | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 |
| Guatemala | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 2 |
| Guyana | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 |
| Honduras | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 |
| Jamaica | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 |
| Panamá | 0 | 0 | 0 | 0 | 1 | 1 | 2 | 1 |
| Perú | 1 | 1 | 2 | 6 | 9 | 5 | 7 | 9 |
| Puerto Rico | 0 | 0 | 2 | 2 | 2 | 2 | 2 | 2 |
| Trinidad | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 |
| Uruguay | 1 | 0 | 1 | 4 | 4 | 7 | 7 | 8 |

**Tabla 2.** Número de certificados ISO 27001 en América Central y Sur desde el 2006 hasta el año 2013 (ISO 27001 Survey Data, 2013)

Al graficar el número de certificaciones de cada país presentados en la Tabla 2 y al convertirlos en porcentaje de acuerdo al total de certificados emitidos el año 2013 en América Central y Sur, se obtiene la siguiente figura:

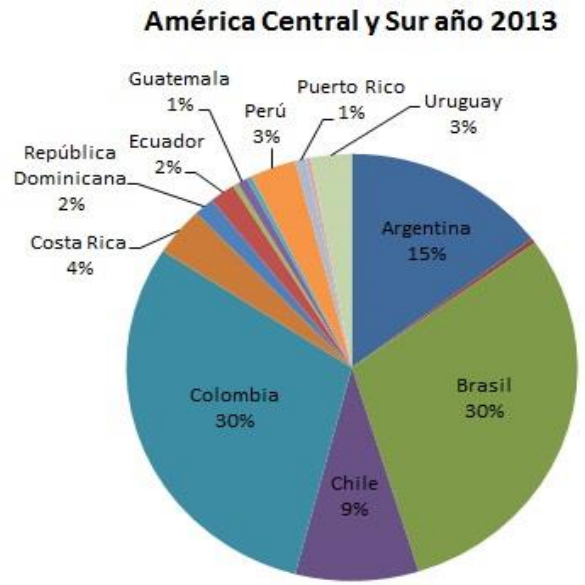



**Figura 6.** Porcentaje certificaciones ISO 27001 en América Central y Sur el año 2013 (ISO 27001 Survey Data, 2013)

En la figura 6, se observa que los países que lideran en el número de certificaciones ISO/IEC 27001 son Brasil y Colombia (ambos con el 30% de certificados), los sigue Argentina con un 15% y luego Chile con un 9%.

Ha existido un crecimiento año tras año en el número de certificaciones en la mayoría de los países, destacando a Brasil, Chile, Colombia y Argentina. Un tanto distinto es el caso de Barbados, Cuba, Guyana, Honduras, Jamaica y Trinidad, países en lo que se observa un estancamiento o disminución de certificados del año 2012 al 2013.

Con respecto al número de certificados ISO/IEC 27001 en el sector industrial, la tabla expuesta en el Anexo 6 da una idea de la cantidad de estos. Considerando que no todas las fuentes de datos respondieron a la solicitud de este detalle adicional, estos valores deben ser tomados como indicadores aproximados, debido a que la suma de los sectores industriales por país puede exceder. De esta tabla (Anexo 6), se puede concluir que los cinco mejores sectores industriales respecto al número de certificaciones emitidos en el 2013 corresponden a:

- ✓ Tecnologías de la información → 5059 certificados.
- ✓ Construcción → 396 certificados.
- ✓ Transporte, almacenamiento y comunicaciones → 322 certificados.
- ✓ Equipamiento eléctrico y óptico →289 certificados.

Observando estos datos, se destaca la cantidad de certificados que posee el área de tecnologías de la información, el cual alcanzó un número importante a nivel mundial.

*2.1.3 Certificaciones ISO/IEC 27001 en Chile*

Los resultados de la encuesta ISO del año 2013, indican que Chile cuenta con 24 instituciones que han logrado la certificación ISO/IEC 27001 al año 2013. Comparando este número con el de los años anteriores, ha existido un incremento como se observa en la figura 7.

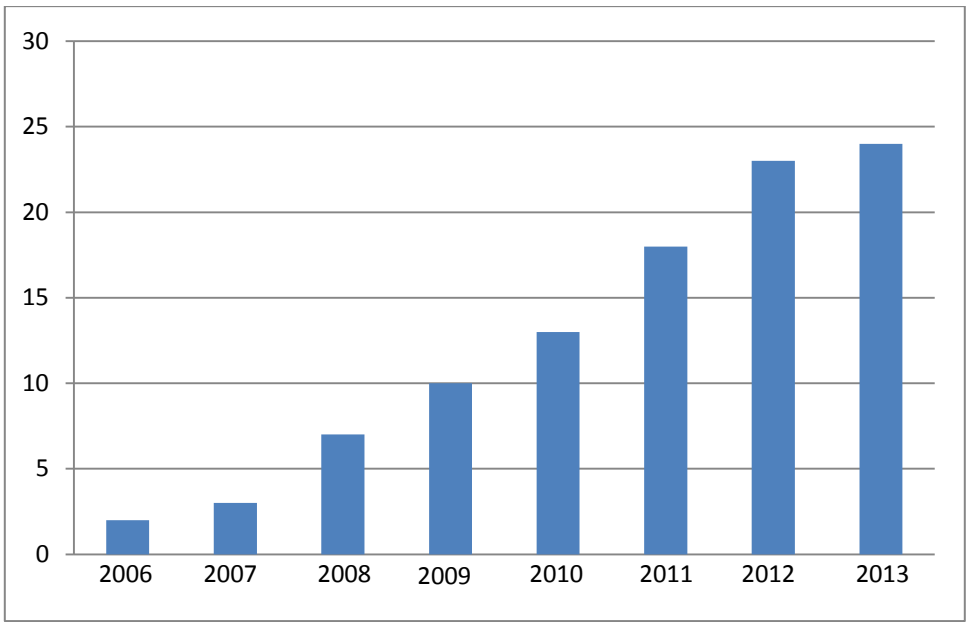



**Figura 7.** Evolución certificaciones ISO 27001 Chile (ISO 27001 Survey Data, 2013)

En el año 2006, Chile partió con 2 certificaciones, luego 3 el 2007, 7 el 2008, 10 el 2009, 13 el 2010, 18 el 2011, 23 el 2012 alcanzando 24 certificaciones el año 2013.

*2.1.4 Tesis de diseño de metodologías para implementar SGSI en distintas organizaciones.*

En busca de metodologías de implementación de un SGSI basado en ISO/IEC 27001 en organizaciones de distintos tipos, se encontró una gran cantidad de información de la cual se tomó como referencia y apoyo en el desarrollo de este trabajo de Título tres tesis que se describen a continuación:

(1) Tesis: "Elaborar una Metodología aplicando la norma ISO/IEC 27001 en la Implementación de un SGSI en el Desitel (Departamento de Sistemas y Telemática) de la ESPOCH (Escuela Superior Politécnica de Chimborazo)" desarrollada por Verónica Gavilanes para optar al título de Ingeniería en Sistemas Informáticos, de la misma escuela de Riobamba, Ecuador (Gavilanes, 2011).

(2) Tesis: "Diseño de una metodología para la implementación del SGSI en el sector de Laboratorios de Análisis Microbiológicos, basado en ISO 27001" desarrollada por Johanna Buitrago, Diego Bonilla y Carol Murillo para optar al título de Especialista en Gerencia Procesos y Calidad, Universidad EAN de Bogotá, Colombia (Buitrago, Bonilla y Murillo., 2012).

(3) Tesis: "Metodología de implantación de un SGSI en grupos empresariales de relación jerárquica", desarrollado por Gustavo Pallas, perteneciente al Grupo de Seguridad Informática, Universidad de la República de Montevideo, Uruguay (Pallas, 2009).

*2.1.3. Buenas prácticas*

A continuación, un listado de buenas prácticas relacionadas a la seguridad de la información tales como proyectos de implementación e implementación de un SGSI, junto con otros sistemas de gestión, que han realizado distintas organizaciones para tener un mayor control de su seguridad.

(1) La Dirección General del Centro de Integración de Informática Médica e Innovación Tecnológica del Hospital Juárez de México presentó el año 2013 un Manual administrativo de aplicación general en materia de Tecnologías de la Información y Comunicaciones y de Seguridad de la Información, que tiene como objetivo regular y homologar su gestión, estableciendo roles definidos que puedan acoplarse a los procesos establecidos para una mejor gestión hospitalaria (Castro, 2013)
(2) La Alcaldía mayor de Bogotá, Colombia, desarrolló el año 2013 un proyecto de Implementación SIG (Sistema Integrado de Gestión) en el Hospital Centro Oriente de esa ciudad, con el objetivo de constituirla como una herramienta de gestión para dirigir y evaluar el desempeño institucional, articulando las acciones de los sistemas de Gestión de la Calidad (SGC), Control Interno (SCI), Gestión Documental y Archivo (SIGA), Gestión de Seguridad de la Información (SGSI), de Seguridad y Salud Ocupacional (S&SO), Responsabilidad Social (SRS) y la Gestión Ambiental (SGA) (Alcaldía Mayor Bogotá, 2015).
(3) Los centros de Hospitales de San Roque, España, cuentan con certificación en las Normas ISO 9001, 14001 y 27001. Con respecto a la certificación de la ISO/IEC 27001, esta garantiza que los controles establecidos por la organización son adecuados y proporcionados para la protección de datos, lo cual otorga confianza en los usuarios. Renovaron la certificación de estas 3 normas hasta el año 2017 (Hospitales San Roque, 2015).
(4) El Hospital del Sur de Bogotá, Colombia, cuenta con un Sistema Integrado de Gestión (SIG), en el cual está inserto un SGSI desde el año 2014. (Hospital Del Sur, 2015) (Camacho, 2015). También el Hospital Centro Oriente de Bogotá cuenta con un SIG en el cual está implementado un SGSI desde el año 2014 (Hospital Centro Oriente, 2015).

Es importante destacar que en el año 2011, el Ministerio de Salud de Chile MINSAL como institución se comprometió a gestionar la seguridad de la información como un proceso continuo en el tiempo. Durante el año 2014, se implementó una intensa agenda de trabajo para dar cumplimiento a los compromisos asumidos en el Programa de Mejoramiento de Gestión (PMG) de la Seguridad de la Información. En este contexto, el Departamento de Gestión TIC Sectorial, asume la responsabilidad del cumplimiento del PMG de Seguridad de la Información y la realización de todas aquellas actividades y tareas que sean necesarias para establecer los niveles de seguridad que la propia institución determine, basándose para ello en metodologías y técnicas estándares en estas materias. Esto con el propósito de lograr introducir un ciclo de mejoramiento continuo y sostenible en el tiempo, que permita lograr niveles adecuados de integridad, confidencialidad y disponibilidad de todos los activos de información relevantes para la institución, como un principio clave en la gestión de sus procesos (Estrategia Digital de Salud 1, 2014). Este proceso se consolidó el 2014 en el nivel central con las últimas dos etapas del PMG correspondiente a la de Implementación y Evaluación del Sistema:

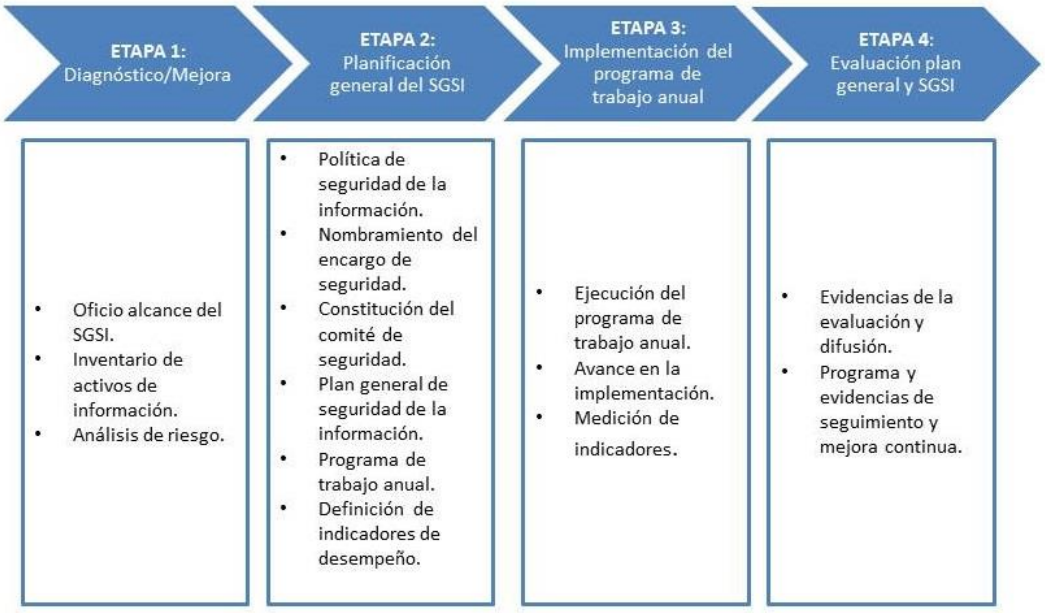



**Figura 8.** Etapas PMG SGSI (Estrategia Digital de Salud 2, 2014)

- **Etapa I:** Diagnóstico. Como producto de esta etapa se obtiene un inventario de activos estructurado que debe ser objeto de actualización permanente, a lo largo del ciclo de vida del Sistema.
- **Etapa II:** Planificación. Se toman aquellos controles que se hayan declarado como no cumplidos en la etapa de diagnóstico, y en base a los productos esperados que se señalen para abordarlos, se formulan iniciativas para su adecuada implementación, que deben ser volcadas en programas de trabajo de carácter anual.
- **Etapa III:** Implementación. Se ejecutan las iniciativas detalladas en el programa de trabajo y se miden los indicadores de desempeño formulados.
- **Etapa IV:** Evaluación. Se debe analizar todo el proceso desarrollado y difundir los resultados de la implementación, hacer las recomendaciones necesarias y velar por su aplicabilidad (Estrategia Digital de Salud 2, 2014).

El 14 de octubre del 2014, a través de la Res.Ex. Nº 781 la Subsecretaría de Salud Pública y Subsecretaría de Redes Asistenciales actualizaron su política de seguridad de la información, lo que permite avanzar en el objetivo de preservar los activos de información del MINSAL (documentos, sistemas, software de aplicación, personas, equipos, etc.) y lograr los niveles adecuados de confidencialidad, integridad y disponibilidad. Además, durante el mes de septiembre y octubre del 2014 el Departamento de Gestión Sectorial TIC realizó un ciclo de capacitaciones en el SGSI junto con auditorias, que tiene como objetivo prioritario disminuir en forma significativa el impacto de los riesgos a los que están sometidos los activos de información de la institución. Con esto, Servicios de Salud, Seremis y Divisiones del MINSAL se capacitan en seguridad de la información (Estrategia Digital de Salud 3, 2014).

### *2.1.4. Seguridad de la información en la UEA del HCVB*

La UEA no posee actualmente (año 2015) un SGSI, por lo que tampoco posee una política de seguridad de la información ni mayores controles que permitan tener un nivel de riesgos aceptable.

Existe un reglamento nacional que regula la seguridad de la información. La Unidad tiene conocimiento de este y lo intenta cumplir a cabalidad. A continuación, se explican las leyes chilenas por las cuales se norma y el área específica que abarca la Unidad:

- Ley N°20.584

Esta ley tiene por objeto regular los derechos y deberes que las personas tienen en relación con acciones vinculadas a su atención de salud. Sus disposiciones se aplicarán a cualquier tipo de prestador de acciones de salud, sea público o privado. Asimismo, y en lo que corresponda, se aplicarán a los demás profesionales y trabajadores que, por cualquier causa, deban atender público o se vinculen con el otorgamiento de las atenciones de salud. Se hace mención especial al párrafo 5 "De la reserva de la información contenida en la ficha clínica".

El artículo 12 indica que la ficha clínica, independiente del formato que tenga, siempre debe contar con los registros completos y que asegure el oportuno acceso, conservación y confidencialidad de los datos, así como la autenticidad de su contenido y de los cambios efectuados en ella. Además, toda la información que surja, tanto de la ficha clínica como de los estudios y demás documentos donde se registren procedimientos y tratamientos a los que fueron sometidas las personas, será considerada como dato sensible, de conformidad con lo dispuesto en la letra g del artículo 2º de la ley Nº 19.628.

El artículo 13 indica que la ficha clínica permanecerá por un período de al menos quince años en poder del prestador, quien será responsable de la reserva de su contenido. También hace referencia a que aquellas terceras personas que no estén directamente relacionados con la atención de salud de la persona no tendrán acceso a la información contenida en la respectiva ficha clínica. Ello incluye al personal de salud y administrativo del mismo prestador, no vinculado a la atención de la persona. Además, la normativa indica que la información contenida en la ficha, copia de la misma o parte de ella, será entregada, total o parcialmente, a solicitud expresa de las personas y organismos tales como titular de la ficha, tercero debidamente autorizado, tribunales de justicia, fiscales del Ministerio Público y a los abogados, en los casos, forma y condiciones especiales (detalladas en la misma normativa). Las instituciones y personas indicadas precedentemente adoptarán las providencias necesarias para asegurar la reserva de la identidad del titular las fichas clínicas a las que accedan, de los datos médicos, genéticos u otros de carácter sensible contenidos en ellas y para que toda esta información sea utilizada exclusivamente para los fines para los cuales fue requerida.

- Ley N°19.628

La cual habla del proyecto de ley: protección de datos de carácter personal. El tratamiento de los datos de carácter personal en registros o bancos de datos por organismos públicos o por particulares se sujetará a las disposiciones de esta ley, con excepción del que se efectúe en ejercicio de las libertades de emitir opinión y de informar, el que se regulará por la ley a que se refiere el artículo 19, N° 12, de la Constitución Política. Toda persona puede efectuar el tratamiento de datos personales, siempre que lo haga de manera concordante con esta ley y para finalidades permitidas por el ordenamiento jurídico. En todo caso deberá respetar el pleno ejercicio de los derechos fundamentales de los titulares de los datos y de las facultades que esta ley les reconoce.

En este caso, cabe señalar todos los artículos de esta ley en su totalidad ya que abarcan áreas en las que la UEA tiene acceso, esto con respecto a los datos personales de los pacientes.

- Ley N°19.223

Tipifica figuras penales relativas a la informática. Delitos informáticos en Chile.

Para el caso de la UEA, a pesar de no estar informatizada en su totalidad, está susceptible a sufrir alguna intervención deseada y no deseada en sus sistemas informáticos, por ejemplo, el Sistema Orden, cuya intervención puede tener consecuencias negativas. Por ello, es importante destacar los cuatro artículos de esta ley.

### *2.2. Análisis del problema*

La información es un valioso activo del que depende el buen funcionamiento de una organización. Mantener su integridad, confidencialidad y disponibilidad es esencial para alcanzar los objetivos de servicio. Por esta razón, desde tiempos inmemorables las organizaciones han puesto los medios necesarios para evitar el robo y manipulación de sus datos confidenciales. En la actualidad, el desarrollo de las nuevas tecnologías ha dado un giro radical a la forma de entregar los servicios y productos, a la vez que ha aumentado los riesgos paras las organizaciones que se exponen a nuevas amenazas (Alexander, 2007).

#### *2.2.1. Problemática global*

Actualmente, organizaciones de todo tipo se enfrentan cada vez a más riesgos e inseguridades procedentes de una amplia variedad de fuentes que pueden dañar de forma importante sus sistemas de información e información como tal, poniendo en peligro la continuidad del negocio.

La tecnología y el conocimiento avanzan de forma rápida y veraz, dejando áreas de cuidado a la intemperie e inseguridad, ya que entre más tecnología y conocimiento exista en las organizaciones, mayor es el riesgo que tendrá la información si no existe protección constante contra amenazas y un manejo de las vulnerabilidades.

A diario estamos amenazados de riesgos que ponen en peligro la integridad de la información y con ellos la viabilidad de la organización. Riesgos que no sólo provienen desde el exterior de ella, sino que también desde el interior. Existen riesgos físicos, en estos podemos nombrar catástrofes naturales tales como terremotos, inundaciones, incendios y vandalismo. También hay riesgos lógicos, como la deficiencia en el control de acceso de la información, robo de información e identidad y espionaje, entre otros. Además, las organizaciones lo que suelen hacer frente a eventos que ponen en peligro la seguridad de la información es actuar de forma reactiva en lugar de hacerlo en forma proactiva. En otras palabras, se preocupan más de las acciones correctivas tomando medidas cuando ya ha ocurrido el incidente en lugar de evitar que este ocurra. Estos incidentes provocan riesgos para la información, la cual puede ser mal utilizada; divulgada, robada, borrada y saboteada. Además provoca la posible falsificación, venta de información y fraude de esta, por nombrar algunos, afectando de forma directa la confidencialidad, integridad y disponibilidad de la información (Alexander, 2007).

"La información personal en Chile hoy día si es bastante vulnerable" (Vera, 2013). Partiendo en el hecho de que los datos personales sean utilizados para fines no pensados, nos permite observar la vulnerabilidad que tienen estos.

Ante estas circunstancias, es imprescindible que las organizaciones evalúen los riesgos asociados y establezcan las estrategias y controles adecuados que aseguren una permanente protección y salvaguarda de la información. Una gestión eficaz de la seguridad de la información permite garantizar (Aenor, 2014):

- Su confidencialidad, asegurando que sólo quienes estén autorizados puedan acceder a la información.

- Su integridad, asegurando que la información y sus métodos de proceso son exactos y completos.
- Su disponibilidad, asegurando que los usuarios autorizados tienen acceso a la información y a sus activos asociados cuando lo requieran.

Para poder estar preparados ante cualquier imprevisto y actuar con rapidez y eficacia, es necesario implantar un SGSI. Es por ello la importancia de contar con un sistema de gestión que se encargue de la seguridad de los activos de información para evitar impactos que afecten a las organizaciones.



*2.2.2. Problemática específica*

La información que poseen los hospitales está presente en los sistemas informáticos, pero también en papel, en diferentes tipos de archivos y soportes, se transmite a terceros, se muestra en diversos formatos audiovisuales, se comparte en conversaciones telefónicas y reuniones y está presente en el propio conocimiento y experiencia de los trabajadores y funcionarios.

El MINSAL promueve activamente la implementación de un SGSI, que da la posibilidad de disminuir en forma significativa el impacto de los riesgos a los que están sometidos los activos de información. El objetivo del SGSI es "lograr niveles adecuados de integridad, confidencialidad y disponibilidad para toda la información institucional relevante, con el objeto de asegurar continuidad operacional de los procesos y servicios, a través de un sistema de gestión de seguridad de la información" (MINSAL, 2014).

En el primer semestre del año 2014 el MINSAL realizó un diagnóstico a todos los Servicios de Salud del país, el cual pretendía medir el nivel de seguridad de la información. Esta encuesta estaba relacionada con la implementación de los controles y objetivos de control que indica la norma ISO/IEC 27001 en su Anexo A, en los ámbitos de:

(1) Política de seguridad.
(2) Organización de la Seguridad de la Información
(3) Gestión de activos.
(4) Seguridad de Recursos Humanos.
(5) Gestión de un Incidente en la Seguridad de la Información.
(6) Seguridad Física y Ambiental.
(7) Gestión de las comunicaciones y operaciones.
(8) Control de Acceso.
(9) Adquisición, desarrollo y mantenimiento de los Sistemas de Información.
(10) Gestión de la Continuidad del Negocio.

El SSVSA, al observar el resultado no muy favorable de este diagnóstico en la institución, consideró pertinente también conocer el nivel de seguridad de la información de los hospitales del Servicio. Para ello, en junio de ese mismo año, Vanessa Bello desarrolló una encuesta siguiendo la línea del diagnóstico del MINSAL en el trabajo de Seminario de Investigación "Evaluación de la Implementación de SGSI según ISO/IEC 27001 en hospitales públicos de la región de Valparaíso" (Ver Anexo 8), en donde se observó que la gran mayoría de los hospitales evaluados no contaban con políticas de seguridad de la información ni los controles que estipulaba el diagnóstico. Analizando el resultado de esta encuesta a los hospitales, Enrico Olguín, Jefe Sub-Departamento de Informática del SSVSA, ha considerado aplicar como estrategia implementar un SGSI a nivel

institucional, y también en los hospitales del Servicio en un mediano-largo plazo, en donde existe información aún más crítica. La planificación para implementar un SGSI en el SSVSA aún está en proceso de desarrollo, teniendo reuniones para conformar un comité de seguridad y revisar las opciones a considerar.

En su defecto, Enrico Olguín, Jefe del Sub-Departamento de Informática del SSVSA, estipuló necesario desarrollar una guía para la implementación de un SGSI en el Hospital Carlos Van Buren perteneciente al SSVSA, específicamente en la UEA, ya que considera que un hospital y con mayor razón un servicio como el que presta la UEA es un escenario potencial adverso y contiene información aún más critica que la institucional del SSVSA.

En la UEA del HCVB no existe una cultura de seguridad de la información provocando en los funcionarios un desconocimiento de roles y responsabilidades en cuanto a seguridad de la información. También, desconocen la norma ISO/IEC 27001 y lo que proporciona en relación a un SGSI. Ni el Hospital ni la Unidad en cuestión cuentan con una Política que permita regular la seguridad de la información desde la Dirección, provocando que existan controles de seguridad nulos o mínimos, sin resguardo de información. Sólo está considerada la información personal y la ficha clínica ya que están protegidas por ley (ver numeral 3.1.4.) (Gómez, 2014) (Soto, 2015).

Todo lo anterior resulta en que la UEA posee un bajo nivel de seguridad de la información, dejándola vulnerable y en un constante riesgo.

Los efectos que provoca un bajo nivel de seguridad en la información al no tener una política, controles y gestión de riesgos en la Unidad, son la pérdida y filtración de información relacionada con los pacientes y su atención. Por un lado, la filtración provoca que información privada sea de conocimiento público y también sea usada para otros fines no estipulados si llega a manos equivocadas. Por otro lado, la pérdida de información, por ejemplo el extravío de hojas de la ficha clínica o la letra poco legible de un funcionario médico, puede provocar un diagnóstico erróneo y/o incompleto; también un retraso en la entrega de este y cualquier información relacionada (Gómez, 2014) (Soto, 2015). Para árbol del problema ver Anexo 1.

Por ello, este trabajo de Título entregará una metodología basada en ISO/IEC 27001, que entrega directrices para lograr la implementación de un SGSI en cualquier institución (en este caso en la UEA del HCVB) ya que este sistema proporciona mecanismos para salvaguardar los activos de información y de los sistemas que los procesan.

## 3. Desarrollo de la propuesta

### *3.1. Marco Teórico*

El marco teórico será abordado a través de los términos que conforman el título del trabajo para lograr su comprensión, describiendo la ISO/IEC 27001, lo que es un SGSI, el modelo PHVA y su aplicación a los procesos del SGSI. Además, se presentará el marco legal y jurídico chileno que tiene relación con la seguridad de la información, y finalmente, la descripción de la UEA, sus procesos y actividades.

#### *3.1.1. Norma ISO/IEC 27001*

ISO e IEC desarrollaron la familia de normas ISO/IEC 27000. Esta familia contempla una serie de estándares, entre ellos, la norma ISO/IEC 27001. Es una norma de carácter internacional que tiene como objetivo garantizar que los controles que existen para salvaguardar la información de las partes interesadas son adecuados para proteger la confidencialidad, integridad y disponibilidad de la información. Estos controles deben tener en cuenta la información de clientes, empleados,

socios, y las necesidades de la sociedad en general. Esta norma certifica un SGSI (ISO/IEC 27001, 2005).

Fue publicada en el año 2005; y fue preparada por el comité técnico conjunto ISO 27001 JTC 1, tecnología de la información, subcomité SC 27 y técnicas de seguridad TI.

Los requisitos de esta norma aplican a todo tipo de organizaciones, independientemente de su tipo, tamaño, o área de actividad. Además, este estándar se alinea con ISO 9001 e ISO 14001 para dar soporte a una implementación y operación consistente e integrada con los estándares de gestión relacionados. Por lo tanto, un sistema de gestión adecuadamente diseñado puede satisfacer los requerimientos de todos estos estándares. Está diseñado para permitir que una organización se alinee o integre su SGSI con los requerimientos del sistema de gestión relacionado (ISO/IEC 27001, 2005).

*3.1.2. Sistema de Gestión de Seguridad de la Información (SGSI)*

SGSI es la abreviatura utilizada al referirse a un Sistema de Gestión de Seguridad de la Información. ISMS es el equivalente en el idioma inglés, siglas de Information Security Management System.

Un SGSI es una parte del sistema general de gestión de una institución con base en un enfoque de riesgo empresarial para establecer, operar, supervisar, revisar, mantener y mejorar la seguridad de la información (entiéndase por información a un conjunto de datos organizados en poder de un entidad que posean valor para la misma, independiente de su formato, transmisión y lugar en que se guarde o almacene).

La ISO/IEC 27001 expresa que un SGSI es un sistema de gestión que comprende la política, estructura organizativa, los procedimientos, los procesos y los recursos necesarios para implantar la gestión de la seguridad de la información. Este sistema es la herramienta de que dispone la Dirección de las organizaciones para llevar a cabo las políticas y los objetivos de seguridad (confidencialidad, integridad y disponibilidad), asignación de responsabilidad, autenticación, etc.). Este sistema proporciona mecanismos para la salvaguarda de los activos de información y de los sistemas que los procesa, en concordancia con las políticas de seguridad y planes estratégicos de la organización (Universidad Nacional de Colombia, 2015).

Garantizar un nivel de protección total es virtualmente imposible, incluso en el caso de disponer de un presupuesto ilimitado. El propósito de un sistema de gestión de la seguridad de la información es, por tanto, garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías (ISO/IEC 27000, 2014).

*3.1.3. Modelo del proceso Planear-Hacer-Verificar-Actuar (PHVA) aplicado a SGSI.*

Las siglas PDCA son el acrónimo de las palabras inglesas Plan, Do, Check, Act, equivalentes en español a Planificar, Hacer, Verificar, y Actuar.

El ciclo PHVA o PDCA, también conocido como "Círculo de Deming", ya que fue el Dr. Williams Edwards Deming uno de los primeros que utilizó este esquema lógico de la calidad y le dio un fuerte impulso. Basado en un concepto ideado por Walter A. Shewhart, el Ciclo PHVA constituye una estrategia de mejora continua de la calidad en cuatro pasos, también se lo denomina espiral de mejora continua y es muy utilizado por los diversos sistemas en las organizaciones para gestionar áreas tales como Calidad (ISO 9001), Medio Ambiente (ISO 14001), Seguridad de la Información (ISO 27001), entre otras (Calidad y Gestión, 2015).


**Figura 9.** Ciclo Continuo PDCA (Gestión y Calidad, 2015)

La interpretación de este ciclo es muy sencilla: cuando se busca obtener algo, lo primero que hay que hacer es planificar cómo conseguirlo, después se procede a realizar las acciones planificadas (hacer), a continuación se comprueba qué tal se ha hecho (verificar) y finalmente se implementan los cambios pertinentes para no volver a incurrir en los mismos errores (actuar). Nuevamente se empieza el ciclo planificando su ejecución pero introduciendo las mejoras provenientes de la experiencia anterior (Calidad y Gestión, 2015).

Los resultados de la implementación de este ciclo permiten a las organizaciones una mejora integral de la competitividad, de los productos y servicios, mejorando continuamente la calidad, reduciendo los costos, optimizando la productividad, reduciendo los precios, incrementando la participación del mercado y aumentando la rentabilidad en las instituciones (Díaz, 2010).

Para garantizar que la seguridad de la información es gestionada correctamente, se debe hacer uso de un proceso sistemático, documentado y conocido por toda la organización, desde un enfoque de riesgo empresarial. Este proceso es el que constituye un SGSI.

La norma ISO/IEC 2007 adopta el modelo del proceso PHVA, el cual es tradicional en los sistemas de gestión y se puede aplicar a todos los procesos SGSI.

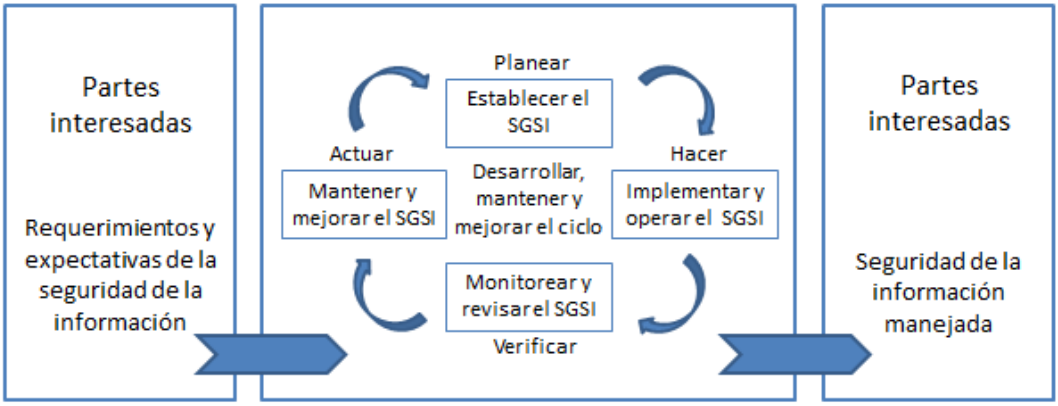



**Figura 10.** Modelo PDCA aplicado a los procesos SGSI (ISO/IEC 27001, 2005)

A continuación una breve descripción de cada etapa del proceso del SGSI:

(1) Planear: Establecer el SGSI. Establecer política, objetivos, procesos y procedimientos SGSI relevantes para manejar el riesgo y mejorar la seguridad de la información para entregar resultados en concordancia con las políticas y objetivos generales de la organización.

(2) Hacer: Implementar y operar el SGSI. Implementar y operar la política, controles, procesos y procedimientos SGSI.

(3) Verificar: Monitorear y revisar el SGSI. Evaluar y, donde sea aplicable, medir el desempeño del proceso en comparación con la política, objetivos y experiencias prácticas SGSI y reportar los resultados a la gerencia para su revisión.

(4) Actuar: Mantener y mejorar el SGSI. Tomar acciones correctivas y preventivas, basadas en los resultados de la auditoría interna SGSI y la revisión gerencial u otra información relevante, para lograr el mejoramiento continuo del SGSI.



*3.1.4. Marco legal y jurídico de la seguridad*

El creciente uso de las nuevas tecnologías ha propiciado la creación de un marco legal jurídico que proteja a todas las partes interesadas en el uso de estas tecnologías, intercambio y tratamiento de la información a través de ellas. Cada día surgen nuevas formas de delito informático que pueden afectar a la seguridad de la información en las organizaciones. Por ello, cumplir con la legislación vigente en Chile es uno de los requisitos bases que se deben satisfacer para implantar y certificar un SGSI. Su cumplimiento protegerá de amenazas externas e internas, nos permitirá respetar los derechos de los pacientes y proveedores y evitará infracciones involuntarias con sus respectivos costos.

A continuación, se detallan las leyes que están relacionadas con seguridad de la información:

(1) Norma Chilena 27.777 → Homologación de ISO 17799 (ISO 27002). TI: Código de práctica para la GSI.
(2) Ley Nº 19.233 →Los delitos informáticos y la función de auditoría informática.
(3) Decreto Supremo 93 → Adopción de medidas destinadas a minimizar los efectos perjudiciales de los mensajes electrónicos.
(4) Ley Nº 17.366 → Propiedad intelectual.
(5) Ley Nº 19.039 → Ley de propiedad industrial.
(6) Ley Nº 19.628 →Sobre protección de la vida privada.
(7) Ley Nº 19.799 → Documentos electrónicos, firma electrónica y servicios de certificación de dicha firma.
(8) Ley Nº 19.880 → Bases de los procedimientos administrativos que rigen los actos de los órganos de la administración del estado.
(9) Ley Nº 20.285 →Acceso a la información pública.
(10) Ley Nº 20.584 → Derechos y deberes de las personas en atención de salud, acciones vinculadas a la atención en salud.
(11) Decreto 14 → Aprueba reglamento de la Ley Nº 19.799.
(12) Decreto 83 →Aprueba norma técnica para los órganos de la administración del estado sobre seguridad y confidencialidad de los documentos electrónicos.

*3.1.5. Unidad de Emergencia Adulto del HCVB*

El Hospital Carlos Van Buren (HCVB) es el establecimiento de mayor complejidad de la Red Asistencial del Servicio de Salud Valparaíso-San Antonio (SSVSA).

El modelo general de atención de urgencia representa principales procesos llevados a cabo en la atención de salud de un paciente en el Servicio de Urgencia. Esto se inicia con el proceso administrativo de la admisión, luego el paciente es categorizado en el selector de demanda, de donde resulta una categoría que representará el grado de urgencia que tiene el paciente de ser atendido. Con esta categorización, el equipo de salud realiza las coordinaciones necesarias para lograr que el paciente reciba atención clínica necesaria y en el tiempo de acuerdo a su categorización.

Una vez que el paciente es evaluado por un médico u otro profesional de la salud, se decide el plan de acción a seguir. Dependiendo del estado de salud del paciente, el plan de acción podría contemplar la realización de exámenes para el apoyo diagnóstico, administración de indicaciones médicas, hospitalización o el traslado del paciente a pabellón para una cirugía. Una vez finalizadas todas las atenciones de urgencia, el paciente se retira de la Unidad (es dado de alta) en alguno de los siguientes estados: mejorado, no mejorado o fallecido. El alta del paciente va acompañada de un acto administrativo, se cierra el evento y se entregan informe con los Datos de la Atención de Urgencia llamada hoja DAU (Logra, 2012).

El HCVB posee cuatro tipos de Servicios de Urgencia, los cuales son: Unidad de Emergencia Adulto (UEA), Gineco-obstétrica, Unidad de Emergencia Infantil (UEI) y el Sistema de Atención Médica de Urgencia (SAMU). Este trabajo de título se centra específicamente en la UEA.

El proceso de atención de urgencia es el conjunto de actividades médicas, clínicas y administrativas que se llevan a cabo en el servicio de urgencia. Tiene como objetivo brindar cuidados de salud a un paciente que necesita atención médica inmediata. El proceso se inicia ya sea por demanda espontánea, derivación desde la atención primaria o desde el SAMU. En el caso de ser un paciente no grave, comienza el proceso de Admisión del Paciente, en donde el paciente/familiar/equipo de salud que acompaña a la persona que realizará éste trámite entrega los datos necesarios. En caso de que sea paciente grave, este es enviado directamente a Evaluación Médica en donde se lleva a cabo la reanimación, que consiste en realizar todos los procesos de la fase de atención pero de forma más rápida debido a la condición en que ingresa el paciente. A su vez, paralelamente se inicia el proceso de Coordinación de Actividades y el proceso de Atención y Entrega de Información al Público; ambos procesos están presentes durante toda la estadía del paciente en la Atención de Urgencia. La Coordinación de Actividades, tiene como objetivo principal coordinar que se lleven a cabo todas las actividades relacionadas con el paciente en su atención clínica. En tanto, la Atención y Entrega de Información al público, tiene como objetivo principal mantener informados periódicamente, y en forma proactiva, a los familiares y/o acompañantes, respecto del estado, evolución y procedimientos realizados a las personas que se encuentran en atención, mejorando de ésta forma la satisfacción usuaria. Luego de la Admisión, el paciente ingresa al Selector de Demanda, cuyo objetivo es categorizar el nivel de urgencia del paciente con la finalidad de determinar qué tan rápido debe ser atendido (Logra, 2012).

La categorización consiste en lo siguiente:

- Categoría C1: Emergencia vital → Atención inmediata.

  Acción clínica; evaluación y manejo simultáneo (sin tiempo de espera). Por su condición de riesgo vital, el paciente es directamente reanimado.
- Categoría C2: Emergencia Evidente →Atención antes de los 30 minutos.

  Acción clínica; emergencia médica. Paciente con compromiso vital evidente y hemodinamia alterada. Por su condición, el paciente debe ser estabilizado.
- Categoría C3: Urgencia → Atención antes de 90 minutos o en su defecto reevaluar.

  Acción clínica; paciente con hemodinamia inestable o compromiso neurológico o de patrón respiratorio evidente. Por su condición, el paciente debe ser tratado.
- Categoría C4: Urgencia inmediata→ Atención antes de 180 minutos o en su defecto reevaluar.

  Acción clínica; atención médica de urgencia. Paciente hemodinámicamente estable que requiere un procedimiento diagnóstico o terapéutico) asociado. Por su condición, el paciente debe ser evaluado.

- Categoría C5: Atención general
  Acción Clínica Atención Médica general, paciente estable. Por su condición clínica, el paciente es educado por el equipo médico (Guzmán y Moreno, 2011).



En el caso de que el paciente no haya sido atendido dentro de los tiempos estipulados debe ser categorizado nuevamente, ya que luego de haber transcurrido una cierta cantidad de tiempo lo más probable es que su estado haya sufrido modificaciones. Posterior a la categorización, continúa la evaluación médica, en donde se establece una hipótesis diagnóstica, se dejan indicaciones en donde se lleva a cabo el proceso de gestión de indicaciones, siendo las posibles opciones: imágenes, medicamento, procedimientos, laboratorio, interconsulta u otras indicaciones.

En algunos casos, el paciente necesita ser derivado a Indicación de Observaciones, en donde el equipo de salud, después de un tiempo, evaluará su evolución y pasos a seguir.

Finalmente se procede a dar el alta al paciente, alta administrativa y alta clínica, que consiste en la entrega de los certificados e indicaciones del alta y pago de la atención en caso que corresponda (Logra, 2012). Diagrama del proceso de urgencia en Anexo 7.

El proceso de urgencia consta de los siguientes subprocesos (Logra, 2012):

- Admisión de urgencia.
- Atención y entrega de información al público.
- Selector de demanda.
- Coordinación de actividades.
- Evaluación clínica.
- Indicación de observaciones.
- Registro de prestaciones e insumos.
- Alta administrativa.
- Alta médica.

La UEA tiene como propósito atender a toda persona que tenga una enfermedad de alta complejidad médica o quirúrgica, que requiera ser resuelta antes de 24 horas, por riesgo vital, secuelas, o descompensación aguda de enfermedades crónicas. Las personas que pueden ser atendidas en esta unidad son los mayores de 15 años. Una vez atendido el paciente, este será hospitalizado, derivado a su centro de atención primaria de salud o dado de alta (Hospital Carlos Van Buren, 2015).

### *3.2. Diseño de la Propuesta*

El desarrollo de esta metodología para la implementación de un SGSI será abordado con la metodología de trabajo esquematizada en la siguiente figura, que incluye dos (02) etapas y un (01) producto, basados en los objetivos específicos planteados y los criterios de la norma ISO/IEC 27001.

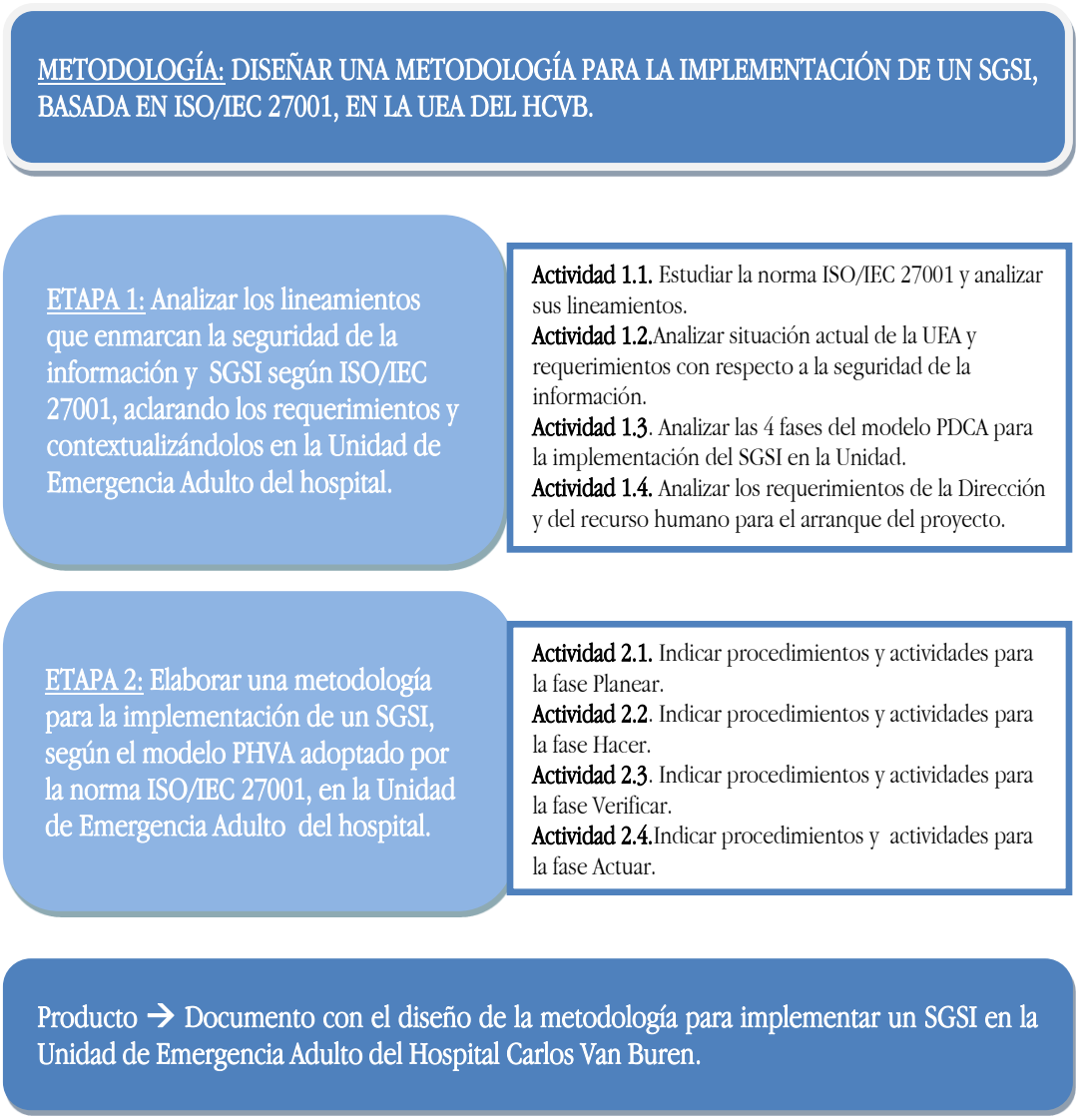



**Figura 11.**Metodología de trabajo (Elaboración propia).

A continuación, se detallará la metodología de las etapas y sus correspondientes actividades propuestas para este trabajo de Título.

**Etapa 1: Analizar los lineamientos que enmarcan la seguridad de la información y SGSI, según ISO/IEC 27001, aclarando los requerimientos y contextualizándolos en la Unidad de Emergencia Adulto del hospital.**

Actividad 1.1: Estudiar la norma ISO/IEC 27001 y analizar sus lineamientos. Conocer directrices y criterios que entrega la norma para la implementación de un SGSI en organizaciones. Analizar los lineamientos que gobiernan los sistemas y redes de seguridad de la información.

Actividad 1.2: Analizar situación actual de la UEA y requerimientos con respecto a la seguridad de la información. Conocer a modo general medidas de seguridad y controles que posea la unidad en cuanto a la información que se maneje en ella.

Actividad 1.3: Analizar las 4 fases del modelo PDCA para la implementación del SGSI en la unidad. Entender en qué consiste cada etapa del ciclo continuo PDCA y las actividades que contempla, para luego relacionarlo con los procesos SGSI.

Actividad 1.4: Analizar los requerimientos de la Dirección y del recurso humano para el arranque del proyecto. Conocer los requerimientos que solicita la norma ISO/IEC 27001 de acuerdo a estos dos ámbitos, para dar inicio a la implementación del SGSI (arranque del proyecto).

**Etapa 2: Elaborar una metodología para la implementación de un SGSI, según el modelo PHVA adoptado por la norma ISO/IEC 27001, en la Unidad de Emergencia Adulto del hospital.**

Actividad 2.1: Indicar procedimientos y actividades para la fase Planear. Política de seguridad, definir el alcance del SGSI; definir herramientas para la identificación de activos, identificar riesgos e impacto; definir la forma de tratamiento de los riesgos; análisis y evaluación del riesgo.

Actividad 2.2: Indicar procedimientos y actividades para la fase Hacer. Definir el plan de tratamiento de riesgo; definir forma de gestión del riesgo; seleccionar y definir controles para su implementación y mitigación en la UEA; definir formas para concientizar a todo el personal de la Unidad en relación a la seguridad de la información; objetivos de control e indicadores.

Actividad 2.3: Indicar procedimientos y actividades para la fase Verificar. Analizar formas de revisión del SGSI; analizar herramientas propuestas para la revisión; indicar la planificación de auditorías internas.

Actividad 2.4: Indicar procedimientos y actividades para la fase Actuar. Analizar herramientas propuestas para el establecimiento de planes de acción; revisar posibles acciones correctivas y preventivas para resolver disconformidades.

### *3.3. Implementación*

En esta sección se señala la manera que se ha desarrollado el trabajo, de acuerdo a las etapas planteadas en el Diseño de la Propuesta (numeral 3.2).

**ETAPA 1: Analizar los lineamientos que enmarcan la seguridad de la información y SGSI, según ISO/IEC 27001, aclarando los requerimientos y contextualizándolos en la Unidad de Emergencia Adulto del hospital.**

Es necesario estudiar y analizar detalladamente la norma ISO/IEC 27001, de esta forma se logra entender las partes que la conforman, estructura, lineamientos, requerimientos, entre otras cosas. Luego de estudiar y conocer la norma, se debe conocer la situación actual de la UEA con respecto a la seguridad de la información. Saber si poseen controles y cuáles son y las normas reguladas por leyes relacionadas al mismo ámbito. Luego, es necesario analizar la metodología PHVA, comprender sus etapas y como este modelo se aplica a los procesos SGSI como lo estipula la norma ISO/IEC 27001. Finalmente, se deben analizar los requerimientos de la Dirección y recurso humano para el arranque del proyecto de la implementación del SGSI.

Actividad 1.1. Estudiar la norma ISO/IEC 27001 y analizar sus lineamientos.

Para analizar los lineamientos de la norma ISO/IEC 27001, fue necesario estudiarla y analizar su estructura y directrices para así comprender cada una de sus partes. Analizar el enfoque que posee, su alcance, aplicación, requerimientos generales, de documentación y como muestra los procesos del SGSI.

Además de la norma ISO/IEC 27001, existe gran cantidad de información disponible que trata sobre lo qué es y en qué consiste un SGSI basado en la norma ISO/IEC 27001. De cierta manera, el contar con un alto volumen de información posee sus beneficios y también sus contras. Como beneficios, podemos nombrar la facilidad de adquirir información ya que ésta se encuentra disponible y al alcance. Por otra parte, respecto a los contras, podemos nombrar el tiempo que se emplea en la revisión de estos documentos y su selección para luego sintetizar la información que más se adecue a lo que se plantea como producto, dedicando tiempo considerable.

Se encontró información respecto al plan de trabajo que ha desarrollado el Departamento de Gestión Sectorial TIC perteneciente al MINSAL, relacionado con la seguridad de la información. Se analizaron las etapas que consideraron para la implementación de un SGSI, ya que es parte del Programa de Mejoramiento de Gestión (PMG) y lo que han aplicado actualmente. Para la obtención de esta información, se utilizó la página web de la Estrategia Digital de Salud del MINSAL, en donde en la sección prensa se detallan los avances que han tenido en la implementación, junto con las reuniones y auditorias que han estado efectuando para ir controlando y mejorando esto mismo. Además, se contó con el apoyo de Enrico Olguín, Jefe del Sub-departamento de Informática del SSVSA, con el cual se tuvieron reuniones (minutas de reunión en Anexo 11) informativas y de consulta con respecto a la seguridad de la información a nivel del servicio y hospitales pertenecientes al servicio.

Actividad 1.2. Analizar situación actual de la UEA y requerimientos con respecto a la seguridad de la información.

Para conocer y analizar la situación actual de la UEA con respecto a la seguridad de la información, se realizaron reuniones el segundo semestre del 2014 junto al entonces Enfermero Supervisor de la UEA, José Gómez, que actualmente ocupa el cargo de Enfermero Coordinador Área Crítica. En la primera reunión, se presentó el tema central del trabajo, lo que expone la norma ISO/IEC 27001 y la forma en que será abordada. Se establecieron canales de comunicación y el plan de trabajo en esta primera etapa, se presentaron los objetivos de trabajo y las decisiones que a ellos les correspondían tomar respecto a los mismos. En un principio fue complejo reunirnos por falta de coordinación, pero desde noviembre del 2014 esto mejoró. También, se analizaron los controles y requerimientos de seguridad de la información que como Unidad necesitan (para ver minutas de reunión ir al Anexo11). Estos requerimientos de seguridad se analizaron según las siguientes fuentes principales (Project Management, 2014):

(1) Fuente que se deriva de evaluar los riesgos para la organización, tomando en cuenta la estrategia general y los objetivos de la organización. A través de la evaluación del riesgo, se identifican las amenazas para los activos, se evalúa la vulnerabilidad y probabilidad de ocurrencia y se calcula el impacto potencial.
(2) Los requerimientos legales, reguladores, estatutarios y contractuales que tienen que satisfacer una organización, sus socios comerciales, contratistas y proveedores de servicio; y su ambiente socio-cultural.
(3) El conjunto particular de principios, objetivos y requerimientos comerciales para el procesamiento de la información que una organización ha desarrollado para sostener sus operaciones.

En el caso de la UEA, se optó por la primera fuente, la que se deriva de una evaluación de riesgos, identificando amenazas para los activos, sus vulnerabilidades y su impacto.

Para conocer el funcionamiento del proceso de Urgencia, además de las preguntas realizadas en las reuniones, se analizó la "Consultoría para la Estandarización de procesos de redes asistenciales MINSAL" realizado por LOGRA S.A el año 2012, documento que hace referencia a los objetivos de los procesos, mapa de procesos de atención de urgencia, modelos de procesos estandarizados (subprocesos) y oportunidades de mejora.

Actividad 1.3. Analizar las 4 fases del modelo PDCA para la implementación del SGSI en la Unidad.

Se buscó información acerca de la metodología PDCA (PHVA) en la web, con la idea de comprender su estructura y su adaptación a los procesos del SGSI. Se volvió a repasar la norma ISO/IEC 27001 en las partes donde entrega las directrices y lo que debe contener cada una de las fases del SGSI de acuerdo a esta metodología (ciclo continuo).

Con la idea de organizar la información contenida en la ISO/IEC 27001 respecto al SGSI en sus cuatro fases según la metodología PHVA, se realizó la siguiente figura, la cual contiene las actividades a realizar en cada una de las fases:


**Figura 12.** Metodología PHVA aplicado a los procesos del SGSI según ISO/IEC 27001(Elaboración propia)

Actividad 1.4. Analizar los requerimientos de la Dirección y del recurso humano para el arranque del proyecto.

Es la primera parte de los resultados de este trabajo. Es el punto que da inicio al desarrollo de la metodología de implementación: el arranque del proyecto. Se analiza de forma previa a la aplicación del modelo PHVA, por lo que no es parte de este último.

Para conocer que se debe hacer para arrancar este proyecto, se analizó nuevamente la norma ISO/IEC 27001, la cual es clara en indicar que se debe contar con el apoyo y compromiso de la Dirección. Esto no por el sólo hecho de ser considerado un punto especial, sino por el cambio de cultura que se debe realizar en conjunto con el recurso humano. En este punto, el alcance que tiene este trabajo sólo consiste en indicar este requisito para cuando quieran realizar la

implementación de un SGSI en la UEA (ya que es el diseño una metodología y no la implementación de esta).

**ETAPA 2: Elaborar una metodología para la implementación de un SGSI, según el modelo PHVA adoptado por la norma ISO/IEC 27001, en la Unidad de Emergencia Adulto del hospital.**

Para desarrollar la metodología de la implementación de las cuatro etapas del SGSI (nombradas en la figura 12) en la UEA, se procedió a repasar la norma ISO/IEC 27001 en cuanto a las directrices y requerimientos que se deben satisfacer en las fases Planear, Hacer, Verificar y Actuar. Esta información se complementó con la obtenida en la página web en español de la familia de normas ISO 27000, en dónde se explica de modo general las directrices que estipula la ISO/IEC 27001. Además, fue de gran apoyo la tesis titulada "Diseño de una metodología para la implementación del SGSI en el sector de laboratorios de análisis microbiológicos, basado en ISO 27001" de Buitrago, Bonilla y Murillo junto con la tesis titulada "Elaborar una metodología aplicando la norma ISO/IEC 27001 en la implementación de un SGSI en el Desitel de la ESPOCH" de Gabilanes (ambas tesis nombradas en el numeral 2.1.3 de buenas prácticas y referenciadas).

Estas tesis son propuestas similares a la del presente trabajo de Título, pero su enfoque, alcance e institución de aplicación es distinta.

Actividad 2.1. Indicar procedimientos y actividades para la fase Planear.

Se repasó lo que indicaba la norma ISO/IEC 27001 en cuanto a procedimientos y actividades a realizar en esta primera fase del ciclo continuo (ver figura 13).

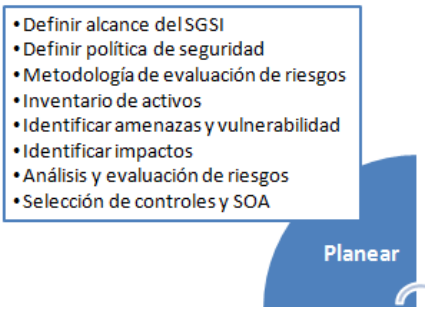



**Figura 13.** Fase Planear de la Metodología PHVA aplicado a los procesos del SGSI. (Elaboración propia)

Para las actividades siguientes: definir el alcance del SGSI, definir política de seguridad y metodología de evaluación de riesgos, se explicó cada paso según lo que indicaba la ISO/IEC 27001 y lo que resumía la página oficial de ISO 27000 en español.

En inventario de activos, identificar amenazas y vulnerabilidad e identificar impactos, la norma ISO/IEC sólo indica que hay que realizar una identificación de activos dentro del alcance del SGSI, sus amenazas, vulnerabilidades e impactos que pueden tener las pérdidas de confidencialidad, integridad y disponibilidad (perfil CID). En apoyo a estas actividades, se le recomendó a la enfermera supervisora de urgencia hacer un inventario de activos que tuviera los siguientes campos para facilitar su identificación: activo, tipo de activo, detalle, propietario, ubicación y perfil CID, resultando la tabla mostrada en la figura 14.

| | Proceso: | | | | | Fecha revisión: | | |
|---|---|---|---|---|---|---|---|---|
| | Activo | Tipo de activo | Detalle | Propietario | Ubicación | Perfil CID | | |
| | | | | | | C | I | D |
| 1 | | | | | | | | |
| 2 | | | | | | | | |
| 3 | | | | | | | | |
| 4 | | | | | | | | |
| 5 | | | | | | | | |
| 6 | | | | | | | | |
| 7 | | | | | | | | |
| 8 | | | | | | | | |
| 9 | | | | | | | | |
| 10 | | | | | | | | |

C: confidencialidad I: Integridad D: Disponibilidad

Elaborado por:
Revisado por:

**Figura 14.** Inventario de activos (elaboración propia)

Luego, se procedió a la identificación de activos de información en la Unidad de Urgencia en conjunto con la supervisora y dos enfermeros de la Unidad. Se lograron identificar seis (06) activos, a los cuales también se les identificó sus amenazas y vulnerabilidad. Posterior a ello, y como lo indica la norma, se procedió a la identificación de su impacto en cuanto al perfil CID. Para ello, se averiguó en la web los valores que se le podía dar al impacto de la pérdida en cuanto a la confidencialidad, integridad y disponibilidad de la información, resultando en la clasificación: baja, media y alta. Esta clasificación fue adquirida de una guía de implementación de SGSI de la empresa ATSEC (Atsec, 2014). Esta información estaba en inglés, por lo que se tradujo al español. La tabla original, con la descripción del perfil CID y su impacto por pérdida se muestra en la figura 15.

| Impact of Loss ► | LOW | MEDIUM | HIGH |
|---|---|---|---|
| ***Confidentiality***<br><br>Ensuring that information is accessible only to those authorized to have access | The unauthorized disclosure of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals. | The unauthorized disclosure of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. | The unauthorized disclosure of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals. |
| ***Integrity***<br><br>Safeguarding the accuracy and completeness of information and processing methods | The unauthorized modification or destruction of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals. | The unauthorized modification or destruction of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. | The unauthorized modification or destruction of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals. |
| ***Availability***<br><br>Ensuring that authorized users have access to information and associated assets when required | The disruption of access to or use of information or an information system could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals. | The disruption of access to or use of information or an information system could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. | The disruption of access to or use of information or an information system could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals. |

**Figura 15.** Matriz CID (Atsec, 2014)

Luego, la norma indica que se debe hace un análisis y evaluación de riesgos. Para esto, se recomendó utilizar la herramienta de Análisis Modal de Fallas y Efectos (AMFE). La información relativa a la aplicación de esta herramienta fue estudiada de una guía de buenas prácticas elaborada por Bestretén y Orriols, en la cual se explicaba la función de esta herramienta, definiciones de términos fundamentales del AMFE, la descripción del método y un ejemplo de aplicación. Para el desarrollo de esta parte se tomó como referencia la guía de buenas prácticas NTP "Análisis modal de fallas y efectos" del Instituto Nacional de Seguridad e Higiene en el Trabajo (INSHT) (Bestratén, Orriols y Mata., 2004). La tabla del AMFE realizada en la UEA fue completada en conjunto con la Supervisora de la Unidad. Además, se explicaron de forma general los 4 tipos de tratamientos para el riesgo que indica la norma, de los cuales se debe seleccionar el que más se acomode a los requerimientos y alcance de la Unidad.

Finalmente, la última actividad a realizar en esta etapa según la ISO/IEC 27001 es la selección de controles, los cuales fueron estudiados del Anexo A de la norma, y también el SOA, explicando su contenido de acuerdo a lo que indica la norma.

Actividad 2.2. Indicar procedimientos y actividades para la fase Hacer.

Se repasó lo que indicaba la norma ISO/IEC 27001 en cuanto a procedimientos y actividades a realizar en esta segunda fase del ciclo continuo (ver figura 16).

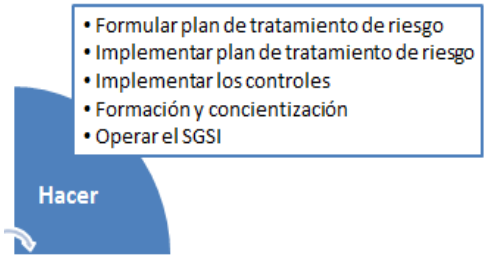



**Figura 16.** Fase Hacer de la Metodología PHVA aplicado a los procesos del SGSI. (Elaboración propia)

Para la formulación de plan de tratamiento del riesgo (mitigación del riesgo), la explicación de las fases para su implementación fueron apoyadas por lo que indica el módulo 9 de un informe de José Poveda que trataba de la gestión y tratamientos del riesgo.

Con respecto a la actividad de implementar los controles, al ser un diseño de metodología, se realizó un listado con los posibles controles a implementar en la Unidad. Esta selección se realizó de acuerdo a la importancia de su aplicación, la identificación de falencias en ciertas áreas y lo que indicó la supervisora de la Unidad. En este listado se indicó el nombre del control (según lo que indica el Anexo A de la norma), el objetivo de control y algunas medidas a considerar en su implementación.

En las actividades que conllevan la formación y concientización, se indicó lo que la norma expone para este punto, sin agregar información extra.

En lo que respecta la operación del SGSI, se indicó lo que debe realizar la Unidad para que el SGSI comience a funcionar. Se analizó lo que la ISO/IEC 27001 indica con respecto a las acciones que formarán parte de la mejora continua del SGSI, la definición de objetivos y el establecer indicadores que midan el cumplimiento de ellos. También se indicó una tabla con criterios para la selección de indicadores como guía para el personal que vaya a establecerlos. Esta tabla se obtuvo de la Metodología de línea base de indicadores, creado por el Departamento Administrativo Nacional de Estadística DANE (Dane, 2015).

Actividad 2.3. Indicar procedimientos y actividades para la fase Verificar.
Se repasó lo que indicaba la norma ISO/IEC 27001 en cuanto a procedimientos y actividades a realizar en esta tercera fase del ciclo continuo (ver figura 17).

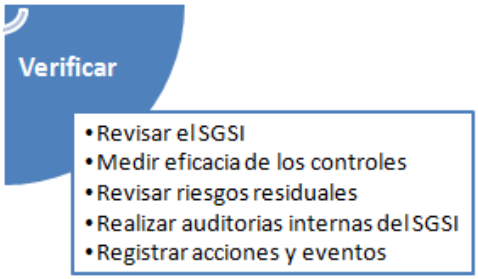



**Figura 17.** Fase Verificar de la Metodología PHVA aplicado a los procesos del SGSI. (Elaboración propia)

Se indicó todo lo que abarca la norma ISO/IEC 27001 con respecto a esta fase, lo que es la revisión del SGSI, revisión de los riesgos residuales, la labor que cumplen las auditorías internas y el registro de las acciones y eventos que se identificaron en ellas. Como apoyo e información extra, se nombraron algunas herramientas que pueden ayudar en la medición de la eficacia de los controles que vayan a implantar, a través del seguimiento del SGSI, estas herramientas son: cartas de control, balanced scorecard, cuadro de mando integral y planes de verificación del SGSI.

Actividad 2.4.Indicar procedimientos y actividades para la fase Actuar.
Se repasó lo que indicaba la norma ISO/IEC 27001 en cuanto a procedimientos y actividades a realizar en esta cuarta y última fase del ciclo continuo (ver figura 18).

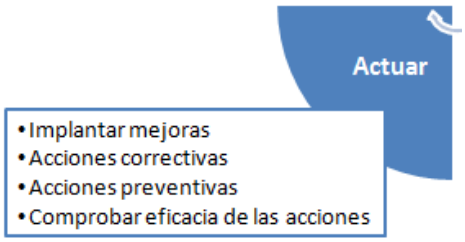



**Figura 18.** Fase Actuar de la Metodología PHVA aplicado a los procesos del SGSI. (Elaboración propia)

En esta última fase del SGSI, las indicaciones que se entregaron a la UEA en la metodología propuesta, fueron las mismas que indica la ISO/IEC 27001 para la implantación de mejoras, acciones a realizar y la comprobación de la eficacia de las acciones tomadas. No se explayó más en esta fase ni en la anterior, ya que primero es necesaria la selección de controles, objetivos de control y posteriormente si aplicación en la Unidad. Una vez realizadas estas actividades, se puede verificar el funcionamiento del SGSI y de acuerdo al resultado de lo verificado, se pueden implantar mejoras.

Este trabajo de Título está enfocado mayormente en la etapa de planear, ya que las siguientes tres etapas (hacer, verificar y monitorear) al ser prácticas sólo se darán los pasos a seguir para aplicarlas en la UEA.

## 4. Resultados

Una de las bases fundamentales para iniciar un proyecto de este tipo es el apoyo claro y decidido de la Dirección de la institución. Esto no sólo por ser considerado un punto especial, sino porque conlleva un cambio de cultura que debe partir desde arriba, además que la implantación de un SGSI hace necesario el impulso constante de la Dirección (ISO/IEC 27000, 2014).

En este sentido, la norma ISO/IEC 27001 hace referencia de los compromisos que debe tener tanto la Dirección como la gestión de los recursos para lograr el funcionamiento del SGSI. Estos compromisos son:

- La dirección debe proporcionar evidencia de su compromiso con el establecimiento, implementación, operación, monitoreo, revisión, mantenimiento y mejoramiento del SGSI a través de: establecer una política SGSI; asegurar que se establezcan los objetivos y planes SGSI; establecer roles y responsabilidades para la seguridad de la información; comunicar a la organización la importancia de lograr los objetivos de seguridad de la información y cumplir la política de seguridad de la información; sus responsabilidades bajo la ley y la necesidad de un mejoramiento continuo; proporcionar los recursos necesarios; decidir el criterio para la aceptación del riesgo y sus niveles; asegurar que se realicen auditorías internas SGSI y realizar revisiones del SGSI (ISO/IEC 27001, 2005).
- La Dirección debe determinar y proporcionar los recursos necesarios para: establecer, implementar, operar, monitorear, revisar, mantener y mejorar un SGSI; asegurar que los procedimientos de seguridad de la información respalden los requerimientos del negocio; identificar y tratar los requerimientos legales y reguladores y las obligaciones de seguridad contractuales; mantener una seguridad adecuada mediante la correcta aplicación de todos los controles implementados; llevar a cabo revisiones cuando sean necesarias, y reaccionar apropiadamente ante los resultados de estas revisiones donde sea necesario y mejorar la efectividad del SGSI (ISO/IEC 27001, 2005).

La metodología de implementación será expuesta y explicada en las cuatro etapas del ciclo continuo aplicado al proceso SGSI, explicado anteriormente en el numeral 3.3 (implementación).

### *4.1. Planear*

En esta primera etapa del ciclo, se define el alcance que tendrá la implementación del SGSI dentro del hospital, además de las políticas y lineamientos sobre los que se desarrollará. Se presentan herramientas para la metodología de evaluación de riesgos, comprendiendo su identificación, análisis y evaluación, de acuerdo a la información que se vería afectada y al impacto que esto tendría. También un objetivo de esta etapa es definir el tratamiento o forma de tratamiento de los riesgos que han sido identificados (ISO/IEC 27000, 2014).

#### *4.1.1. Alcance del SGSI*

Como primer paso, el hospital debe establecer el alcance que tendrá el SGSI, ya que no necesariamente debe abarcar la institución en su totalidad, es más, se recomienda empezar por un alcance limitado. Este alcance junto con los límites del SGSI debe estar en función de las características del negocio, organización, localización, activos y tecnología.

También es importante disponer de un mapa de procesos, en el que se defina de forma clara el alcance y proceso o los procesos que abarcará el SGSI; determinar las terceras partes como proveedores, clientes, etc., que tienen influencia sobre la seguridad de la información; crear mapas de alto nivel de redes y sistemas; definir ubicaciones físicas; disponer de diagramas organizativos; definir claramente los requisitos legales y contractuales relacionados con seguridad de la información (ISO/IEC 27000, 2014).

Para el caso de este trabajo, el alcance será la Unidad de Emergencia Adulto UEA, ya que es un proceso clínico que considera un escenario potencial adverso (Olguín, 2014).

*4.1.2. Política del SGSI*

Como primera instancia, es importante que el hospital cuente con una misión y visión clara, los que en su conjunto permiten desplegar estrategias y procesos organizacionales. La política del SGSI es un documento general que debe estar alineada con los objetivos organizacionales y estratégicos del hospital, una especie de "declaración de intenciones" de la Dirección que debe considerar el marco general y los objetivos de seguridad de la información de la institución. Debe contemplar los requisitos de negocio además de considerar los requerimientos legales o contractuales relativos a la seguridad de la información, establecer los criterios con los que se va a evaluar el riesgo y que esté aprobada por la Dirección. Además, debe tener la metodología y los criterios con los que se va a evaluar el riesgo. Esta política debe ser de conocimiento público por lo que su divulgación en la institución es indispensable.

La UEA debe desarrollar una política de seguridad de la información que esté alineada con los objetivos organizacionales del hospital, y a su vez, alineada con la política de seguridad de este mismo. Esta política debe ser revisada y aprobada por la Dirección del hospital.

*4.1.3. Metodología de evaluación de riesgos*

La evaluación de riesgos es el proceso de identificación de riesgos mediante el análisis de las amenazas, sus repercusiones, las vulnerabilidades de los sistemas de información y las instalaciones de procesamiento de estas. La elección de un método de evaluación de riesgos es quizás una de las decisiones más importantes de la implementación de un SGSI. Hay que considerar que el riesgo nunca es totalmente eliminable, por lo que es necesario definir una estrategia de aceptación de riesgo estableciendo criterios de aceptación del riesgo y especificar los niveles de riesgo aceptable.

Para cumplir con los requisitos que informa la ISO/IEC 27001, se debe definir y documentar un método de evaluación de riesgos y luego aplicarlo para identificar los activos de información, tomar decisiones sobre qué riesgos son intolerables y que por lo tanto deben ser mitigados, y gestionar los riesgos residuales a través de políticas consideradas, procedimientos y controles.

Existen varias alternativas de metodologías de evaluación de riesgos. La Unidad puede optar por cualquiera de ellas, combinarlas o crear una propia, ya que la ISO/IEC 27001 no impone ninguna ni tampoco da indicaciones de cómo definirla. Sin embargo, esta norma entrega una serie de directrices que guían en esta materia, definiendo las tareas que este método debe realizar. Estas tareas son:

(1) Identificar todos aquellos activos de información que tienen algún valor para la Unidad de Urgencia, que están dentro del alcance del SGSI y a sus responsables directos denominados propietarios.
(2) Identificar las amenazas relevantes asociadas a los activos identificados
(3) Identificar las vulnerabilidades que puedan ser aprovechadas por dichas amenazas
(4) Analizar y evaluar el riesgo basado en los niveles de confidencialidad, integridad y disponibilidad.

Siguiendo esta línea, en los ítems que vienen a continuación se desarrollan estas tareas.

*4.1.4. Identificación de activos*

La identificación del riesgo contempla de forma inicial hacer una lista de todos o la mayoría de los activos de información que están dentro del alcance designado para la implementación del SGSI, teniendo en cuenta su ubicación, responsable o propietario. Para esto, se realizó una planilla que

contenga los campos pertinentes para tener la información necesaria respecto a cada activo. A continuación, se detalla cada campo que contiene el inventario:

(1) Proceso → Corresponde al proceso o subproceso al cual pertenece el activo.
(2) Activo → Es la identificación del activo, nombre o como es reconocido por la organización.
(3) Tipo de activo →Es la clasificación que tiene el activo.
(4) Detalle → De ser necesario, escribir más información acerca del activo para identificarlo más fácilmente.
(5) Ubicación → Corresponde al lugar físico donde se encuentra ubicado el activo.
(6) Perfil CID → Indica el impacto para la organización que tendría la pérdida o alteración del activo en cuanto a confidencialidad, integridad y disponibilidad. Este campo será detallado en el punto (f) "Identificación de impacto".

Con respecto al tipo o clasificación del activo definido en el punto 3, existen tres niveles básicos de activos de información, los cuales son:

(a) La información propiamente tal, en sus múltiples formatos (papel, digital, texto, imagen, audio, video, etc.).
(b) Los equipos/sistemas/infraestructura que soportan esta información.
(c) Las personas que utilizan la información y que tienen conocimiento de los procesos institucionales (GSI, 2012).

En la tabla siguiente, se presenta el inventario de activos del proceso de Urgencia adulto. Esta información fue levantada junto a José Gómez y Gastón Letelier, enfermeros de la UEA; en conjunto con Karen Soto, enfermera Supervisora de la UEA.

HOSPITAL CARLOS VAN BUREN
UN MEJOR HOSPITAL PARA TODOS

**Proceso:** Urgencia adulto

| Nº | Activo | Tipo de activo | Detalle | Propietario | Ubicación |
|---|---|---|---|---|---|
| 1 | DAU | Información | Datos de la atención de urgencia | Jefe Recaudación | Recaudación |
| 2 | Sistema de orden | Sistemas | Sistema informático con el que se trabaja | Jefe Informática | Departamento Informática |
| 3 | Equipo clínico | Personas | Médicos, enfermeras, paramédicos | Jefe Recurso Humano | Lugar de atención, puesto de trabajo |
| 4 | Computadores | Equipos | Utilizados por equipo clínico | Jefe Informática | Oficinas |
| 5 | Instalaciones físicas | Infraestructura | Lugar donde se desarrolla el proceso | Jefe de Calidad | Coordenadas de la infraestructura |
| 6 | Ficha médica | Información | Historial clínico del paciente hospitalizado | Equipo Clínico | Recaudación |

**Elaborado por:** José Gómez, Gastón Letelier, Karen Soto, Vanessa Bello
**Revisado por:** Karen Soto

**Tabla 3.** Inventario de activos Urgencia Adulto (elaboración propia)

*4.1.5. Identificación de amenazas y vulnerabilidades.*

Luego de identificar cada activo, el siguiente paso es identificar sus riesgos y clasificarlos de acuerdo a sus amenazas y vulnerabilidades. Para identificar las amenazas y vulnerabilidades reales o potenciales, primeramente hay que tener claro el concepto de cada una de ellas, a continuación su definición:

- Amenaza: Posible causa de un incidente no deseado, que puede resultar en daños a un sistema u organización (ISO/IEC 27000, 2009). Una amenaza es la ocurrencia de cualquier evento que causa un impacto no deseado o pérdidas de activos de la organización (Pérez, 2011).
- Vulnerabilidad: La debilidad de un activo o control que puede ser explotada por una amenaza (ISO/IEC 27000, 2009). Es un ataque de vía potencial, una característica o combinación de características que permite a un adversario colocar a un sistema en un estado contrario a los deseos de las personas responsables o autorizadas e incrementa la probabilidad o magnitud del comportamiento no deseado del sistema. Posibilidad de ocurrencia de la materialización de una amenaza sobre un activo (Pérez, 2011).

Luego de aclarar ambos conceptos, es conveniente realizar una lista con las posibles amenazas y riesgos que pueden tener los activos identificados en el proceso de atención de urgencia adulto, para tener una mirada del riesgo potencial. Para la identificación de potenciales amenazas y vulnerabilidades para cada activo se sugiere realizar las siguientes actividades:

(1) Identificar las amenazas que puedan presentarse en forma accidental o intencional en la unidad con relación a los activos de información.
(2) Identificar las vulnerabilidades que puedan existir para que los activos y las amenazas que poseen resulten en esas vulnerabilidades.
(3) Para cada activo, se deberá realizar una descripción de la amenaza y vulnerabilidad y, utilizando la metodología de evaluación de riesgo designada anteriormente, asignar los niveles de confidencialidad, integridad y disponibilidad de ese activo.

A modo general, se cuenta con la siguiente información de amenazas y vulnerabilidades de los activos identificados en la tabla 3 (información entregada por los mismos Enfermeros de la UEA):

Amenazas:

- Computadores/sistemas informáticos amenazados por hackers, spyware, spam, virus, etc.
- Potenciales aplicaciones informáticas instaladas no autorizadas.
- Uso inapropiado del email y web por los funcionarios.
- Catástrofes y contingencias no previstas.
- Pérdida, sustracción, robo de información crítica de la organización en cualquier soporte.
- Divulgación de información.

Vulnerabilidades:

- Todos los funcionarios tienen acceso a información crítica. No existe restricción.
- Pérdida de información.
- Falta de controles e inspección de los soportes y activos de información.
- Información crítica en formato escrito (papel).
- Infraestructura antigua.

*4.1.6. Identificación del impacto.*

Luego de identificar los activos de información, sus amenazas y vulnerabilidades, se debe identificar el impacto que tendría el activo, en el proceso respectivo, si éste se viera afectado por esa amenaza o vulnerabilidad. El impacto, en este caso, es el grado en que se ve afectado un proceso determinado al ser alterado alguno de sus activos de información. A mayor correlación entre el resultado del proceso y la alteración del activo, el impacto de ese activo será mayor.

La norma ISO/IEC 27001 propone 3 requisitos propios de los activos de información, mediante los cuales se busca cuantificar el impacto que tiene dentro del proceso y con esto valorar el activo: confidencialidad, integridad y disponibilidad. A continuación, se presenta una matriz que define los niveles de confidencialidad, integridad y disponibilidad (Perfil CID), con la idea de proporcionar orientación en cuanto a cuándo y cómo se deben aplicar esos niveles:

**Tabla 4.** Matiz CID (Atsec, 2014. Traducida y modificada por el autor)

| Impacto de la pérdida → | Baja | Media | Alta |
|---|---|---|---|
| **Confidencialidad** Asegurar que la información es accesible sólo a aquellos autorizados para tener acceso. | La divulgación no autorizada de información podría esperarse que tenga un efecto adverso limitado en las operaciones de la organización, activos de la organización, o personal. | La divulgación no autorizada de información podría esperarse que tenga un efecto adverso grave en las operaciones de la organización, los activos de la organización, o individuos. | La divulgación no autorizada de información podría esperarse que tenga un efecto adverso grave o catastrófico en las operaciones de la organización, los activos de la organización, o individuos. |
| **Integridad** Salvaguardar la exactitud y la integridad de la información y el método de procesamiento. | La modificación o destrucción de información no autorizada podría esperarse que tenga un efecto negativo limitado sobre las operaciones de la organización, los activos de la organización, o individuos. | La modificación o destrucción de información no autorizada podría esperarse que tenga un efecto adverso grave en las operaciones de la organización, los activos de la organización, o individuos. | La modificación o destrucción de información no autorizada podría esperarse que tenga un efecto adverso grave o catastrófico en las operaciones de la organización, los activos de la organización, o individuos. |
| **Disponibilidad** Asegurar que los usuarios autorizados tengan acceso a la información y activos asociados cuando sea necesario. | La interrupción del acceso o uso de información o un sistema de información podría esperarse que tenga un efecto adverso limitado en las operaciones de la organización, los activos de la organización, o individuos. | La interrupción del acceso o uso de información o un sistema de información podría esperar que tenga un efecto adverso grave en las operaciones de la organización, los activos de la organización, o individuos. | La modificación o destrucción de información no autorizada podría esperar que tenga un efecto adverso grave o catastrófico en las operaciones de la organización, los activos de la organización, o individuos. |

Para hacer la evaluación del impacto, es importante considerar los controles que posee el hospital en el manejo de riesgos, ya que cambian el valor que se le da al impacto y las consecuencias sobre un activo. De este modo, se puede lograr un mejor resultado de la evaluación del impacto.

Actualmente la UEA no cuenta con controles que reduzcan los riesgos, son más bien sistemas de software y claves para el acceso al sistema. Además, las condiciones de las instalaciones físicas

de la Unidad, construcción, ubicación y alrededores generan cierta inseguridad que puede extenderse a los activos, ya que no hay resguardo de información.

Con los activos de la tabla 3, se realizó la identificación de su impacto a través del perfil CID en condiciones normales de operación y considerando los controles que posee la UEA, complementando la información para el inventario de activos.

**Tabla 5.** Inventario de activos y perfil CID urgencia adulto (Elaboración propia)

HOSPITAL CARLOS VAN BUREN
UN MEJOR HOSPITAL PARA TODOS

**Fecha emisión:** 18/05/2015

**Proceso:** Urgencia adulto

| Nº | Activo | Tipo de activo | Detalle | Propietario | Ubicación | Perfil CID | | |
|---|---|---|---|---|---|---|---|---|
| | | | | | | C | I | D |
| 1 | DAU | Información | Datos de la atención de urgencia | Jefe Recaudación | Recaudación | Alta | Alta | Alta |
| 2 | Sistema de orden | Sistemas | Sistema informático con el que se trabaja | Jefe Informática | Departamento Informática | Alta | Alta | Alta |
| 3 | Equipo clínico | Personas | Médicos, enfermeras, paramédicos | Jefe Recurso Humano | Lugar de atención, puesto de trabajo | Media | Alta | Media |
| 4 | Computadores | Equipos | Utilizados por equipo clínico | Jefe Informática | Oficinas | Media | Media | Media |
| 5 | Instalaciones físicas | Infraestructura | Lugar donde se desarrolla el proceso | Jefe de Calidad | Coordenadas de la infraestructura | Media | Media | Media |
| 6 | Ficha médica | Información | Historial clínico del paciente hospitalizado | Equipo Clínico | Recaudación | Alta | Alta | Alta |

C: Confidencialidad I: Integridad D: Disponibilidad

**Elaborado por:** José Gómez, Gastón Letelier, Karen Soto, Vanessa Bello
**Revisado por:** Karen Soto

*4.1.7. Análisis y evaluación del riesgo.*

Una vez identificados los activos y su impacto, el paso siguiente es valorar el impacto con el fin de estimar la importancia que tienen para la Unidad. Para estimar este valor, se debe considerar el riesgo que puede causar a la UEA la alteración de algún activo. La idea es realizar un listado de riesgos asociados a los activos identificados, de acuerdo a la probabilidad de que ocurra una amenaza y las consecuencias de su impacto, todo esto ligado a las vulnerabilidades existentes en la Unidad respecto a la seguridad de los mismos.

Para esta etapa de evaluación del riesgo, se recomienda utilizar el método de Análisis Modal de Fallas y Efectos (AMFE) (Bestratén, Orriols y Mata, 2004), ya que es una herramienta que busca el aseguramiento de la calidad en la identificación y prevención de los modos de falla, tanto de un producto como de un proceso; evaluando su gravedad, ocurrencia y detección a través del cálculo del número o índice de prioridad de riesgo (IPR) (Bestratén, Orriols y Mata, 2004).

El principal interés del AMFE es resaltar los puntos críticos con el fin de eliminarlos o establecer un sistema preventivo (mediante correctores) para evitar su aparición o minimizar sus consecuencias, con lo que se puede convertir en un riguroso procedimiento de detección de riesgos potenciales si se aplica de manera sistemática. El valor del IPR se obtiene de la siguiente ecuación:

$$IPR = G * F * D$$

En donde G: gravedad F: frecuencia y D: detectabilidad. A continuación la descripción de cada término y su respectiva clasificación de acuerdo al riesgo asociado:

**Gravedad** → Mide el daño normalmente esperado que provoca la falla en cuestión, según percepción del propietario del activo y/o del equipo del SGSI. También cabe considerar el daño máximo esperado, el cual iría asociado también a su probabilidad de generación.

| Gravedad | Criterio | Valor |
|---|---|---|
| Muy baja *Repercusiones imperceptibles* | No es razonable esperar que esta falla de pequeña importancia origine efecto real alguno sobre el rendimiento del sistema. Probablemente, el propietario o usuario del activo ni se daría cuenta de la falla. | 1 |
| Baja *Repercusiones irrelevantes apenas perceptibles* | El tipo de falla originaria un ligero inconveniente al propietario o usuario. Probablemente, éste observará un pequeño deterioro del rendimiento del sistema sin importancia. Es fácilmente subsanable. | 2-3 |
| Moderada *Defectos de relativa importancia* | La falla produce cierto disgusto e insatisfacción en el propietario o usuario. Estos últimos observarán deterioro en el rendimiento del sistema | 4-6 |
| Alta | La falla puede ser crítica y verse inutilizado el sistema. Produce un grado de insatisfacción elevado. | 7-8 |
| Muy alta | Modalidad de falla potencial muy crítica que afecta el funcionamiento de seguridad del producto o proceso y/o involucra seriamente el incumplimiento de normas reglamentarias. Si tales incumplimientos son graves corresponde un 10 | 9-10 |

**Tabla 6.** Clasificación gravedad del riesgo (Bestratén, Orriols y Mata, 2004)

**Frecuencia** → Mide la repetitividad potencial u ocurrencia de una determinada falla, es lo que en términos de fiabilidad o de prevención llamamos la probabilidad de aparición de falla.

| Frecuencia | Criterio | Valor |
|---|---|---|
| Muy baja Improbable | Ningún fallo se asocia a procesos casi idénticos, ni se ha dado nunca en el pasado, pero es concebible. | 1 |
| Baja | Fallos asilados en procesos similares o casi idénticos. Es razonablemente esperable en la vida del sistema, aunque es poco probable que suceda. | 2-3 |
| Moderada | Defecto aparecido ocasionalmente en procesos similares o previos al actual. Probablemente aparecerá algunas veces en la vida del componente/sistema. | 4-6 |
| Alta | El fallo se ha presentado con cierta frecuencia en el pasado en procesos similares o previos procesos que han fallado. | 7-8 |
| Muy alta | Fallo casi inevitable. Es seguro que el fallo se producirá frecuentemente. | 9-10 |

**Tabla 7.** Clasificación frecuencia del riesgo (Bestratén, Orriols y Mata, 2004)

**Detectabilidad**→ Trata de averiguar cuan probable es que no se detecte un fallo o "output" defectuoso durante un proceso, pasando a etapas posteriores y generando los consiguientes problemas afectando al usuario final (propietario del activo o la organización en sí). Esto implica

que entre más difícil o demoroso sea detectar el fallo existente, más importantes pueden ser las consecuencias del mismo.

**Tabla 8.** Clasificación detectabilidad del riesgo (Bestratén, Orriols y Mata, 2004)

| Detectabilidad | Criterio | Valor |
|---|---|---|
| Muy alta | El defecto es obvio. Resulta muy improbable que no sea detectado por los controles existentes. | 1 |
| Alta | El defecto, aunque es obvio y fácilmente detectable, podría en alguna ocasión escapar a un primer control, aunque sería detectado con toda seguridad a posteriori. | 2-3 |
| Mediana | El defecto es detectable y posiblemente no llegue al propietario o usuario del activo. Posiblemente se detecte en los últimos estadios de producción. | 4-6 |
| Pequeña | El defecto es de tal naturaleza que resulta difícil detectarlo con los procedimientos establecidos hasta el momento. | 7-8 |
| Improbable | El defecto no puede ser detectable. Casi seguro que lo percibirá el propietario o usuario final. | 9-10 |

Luego de determinar la gravedad, frecuencia y detectabilidad, se puede obtener el valor del IPR, el cual es un número adimensional que permite priorizar la urgencia en la intervención, así como el orden de las acciones correctoras, ya que debe ser calculado para todas las causas de falla.

Es importante que la UEA evalúe y establezca, en el contexto del SGSI, los límites del IPR para decidir en la matriz AMFE cuales riesgos necesitan tratamiento. El IPR ofrece una primera aproximación de la importancia del riesgo, lo que ha de facilitar la toma de decisiones para determinar el control o tratamiento del riesgo.

La definición de los tres conceptos claves presentes en el ítem de fallas potenciales de la matriz AMFE son los siguientes:

- Falla o modo de falla: hace referencia al riesgo potencial identificado en el proceso o en una actividad específica del mismo.
- Efectos de la falla: es el síntoma detectado por el paciente/usuario del modo de falla, es decir, si ocurre la falla potencial cómo lo percibe el cliente, pero también cómo repercute en el sistema. Se trata de describir las consecuencias no deseadas de la falla que se puede observar o detectar.
- Causas modo de falla: describe la amenaza, lo que puede causar daño o pérdida del activo por medio de la explotación.

La evaluación del riesgo se desarrolla a partir de los límites y criterios definidos en el contexto del SGSI. En esta etapa se define la prioridad de los riesgos que deben ser tratados y gestionados, de acuerdo al resultado de la matriz AMFE y al análisis del IPR. No se establece un criterio de clasificación de tal índice, no obstante un IPR inferior a 100 no requeriría intervención, salvo que la mejora fuera fácil de introducir y contribuyera a mejorar aspectos de calidad del producto, proceso o trabajo.

La UEA, en conjunto con la Dirección del Hospital, debe definir los límites en las políticas del SGSI, ya que así se da prioridad a los activos que están en mayor riesgo.

Se sugiere intervenir en aquellos activos en los que su IPR sea superior a 100, dándole mayor énfasis a la hoja DAU (Datos de Atención de Urgencia) y la Ficha Clínica, ya que son activos de información críticos en el proceso de urgencia adulto (Soto, 2015).

ANÁLISIS MODAL DE FALLAS Y EFECTOS (A.M.F.E.)

| | | |
|---|---|---|
| Proceso: Urgencia adulto | Fecha de elaboración: | 18/05/2015 |
| Responsable del área: Enfermera Supervisora UEA | Versión: 1 | |
| Participantes de la organización: Enfermera Supervisora, Enfermeros de turno | Hoja: 1 de 1 | |

| Proceso | Actividad/Operación | Activo | Falla Nº | Fallas potenciales | | | Estimación | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | Modo de falla | Efectos | Causas modo de falla | F | G | D | IPR |
| Urgencia | Alta administrativa | DAU | 1.1 | Pérdida de confidencialidad | Información privada es de conocimiento público | Divulgación de la información | 6 | 10 | 8 | 480 |
| | | | 1.2 | Pérdida de información | Diagnóstico erróneo, incompleto | Letra poco legible y extravío de documento | 6 | 10 | 6 | 360 |
| Urgencia | Alta administrativa | Sistema Orden | 2.1 | Suplantación de identidad | Robo de información | Contraseñas poco seguras | 3 | 6 | 3 | 54 |
| | | | 2.2 | Acceso no autorizado | Filtración de información | Falta de restricción en el acceso | 3 | 6 | 3 | 54 |
| | | | 2.3 | Pérdida de información por fallos en el servidor | Retraso en la entrega de información, aumento de costos | Virus, código malicioso, hackers | 1 | 3 | 3 | 9 |
| Urgencia | Alta administrativa | Equipo clínico | 3.1 | Falta de capacitación | Desconocimiento de roles y responsabilidades | Ignorancia de seguridad de la información | 3 | 8 | 3 | 72 |
| Urgencia | Alta administrativa | Computadores | 4.1 | Pérdida de información | Información privada divulgada | Sabotaje, espionaje, acceso no autorizado | 3 | 3 | 6 | 54 |
| Urgencia | Alta administrativa | Instalaciones fisicas | 5.1 | Incumplimiento en el servicio | Aumento de costos, pérdida de información, disconformidad | Catástrofes naturales | 4 | 4 | 6 | 96 |
| Urgencia | Derivación a hospitalizados | Ficha médica | 6.1 | Pérdida de confidencialidad | Información privada es de conocimiento público | Divulgación de la información | 8 | 10 | 8 | 640 |
| | | | 6.2 | Pérdida de información | Diagnóstico erróneo, incompleto | Letra poco legible y extravío de documento | 6 | 10 | 8 | 480 |

**Tabla 9.** AMFE proceso de urgencia adulto (elaboración propia)

Una vez que se han identificado y analizado los riesgos de la Unidad, se debe determinar el tratamiento que tienen que recibir y las acciones necesarias. Un resultado del análisis de riesgos habrá sido el criterio para determinar cuáles van a ser los niveles de riesgo aceptables y en consecuencia, cuáles van a ser los niveles inaceptables y que por lo tanto son susceptibles de ser gestionados. Existen cuatro tipos de tratamientos para el riesgo (Poveda, 2007):

- **Mitigar el riesgo:** Reducirlo mediante la implantación de controles que reduzcan el riesgo a un nivel aceptable, implica seleccionar dichos controles, definir y documentar los métodos para ponerlos en marcha y gestionarlos.
- **Asumir el riesgo:** La Dirección asume el riesgo ya que está por debajo de un valor de riesgo aceptable, simplemente requiere que quede documentado que la Dirección conoce y acepta estos riesgos. Los riesgos que se han asumido han de ser controlados y revisados periódicamente para evitar que evolucionen y se conviertan en riesgos mayores.
- **Transferir el riesgo a un tercero:** Como por ejemplo, asegurando el activo que tiene el riesgo o subcontratando el servicio. Deben evaluarse las opciones y tomar las acciones pertinentes para ejecutar la opción escogida, en función del valor del activo y del costo de realizar esta transferencia (no sólo costo económico sino también los riesgos que conlleva esta transferencia en cuanto a la inclusión de un tercero).

- **Eliminar el riesgo:** Aunque no suele ser la opción más viable, ya que puede resultar difícil o demasiado costoso, si se cree posible o necesario, habrá que establecer los pasos para conseguirlo: eliminar el activo, eliminar el proceso o incluso el área de negocio que es la fuente del riesgo.


**Figura 19.**Tratamientos del riesgo en el SGSI (Poveda, 2007)

*4.1.8. Selección de controles y SOA.*

En esta parte, se deben preseleccionar o en definitiva seleccionar los objetivos de control y los controles del Anexo A de la norma ISO/IEC 27001, como ayuda y guía, para el tratamiento del riesgo que cumplan con los requerimientos identificados en el proceso de evaluación del riesgo.

La Dirección del hospital debe aprobar tanto los riesgos residuales como la implementación y uso de los controles en el SGSI. Es importante saber que los riesgos de seguridad de la información son riesgos de "negocio" y sólo la Dirección puede tomar decisiones sobre su aceptación final en cada revisión y/o acciones de tratamiento. El riesgo residual es el que queda, aún después de haber aplicado controles.

Se debe definir una declaración de aplicabilidad, también llamado SOA (Statement of Applicability), la que debe incluir lo siguiente:

- Los objetivos de control y controles seleccionados y los motivos para su elección.
- Los objetivos de control y controles que actualmente ya están implantados.
- Los objetivos de control y controles del Anexo A excluidos y los motivos para su exclusión; este es un mecanismo que permite, además, detectar posibles omisiones involuntarias.

Con respecto a los controles de seguridad, el estándar ISO 27002 (antigua ISO 17799) proporciona una guía completa de implantación que contiene 133 controles, según 39 objetivos de control agrupados en 11 dominios. Este estándar es referenciado en la ISO/IEC 27001, en su segunda cláusula, en términos de "Documento indispensable para la aplicación de este documento" y deja abierta la posibilidad de incluir controles adicionales. Además, la ISO/IEC 27001 en su Anexo A contiene los controles y objetivos de control de la norma ISO 27002 de forma resumida.

*4.2. Hacer.*

Siguiendo la metodología del PDCA indicada por la ISO/IEC 27001, en la segunda fase llamada "hacer" corresponde formular el plan de tratamiento de riesgos que identifique las acciones, recursos, responsabilidades y prioridades en la gestión de los riesgos de seguridad de la información de la Unidad.

La idea en esta etapa es implementar el plan, con el fin de alcanzar los objetivos de control identificados en la fase planear. Implantar los controles seleccionados previamente y que se encaminen a los objetivos de control.

También se debe definir un sistema de métricas o indicadores que permita obtener resultados reproducibles y comparables para medir la eficacia de los controles o grupos de controles implantados.

El paso siguiente y final en esta fase es inculcar a todo el personal de la UEA la toma de conciencia y formarlos en lo relativo a la seguridad de la información. Este paso es muy importante para que se lleve a cabo el SGSI y así genere los beneficios que se esperan en la implementación.

Se recomienda desarrollar un marco normativo, normas, manuales, procedimientos e instrucciones que permitan gestionar las operaciones del SGSI.

*4.2.1. Formular plan de tratamiento del riesgo.*

El plan de tratamiento del riesgo se encarga de implantar de manera planificada los controles para los riesgos que superan el nivel aceptable.

Una institución que conoce sus riesgos nunca podrá ignorarlos, ya que no estaría vigilando que estos no se convirtiesen en riesgos que la institución no sea capaz de asumir o que, por no haberlos tenido en cuenta, se materialicen y den lugar a un incidente de seguridad.

En la fase anterior (planear) se mostraron los 4 tipos de tratamientos para el riesgo. En esta fase (hacer) se debe decidir por uno de ellos y formularlo.

Una vez decididas las acciones a tomar, se debe volver a realizar un análisis de riesgos, teniendo en cuenta la nueva situación con los controles y medidas que se han decidido implantar y que van a reducir en mayor o menor medida el riesgo que existía, ya que ese es su objetivo. El nivel de riesgo resultante de este segundo análisis es el riesgo residual, aquel riesgo que subsiste, después de haber implementado controles. Nunca se podrá eliminar totalmente el riesgo, siempre quedará cierto nivel, por lo que es importante que todos los riesgos residuales sean aceptados por la Dirección (Poveda, 2007).

*4.2.2. Mitigación del riesgo.*

Es pertinente considerar como plan de tratamiento del riesgo la mitigación del riesgo, al ser el tratamiento más factible para los potenciales riesgos, ya que tiene como fin de reducirlos a través de la aplicación de controles. Este tratamiento contiene las siguientes fases:

(1) Seleccionar los controles apropiados para los riesgos a los que se quiere hacer frente, en principio del Catálogo de Buenas Prácticas de la ISO 27002 (133 controles posibles), pero pueden añadirse otros que la Unidad considere necesario.
(2) Implantar los controles para lo que deben desarrollarse procedimientos. Aunque sean controles tecnológicos deben desarrollarse para su instalación, uso y mantenimiento.
(3) Verificar que los controles están correctamente implantados.
(4) Establecer indicadores para saber en qué medida la implantación de los controles seleccionados reduce el riesgo a un nivel aceptable.


**Figura 20.**Mitigación del riesgo (Poveda, 2007)

### a) Selección de controles

Los controles se seleccionarán e implementarán para minimizar en lo posible la posibilidad de que los riesgos detectados en el análisis de riesgos dañen los activos. Existen dos grandes grupos de controles. Por un lado los técnicos, tales como sistemas de cifrado, copias de seguridad, sistemas de detección de intrusos, actualizaciones de software, antivirus o cortafuegos, y por otro los organizativos que son medidas organizativas tales como la política de seguridad, procedimientos de uso de los sistemas de información para los usuarios, los planes de formación o los planes de continuidad del negocio (Poveda, 2007).

Se recomienda conseguir un conjunto de controles que contenga controles de los dos tipos, ya que muchas medidas técnicas no pueden impedir que los usuarios de los sistemas cometan errores o dañen intencionadamente los activos y, al contrario, emitir muchas normas internas puede ser inútil si no hay una mínima seguridad técnica implantada.

La combinación de las medidas técnicas y organizativas consigue un nivel de seguridad razonable con unos recursos limitados para el escenario de riesgo que se trataba de mitigar. Otra clasificación que se puede hacer de los controles para facilitar su selección es la de controles preventivos y correctivos. Los controles de tipo preventivo son aquellos que sirven para evitar incidentes de seguridad no deseados mientras que los correctivos son aquellos que se pondrán en marcha ante la ocurrencia de fallos o incidentes de seguridad (Poveda, 2007).

Existen factores y restricciones en el momento de la selección de controles. Hay controles que se encuentran interrelacionados, por lo tanto, hay que tener en cuenta esto para evitar lagunas de seguridad que se puedan presentar y que además puedan suponer nuevas vulnerabilidades. También hay que considerar que la implantación de un control requiere ciertos recursos al igual que su mantención, la disponibilidad, la ayuda que se debe brindar a los colaboradores para desempeñar el control y su aplicabilidad con respecto a los riesgos que se han detectado.

Se deben seleccionar los objetivos de control y controles del Anexo A de la ISO/IEC 27001 como parte de este proceso conforme sea apropiado para cubrir los requerimientos. Se pueden agregar controles y objetivos de control adicionales si lo consideran pertinente (ISO/IEC 27001, 2005).

### b) Implementación de controles.

Seleccionados los controles pertinentes, se deben definir los procedimientos para su implantación. Los controles de tipo organizativo se prestan más a ser implantados mediante procedimientos,

como por ejemplo la gestión de los recursos humanos. Pero incluso los de corte tecnológico pueden ser susceptibles de necesitar documentación, como por ejemplo la realización de copias de seguridad.

Debe analizarse la lista de controles seleccionados y establecer qué procedimientos necesitan ser desarrollados. Hay que contar también que si la organización no tiene procesos muy complejos puede ser posible que varios controles puedan agruparse en un único procedimiento. No es necesario ni recomendable, desarrollar un procedimiento para cada control. La cantidad de documentación generada puede hacer más complejo el gestionar correctamente los controles. Por otro lado, los procedimientos deben ser lo más breves y claros posible. No deben incluir demasiadas instrucciones ni particularidades de la tarea a realizar. El objetivo del procedimiento es contar con una herramienta que permita a cualquiera ejecutarla con un mínimo de rigor aun sin contar con formación o experiencia previa (Poveda, 2007).

### c) Verificación de controles.

Una vez que los controles seleccionados son puestos en marcha, deben ser revisados periódicamente para comprobar que funcionan como se esperaba. De no ser así, se deben tomar acciones necesarias para revertir la situación.

Una herramienta fundamental del SGSI es la verificación de la eficacia de los controles implantados. Para ello deben establecerse objetivos de rendimiento para los controles, marcar puntos de control y medición y registrar los resultados de manera que se sepa si el control realmente protege los activos hasta el punto que la UEA necesita.

### d) Documentación del plan de tratamiento del riesgo.

La documentación de la gestión de riesgos se realiza mediante la Declaración de Aplicabilidad (SOA). Este documento, requerido por la Norma ISO/IEC 27001, es un resumen de las decisiones que se han tomado para tratar los riesgos analizados.

Este documento registra todo lo que se ha realizado y se va a realizar en el futuro inmediato para que la seguridad de la información de la Unidad llegue al nivel que se haya estimado apropiado para sus necesidades y recursos.

El objetivo principal de este documento es que permite repasar todos y cada uno de los controles, se hace una comprobación de que no se ha pasado por alto ningún control por error o descuido que podría ser útil o necesario para la gestión de la seguridad de la información. Constituye de alguna manera un registro de los resultados finales del SGSI, ya que concreta de manera clara y directa en qué va a consistir el SGSI, detallando cada uno de los controles que se tiene la intención de aplicar de manera explícita.

No es obligatorio seleccionar todos los controles asociados a cada uno de los objetivos. Por el contrario, deben escogerse los objetivos de control y controles apropiados a las circunstancias, es decir, aquellos que se considera que cubren los requisitos de seguridad de la Unidad y sean viables.

Una vez que está claro que se va a hacer, debe prepararse un plan para la realización de todo lo que se ha decidido. Este plan, que la Norma ISO/IEC 27001 denomina Plan de Tratamiento de Riesgos, contempla todas las acciones necesarias tanto para implantar el SGSI y gestionarlo, como para la puesta en marcha de los controles escogidos. El plan tiene que contar con los recursos materiales, técnicos y humanos necesarios para que pueda ser llevado a cabo con ciertas garantías de éxito. Debe ser revisado a intervalos regulares para comprobar que no se producen desviaciones. Estas pueden ser de plazo porque no hay recursos para ejecutarlas o han resultado ser más difíciles de ejecutar de lo que se preveía en un principio o también de que no se llevan a cabo las acciones planificadas sino otras, normalmente porque se han tomado decisiones sobre la

marcha para solventar problemas no previstos. Dentro de este plan pueden quedar recogidos los objetivos definidos para medir la eficacia de los controles, estableciendo asimismo el mecanismo de recogida y análisis (Poveda, 2007).

*4.2.3. Implementación de controles en la UEA del HCVB.*



A continuación, se muestran las medidas de seguridad sugeridas de acuerdo a los controles y objetivos de control indicados en el Anexo A de la norma ISO/IEC 27001 considerados necesarios para la UEA según Karen Soto, Enfermera Supervisora UEA, de acuerdo al alcance que tiene la Unidad para tratar las falencias que esta posee en cuanto a seguridad de la información y lo que busca implementar para disminuirlas.

La idea central de implementar los controles es satisfacer los objetivos de control planeados.

Se partirá por la "Política de seguridad", que si bien su creación no está al alcance de la UEA, es importante describirla para conocer su función.

## A.5 Política de seguridad.

Definición de la política de seguridad del Hospital

Establecer una adecuada política de seguridad tiene dos propósitos: informar y concientizar a todos los participantes sobre la estrategia de seguridad del hospital y definir las líneas generales de actuación para evitar amenazas y reaccionar ante incidentes de seguridad. La política debe establecer directrices claras, normas para el tratamiento de la información y definir los responsables de su desarrollo, implantación y gestión. Debe estar alineada con los objetivos organizacionales del hospital, por lo que la Dirección debe establecer un marco de referencia para que posteriormente se puedan fijar objetivos de control específicos para cada proceso de la institución. La Dirección deberá establecer de forma clara las líneas de las políticas de actuación y manifestar su apoyo y compromiso a la seguridad de la información, publicando y manteniendo políticas de seguridad en todo el hospital.

- La política de seguridad debe documentarse, luego este documento se debe publicar y comunicar a todo el personal involucrado.
- Debe ser revisada de forma regular para asegurar la idoneidad, eficiencia y efectividad.

Una estructura de política de seguridad podría ser (ISO/IEC 27002, 2015):

- ✓ Resumen: Política Resumen - Visión general de una extensión breve; una o dos frases y que pueden aparecer fusionadas con la introducción.
- ✓ Introducción: Breve explicación del asunto principal de la política.
- ✓ Ámbito de aplicación: Descripción de los departamentos, servicios, áreas o actividades del hospital a las que afecta/aplica la política. Cuando es relevante en este apartado se mencionan otras políticas relevantes a las que se pretende dar cobertura desde ésta.
- ✓ Objetivos: Descripción de la intención de la política.
- ✓ Principios: Descripción de las reglas que conciernen a acciones o decisiones para alcanzar los objetivos. En algunos casos puede ser de utilidad identificar previamente los procesos clave asociados con el asunto principal de la política para pasar posteriormente a identificar las reglas de operación de los procesos.

- ✓ Responsabilidades: Descripción de quién es responsable de qué acciones para cumplir con los requisitos de la política. En algunos casos, esto puede incluir una descripción de los mecanismos organizativos, así como las responsabilidades de las personas con roles designados.
- ✓ Resultados claves: Descripción de los resultados relevantes para las actividades del hospital que se obtienen cuando se cumplen los objetivos.
- ✓ Políticas relacionadas: Descripción de otras políticas relevantes para el cumplimiento de los objetivos, usualmente se indican detalles adicionales en relación a temas específicos.
- ✓ La política de alto nivel (más genérica) habitualmente relacionada con el SGSI suele estar apoyada por políticas de bajo nivel, específicas a aspectos concretos en temáticas como el control de acceso, la clasificación de la información, la seguridad física y ambiental, uso aceptable de activos, escritorio y pantallas libres de información sensible, dispositivos móviles y teletrabajo, backups, protección contra el malware, entre otros.

### A.7 Gestión de activos.

El objetivo de este dominio es lograr que la UEA tenga conocimiento preciso sobre los activos que posee como parte importante de la administración de riesgos.

Clasificación de la información

Dentro del hospital, específicamente en la UEA, existe una gran cantidad de información, pero no toda posee la misma importancia. La documentación administrativa de la Unidad no es igual de relevante que una ficha clínica de un paciente. Es por esto que se debe clasificar los activos de información de acuerdo a la sensibilidad y criticidad o bien según la funcionalidad que cumplen, para así establecer diferencias entre las medidas de seguridad a aplicar, las que atenderán los criterios de confidencialidad, integridad y disponibilidad.

- Se debe establecer un esquema de clasificación de la información, rigurosa y clara, sin mayor complejidad y en pocos niveles. Por ejemplo una clasificación de la información podría ser: Pública, Restringida y Confidencial.
- Para cada tipo de información se debe definir el personal autorizado, los soportes en los que se almacenarán, los usuarios, ubicación, etc.

### A.8 Seguridad de los recursos humanos.

Definición de funciones y responsabilidad del personal de la UEA

Una de las tantas amenazas dentro de cualquier institución es el acceso de usuarios no autorizados a información relevante pudiendo consultar, modificar, borrar, robar, etc. información crítica.

- Se deben definir funciones y responsabilidades de seguridad al personal del sistema de información. Cada activo de información posee un propietario, el cual debe velar por la seguridad de este. Cada proceso de seguridad debe identificar a un propietario y a los usuarios que participarán en el.
- Las funciones de seguridad y responsabilidades del personal de la Unidad y de terceros deben estar definidas y documentadas conforme a la política de seguridad de la información de la Institución.

Cláusulas de confidencialidad

El personal de la Unidad debe saber de su obligación de mantener secreto profesional sobre cualquier información que conozca en el desarrollo de sus funciones, aún después de acabar con la relación laboral que tenía con el hospital.

- Todos los funcionarios deben firmar un acuerdo de confidencialidad, en el que se detalle sus funciones y obligaciones respecto a la información de la Unidad. Se deben definir exigencias de confidencialidad y no divulgación de información para todo el personal que tiene acceso al sistema de información o información en sí para el desarrollo de sus funciones.
- Los acuerdos y exigencias de confidencialidad deben ser identificados, documentados y revisados de forma regular.

Concientización sobre la seguridad de la información

Una forma para lograr que el personal ayude a cooperar con la gestión de la seguridad de la información es informando y concientizando acerca de la importancia e impacto que tiene para la Unidad el cumplir con las medidas establecidas para la seguridad de la información. Se debe instruir al personal de forma apropiada, logrando entregar la educación necesaria en cuanto al tratamiento de los datos en la Unidad.

- Informar al personal de la Unidad que tenga acceso a datos del sistema de información sobre las normas de utilización y medidas de seguridad que contempla esa acción.
- Aplicar disciplina al personal en el caso de que no cumplan con los requisitos de seguridad, a pesar de haber sido informados.
- La Unidad deberá identificar y revisar las necesidades de confidencialidad y recogerlas en acuerdos de no divulgación.

### A.9 Seguridad física y ambiental

Seguridad física relacionada con el entorno

Establecer un perímetro físico, controles físicos de entrada a los Servicios Clínicos y Administrativos son las primeras medidas de seguridad. Protegiendo el acceso a cualquier Servicio se protege el acceso físico al sistema de información. El establecer perímetros de seguridad y áreas protegidas facilita la implementación de controles de protección de las instalaciones de procesamiento de información crítica o sensible de la Unidad, contra accesos físicos no autorizados.

- Se podría implementar el uso de tarjetas de identificación de colores para indicar áreas accesibles por los visitantes.
- Se debe retener a quien no esté en el área que le corresponde (ISO/IEC 27002, 2015).Debe asegurarse la retirada de todos los pases de funcionarios y de visita cuando se vayan (ISO/IEC 27002, 2015).

### A.11 Control de acceso.

El objetivo de este dominio es controlar el acceso por medio de un sistema de restricciones y excepciones a la información como base de todo sistema de seguridad informática.

Gestión de acceso de usuario

Se recomienda establecer procedimientos formales para controlar la asignación de los permisos de acceso a los sistemas de información. Estos procedimientos debieran cubrir todas las etapas del acceso de los usuarios, desde el registro inicial hasta su baja cuando ya no sea necesario su acceso a los sistemas de información.

- Elaborar un procedimiento formal de alta y baja de usuarios con el objeto de habilitar la asignación de derechos de acceso.
- Implantar un proceso formal de aprovisionamiento de accesos a los usuarios para asignar o revocar derechos de acceso a todos los usuarios y para todos los sistemas.
- La asignación de información confidencial para la autenticación debería ser controlada mediante un proceso de gestión controlado (ISO/IEC 27002, 2005).

*4.2.4. Formación, toma de conciencia y competencia.*

La norma ISO/IEC 27001 establece como último paso en la fase "Hacer", que la UEA debe asegurar que todo el personal que posea responsabilidades y roles con el SGSI y su implementación, debe ser competente para cumplir con sus tareas designadas. Para garantizar esto, la UEA debe determinar las competencias necesarias de los participantes, realizar actividades de formación o solicitar la contratación de personal de ser necesario, evaluar la eficacia de las acciones que se están realizando y mantener un registro de esto. La Unidad debe asegurarse que todo el personal involucrado en la implementación del SGSI tome conciencia de la pertinencia e importancia de sus actividades de seguridad de la información y la influencia que tienen en el cumplimiento de los objetivos de esta.

*4.2.5. Objetivos de control e indicadores.*

La norma ISO/IEC 27001 indica que se deben incluir todas las acciones que se realizarán en la gestión del plan de tratamiento del riesgo. Todas estas acciones formarán parte importante de la mejora continua del SGSI y se deben medir estableciendo objetivos e identificando las oportunidades de mejora. Luego de que se establezcan los objetivos, se deben establecer los indicadores de rendimiento para medir su cumplimiento. Para lograr medir, se debe reunir toda la información recogida a partir de los registros del sistema, los cuales son reflejados en cada uno de los documentos, para lo cual la información debe ser pertinente, precisa y oportuna (ISO/IEC27001, 2005).

Los indicadores de rendimiento o desempeño son una herramienta que entrega información cuantitativa respecto al logro o resultado de los productos (bienes o servicios) generados por la Unidad, pudiendo cubrir aspectos cuantitativos o cualitativos de este logro. Es una expresión que establece una relación entre dos o más variables, la que comparada con periodos anteriores, productos similares o una meta o compromiso, permite evaluar desempeño (DIPRES, 2015). Para construir un indicador, se deben identificar las variables que lo conforman y su relación, para así generar la información necesaria. Estas variables deben definirse con rigurosidad, asignándole un sentido claro, para evitar que se produzcan ambigüedades y discusiones sobre los resultados. También es necesario que se tenga claridad de quién y cómo produce dicha información, con la finalidad de tener un criterio de confidencialidad.

A continuación una tabla en la que se indican criterios para la selección de indicadores, de forma de orientar el establecimiento de indicadores en la Unidad:

Tabla 10. Criterio para selección de indicadores (Dane, 2015)

| Criterio de selección | Pregunta a tener en cuenta | Objetivo |
|---|---|---|
| Pertinencia | ¿El indicador expresa qué se quiere medir de forma clara y precisa? | Busca que el indicador permita describir la situación o fenómeno determinado, objeto de la acción. |
| Funcionalidad | ¿El indicador es monitoreable? | Verifica que el indicador sea medible, operable y sensible a los cambios registrados en la situación actual. |
| Disponibilidad | ¿La información del indicador está disponible? | Los indicadores deben ser construidos a partir de variables sobre las cuales exista información estadística de tal manera que puedan ser consultados cuando sea necesario. |
| Confiabilidad | ¿De dónde provienen los datos? | Los datos deben ser medidos siempre bajo ciertos estándares y la información requerida debe poseer atributos de calidad estadística. |
| Utilidad | ¿El indicador es relevante con lo que se quiere medir? | Que los resultados y análisis permitan tomar decisiones. |

Además de generar indicadores para los objetivos, se pueden establecer métricas en cuanto a cualquier parámetro considerado relevante. Los valores de los parámetros que componen los objetivos (indicadores y métricas) tienen que recogerse de forma objetiva y regular para poder evaluar apropiadamente el proceso. Estos valores se van comparando en el tiempo con los objetivos marcados, analizando las diferencias con los mismos y tomando medidas oportunas cuando no son alcanzados. Todo esto se realiza con el fin de mejorar el proceso de toma de decisiones, además, los indicadores permiten cuantificar los cambios, monitorear el cumplimiento de los requisitos del SGSI, efectuar seguimiento a los planes que permiten tomar acciones correctivas oportunas y mejorar la eficiencia y eficacia del proceso en general (Dane, 2015).

### *4.3. Verificar.*

Fase en la cual se realiza el proceso de verificación y revisión por parte de la Dirección de la UEA del cumplimiento de los objetivos propuestos, el alcance proyectado y las medidas de seguridad implementadas (controles) para mitigar los riesgos. El proceso de seguimiento y monitorización del SGSI se hace con base a los resultados que arroja los indicadores de seguridad propuestos para la verificación de la eficacia y efectividad de los controles implementados.

En esta etapa se debe revisar regularmente la efectividad del SGSI; medir la efectividad de los controles para verificar que se cumple con los requisitos de seguridad; revisar regularmente en intervalos planificados las evaluaciones de riesgo, los riesgos residuales y sus niveles aceptables; realizar periódicamente auditorías internas; actualizar los planes de seguridad; y también registrar acciones y eventos que puedan haber impactado sobre la efectividad o rendimiento del SGSI (ISO/IEC 27001, 2005).

#### *4.3.1.* R*evisar el SGSI*

La norma ISO/IEC 27001 indica que se debe revisar el SGSI de forma regular, por lo menos una vez al año, para así asegurar la continua idoneidad, conveniencia y efectividad de este, es decir, observar si el sistema está llevándose a cabo adecuadamente, de forma apropiada y efectiva para

los propósitos de la UEA. Es una herramienta para el análisis y adopción de oportunidades de mejora al contemplar todos los aspectos del SGSI, teniendo una vista general que permite detectar puntos débiles y determinar una acción sobre cómo mejorarlos.

En definitiva, la UEA deberá ejecutar procedimientos de monitorización y revisión para (ISO/IEC 27000, 2015):

- Detectar a tiempo errores en los resultados generados por el procesamiento de la información.
- Identificar brechas e incidentes de seguridad.
- Ayudar a la Dirección a determinar si las actividades desarrolladas por las personas y dispositivos tecnológicos para garantizar la seguridad de la información se desarrollan en relación a lo previsto.
- Detectar y prevenir eventos incidentes de seguridad mediante el uso de indicadores.
- Determinar si las acciones realizadas para resolver brechas de seguridad fueron efectivas.

Los resultados de las revisiones deben documentarse claramente y se deben mantener registros de modo de proporcionar evidencia de conformidad con los requerimientos y la operación efectiva del SGSI. Existen muchas fuentes a través de las cuales la Dirección puede revisar el SGSI, obteniendo datos útiles e información. La norma ISO/IEC 27001 hace un listado de estas fuentes o insumos de la revisión:

(1) Resultados de auditorías y revisiones anteriores del SGSI.
(2) Retroalimentación de las partes interesadas.
(3) Técnicas, productos o procedimientos que se podrían utilizar en la UEA para mejorar el desempeño y efectividad del SGSI.
(4) El estado de las acciones preventivas y correctivas.
(5) Las vulnerabilidades o amenazas que no hayan sido tratadas adecuadamente en la evaluación del riesgo previas.
(6) Resultados de mediciones de efectividad, es decir, la evaluación de los objetivos.
(7) Cualquier cambio en la institución que pudiera afectar el SGSI.
(8) Recomendaciones para el mejoramiento.

Y el resultado de la revisión o salida del proceso, debe incluir cualquier decisión y acción relacionada con lo siguiente (ISO/IEC 27001, 2005):

(1) Mejoras de la efectividad del SGSI.
(2) Actualización de la evaluación del riesgo y del plan de tratamiento del riesgo.
(3) Modificación de procedimientos y controles que afecten la seguridad de la información, según fuese necesario, para responder a eventos internos o externos que pudieran tener impacto en el SGSI.
(4) Necesidades de recursos.
(5) Mejoramiento de cómo se mide la efectividad de los controles.

*4.3.2. Medición de la eficacia de los controles.*

Se debe medir la efectividad de los controles seleccionados e implantados ya que es fundamental verificar que se están cumpliendo los objetivos de control planeados. Además, se debe realizar un seguimiento a todo el SGSI, ya que es tan necesario como medir la eficacia de sus controles.

Existen varias herramientas que permiten y facilitan el seguimiento del SGSI, tales como: cartas de control, balanced scorecard, cuadro de mando integral y planes de verificación del SGSI, entre otros. Se recomienda que la UEA considere algunas de estas herramientas como apoyo y guía en el seguimiento del SGSI.

*4.3.3. Revisar riesgos residuales.*

La norma ISO/IEC 27001 hace mención sobre la revisión de la evaluación de riesgo, los riesgos residuales y sus niveles de aceptación en intervalos planificados. Para esto, se debe considerar los cambios que se hayan producido en la UEA en cuanto a la tecnología, objetivos, procesos, amenazas identificadas, efectividad de los controles implementados; así también los cambios externos que puedan afectarla (requerimientos legales, obligaciones contractuales, etc.).

*4.3.4. Auditorías Internas.*

Las auditorías internas son otro de los procedimientos que se deben llevar a cabo para la revisión del SGSI implantado, de forma planificada con la finalidad de verificar que los objetivos de control, controles, procesos y procedimientos del SGSI cumplen con los requerimientos de la norma ISO/IEC 27001; cumplen con los requerimientos de seguridad de la información identificados; se implementan y mantienen de manera efectiva; y se realizan conforme a lo esperado.

Las auditorías se deben planificar a través de un programa de auditoría anual, que considere el estado e importancia del proceso o área a ser auditado. En el caso de existir auditorias previas, también se debe considerar sus resultados. La UEA debe definir el criterio, alcance, frecuencia y métodos de auditoría que aplicarán. Las personas que asuman el rol de auditor deben estar capacitadas y poseer la preparación necesaria para llevar a cabo las auditorías. Es importante saber que los auditores no deben auditar su propio trabajo, ya que se debe asegurar la objetividad e imparcialidad de este proceso (ISO/IEC 27001, 2005).

A través de un procedimiento documentado, se deben definir todas las responsabilidades y requerimientos necesarios para la planificación y realización de estas auditorías, junto con ello el reporte de resultados y mantenimiento de registros.

La Dirección del proceso o área auditada, que en este caso sería la UEA o el proceso de urgencia en sí, es la que debe asegurar que se cumplan en el tiempo definido las acciones para eliminar las no conformidades y sus causas detectadas.

*4.3.5. Registrar acciones y eventos.*

Este punto hace referencia a registrar las acciones y eventos que puedan haber causado un impacto en la efectividad o el rendimiento del SGSI. Estos registros se pueden realizar en las mismas auditorías internas que tenga la UEA. Lo importante es documentar todo lo registrado, para que los controles sean protegidos y controlados.

La idea central de este punto es tener un control de registros que proporcionen evidencia de conformidad con los requerimientos y la operación efectiva del SGSI en la Unidad. Como ejemplo de registros se pueden nombrar los registros de libros de visitas, registros de auditoría y las solicitudes autorización de acceso, entre otras.

*4.4. Actuar.*

Es la última fase a considerar en la implementación del SGSI. Consiste en mantener y mejorar el SGSI a través del uso de la política de seguridad de la información, objetivos de seguridad de la información; con la implantación de mejoras, acciones correctivas y preventivas en relación a los resultados obtenidos en la revisión por la Dirección y las auditorías internas realizadas.

Para esta etapa debe estar claro que la misión del SGSI es situar la seguridad de la información al mismo nivel que cualquier otro objetivo de "negocio", y como tal, debe ser optimizado continuamente.

*4.4.1. Implementar mejoras.*

La UEA debe implementar las mejoras identificadas en el SGSI. Esto para lograr mejores niveles de eficacia en la implementación del SGSI, ya que al ser un ciclo con una dinámica de mejora continua, siempre se debe buscar la mejora del sistema.

*4.4.2. Acciones correctivas, preventivas y de mejora.*

Cuando existe incumplimiento de algún requisito del SGSI, se produce una no-conformidad. En este caso la UEA debe tomar las acciones necesarias para resolver esta situación no deseada. La norma ISO/IEC 27001 contempla 3 tipos de acciones:

(1) **Acciones correctivas:** La Unidad debe realizar acciones para eliminar la causa de las disconformidades con los requerimientos del SGSI para poder evitar la recurrencia. En otras palabras, las acciones correctivas tienen como objeto la eliminación de la causa origen del problema para evitar que se pueda repetir en el futuro. Solucionar de forma momentánea el incidente no es una acción correctiva completa.

(2) **Acciones preventivas:** La Unidad debe determinar la acción para eliminar la causa de las no-conformidades potenciales de los requerimientos del SGSI para evitar su ocurrencia, es decir, son las acciones que se toman para eliminar la causa de una posible no-conformidad. Se actúa antes de que ocurra. La Unidad debe identificar los riesgos cambiados e identificar los requerimientos de acción preventiva enfocando la atención sobre los riesgos cambiados significativamente.

(3) **Acciones de mejora:** Son aquellas que no están relacionadas con una no-conformidad. Estas acciones se deciden por la sugerencia del personal, la revisión del SGSI, entre otras. Las acciones de mejora suponen un cambio positivo en la forma de enfrentar una tarea. El SGSI al estar basado en un ciclo de mejora continua, se debe seguir implantando en cada ciclo medidas que lo mejoren.

Habitualmente las acciones correctivas y preventivas se discuten y analizan dentro de un comité de seguridad de la Unidad. Es relevante comunicar estas acciones o mejoras a todas las partes interesadas con el nivel de detalle adecuado y acordar, si es pertinente, la forma de proceder.

*4.4.3. Eficacia de las acciones.*

La UEA debe asegurar que las mejoras introducidas e implementadas alcanzan los objetivos previstos: la eficacia de cualquier acción, medida o cambio debe comprobarse siempre (ISO/IEC 27000, 2015), ya que así se puede tener un control de los cambios implementados, observando si se obtienen mejoras, se mantiene o empeora la implementación del SGSI.

## 5. Discusión

El diseño de una metodología es compleja en el sentido de que debe ser lo más clara posible para quienes la utilizarán pero a su vez cuidando el caer en la redundancia.

Según lo presentado en el numeral 4 de este trabajo, resultados obtenidos, se identifica que los objetivos planteados en este trabajo de título se lograron cumplir. Mediante la metodología de trabajo desarrollada, se siguió un conducto lógico introduciendo primeramente el concepto de seguridad de la información y su importancia dentro de cualquier organización; el concepto SGSI, sus beneficios y lo que indica la norma ISO/IEC 27001 respecto a ambos temas. Analizar el modelo por procesos PDCA para la implementación de un SGSI, identificando también los beneficios y potenciales beneficiarios según las necesidades reales que tiene la UEA.

La política de seguridad es una base, debe contar con la aprobación de la Dirección y además debe ser conocida por todos los involucrados del SGSI. El formato y contenido de esta política queda a disposición de la Dirección, quien determinará lo que abarcará y será la responsable de que sea clara y se alinee con los objetivos estratégicos de la organización.

En la identificación de activos, si bien se mostró un inventario con ciertos campos a llenar, el usuario de la metodología puede determinar agregar o quitar algunos de ellos, según le acomode, ya que la idea principal de ese inventario es entregar una herramienta que facilite el desarrollo de la implantación.

Como lo indica la ISO/IEC 27001, la organización, en este caso la UEA, es libre de elegir una metodología para la evaluación del riesgo, sin embargo, si se desea tener una clasificación más detallada que la que se indica en esta metodología (información como tal, equipos y sistemas que la soportan y las personas que la utilizan), se podría utilizar el método Magerit. Magerit es una metodología de análisis y gestión de riesgos de los sistemas de información elaborada por el Consejo Superior de Administración Electrónica para minimizar los riesgos de la implantación y uso de las tecnologías de la información, enfocada a las administraciones públicas. Actualmente está en su versión 3. Siguiendo la estructura de la metodología Magerit para la clasificación de activos de información en un sistema de información hay dos cosas importantes: la información que maneja y los servicios que presta. Estos activos esenciales marcan los requisitos de seguridad para todos los demás componentes del sistema. De acuerdo a dicha esencia, se pueden identificar otros activos relevantes:

- Datos que materializan la información.
- Servicios auxiliares que se necesitan para poder organizar el sistema.
- Aplicaciones informáticas (software) que permiten manejar los datos.
- Equipos informáticos (hardware) y que permiten hospedar datos, aplicaciones y servicios.
- Soportes de información que son dispositivos de almacenamiento de datos.
- Equipamiento auxiliar que complementa el material informático.
- Redes de comunicaciones que permiten intercambiar datos.
- Instalaciones que acogen equipos informáticos y de comunicaciones.
- Personas que explotan u operan todos los elementos anteriormente citados.

Respecto a uso del método de Análisis Modal de Fallas y Efectos (AMFE), este ayuda en el aseguramiento de la calidad en la identificación y prevención de los modos de falla; evaluando su gravedad, ocurrencia y detección a través del cálculo del índice de prioridad de riesgo. Así, se logra obtener un análisis no sólo cualitativo, si no cuantitativo. Es una herramienta útil para la evaluación

de los riesgos que poseen los activos. Quizás el usuario de esta metodología considere pertinente utilizar otra herramienta más compleja o que entregue datos duros que permitan una mejor intervención en análisis de riesgos, lo que a su vez ayudaría en el desarrollo de indicadores.

Un asunto a discutir es la situación actual que presentan los hospitales en cuanto a la seguridad de la información. Laque evidencia la necesidad de aplicar herramientas que ayuden a manejar los riesgos a los que se encuentran expuestos por no contar con mecanismos de defensa y mucho menos con una política de seguridad que direccione los pasos a seguir para el resguardo de la información. Si bien un SGSI ayuda en gran manera a mejorar los niveles de seguridad de la información en las organizaciones, este no provocará cambios significativos si antes o durante su implantación los involucrados no son concientizados e informados de la importancia que tiene su rol como usuario de la información.

## 6. Conclusiones

### *6.1. Conclusiones*

Todas las organizaciones, sin distinción alguna, están expuestas a un número cada vez mayor de amenazas que, aprovechando la más mínima vulnerabilidad, someten a los activos de información críticos en una serie de riesgos que pueden conllevar a diversas formas de fraude, espionaje, sabotaje o vandalismo. Los virus informáticos, el "hacking" o los ataques de denegación de servicio son algunos ejemplos comunes y conocidos, pero también se deben considerar los riesgos producidos de forma involuntaria, dentro de la propia organización o fuera de ella, o aquellos provocados accidentalmente por catástrofes naturales y fallas técnicas. Ambos provocan incidentes de seguridad que pueden poner en peligro la continuidad del negocio.

El cumplimiento de la legalidad, la adaptación dinámica y puntual a las condiciones variables del entorno, la protección adecuada de los objetivos de negocio para asegurar el máximo beneficio o el aprovechamiento de nuevas oportunidades de negocio, son algunos de los aspectos fundamentales en los que un SGSI logra ser una herramienta de gran utilidad y de importante ayuda para la gestión de las organizaciones.

El nivel de seguridad alcanzado por medios técnicos es limitado e insuficiente por sí mismo. En la gestión efectiva de la seguridad, es la organización en su completitud quien tiene que tomar parte activa, con el apoyo constante de la Dirección y tomando en consideración a clientes y proveedores de bienes y servicios.

El modelo de gestión de la seguridad debe contemplar procedimientos adecuados y la planificación e implantación de controles de seguridad basados en una evaluación de riesgos y en una medición de la eficacia de los mismos. El SGSI ayuda a establecer estas políticas y procedimientos en relación a los objetivos de negocio de la organización, con objeto de mantener un nivel de exposición siempre menor al nivel de riesgo que la propia organización ha decidido asumir. Aun así, es imposible garantizar un nivel de protección total, incluso considerando el caso de disponer de un presupuesto ilimitado. Es por ello, que el propósito de un SGSI es garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización de una forma sistemática, documentada, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías.

La UEA del hospital en cuestión, al no contar con controles de seguridad ni mucho menos tener una cultura de seguridad de la información, ha provocado que se subestime el impacto que causa cuando un activo de información es afectado en su confidencialidad, integridad y disponibilidad. El concientizar a todo el personal que maneje algún tipo de información es una tarea larga y tediosa, pero necesaria ya que se deben inculcar roles y responsabilidades.

Implementar un SGSI en la Unidad será de gran ayuda, pero es importante, y la norma ISO/IEC 27001lo recalca constantemente, que la Dirección esté comprometida con este proyecto, porque o si no todo avance que pueda haber no estará en base a cimientos firmes y los resultados no serán los esperados.

Se espera que este diseño de metodología basado en la ISO/IEC 27001 ayude en la futura implementación de este SGSI en la UEA, mejor aún si su alcance es redefinido a algún subproceso de esta, ya que así será más limitado.

### *6.2. Resumen de las contribuciones*

Este trabajo aportó información que permite conocer en mayor profundidad la importancia y beneficios, en cuanto a calidad y seguridad, que tiene la implementación de un SGSI, sobre todo en la UEA del HCVB, ya que aún no está informatizada y posee activos de información en constante riesgo.

Los beneficios de implantar un SGSI son, en primer lugar, obtener una reducción de riesgos debido al establecimiento y seguimiento de controles sobre ellos. Con ello se logra reducir las amenazas hasta alcanzar un nivel asumible por la institución. De este modo, si se produce una incidencia, los daños se minimizan y la continuidad de los Servicios está asegurada. En segundo lugar, se produce un ahorro de los costos derivados de una racionalización de los recursos. Se eliminan las inversiones innecesarias e ineficientes como las producidas por desestimar o sobrestimar riesgos. En tercer lugar, la seguridad se considera un sistema y se convierte en una actividad de gestión. La seguridad deja de ser un conjunto de actividades más o menos organizadas y pasa a transformarse en un ciclo de vida metódico y controlado, en el que participa toda la institución. En cuarto lugar, la institución se asegura del cumplimiento de la legislación vigente y se evitan riesgos y costes innecesarios. La entidad se asegura del cumplimiento del marco legal que protege a la institución de aspectos que probablemente no se habían tenido en cuenta anteriormente. Por último, pero no por ello menos importante, la certificación del SGSI contribuye a mejorar la competitividad en el mercado, diferenciando a las instituciones que lo han conseguido y haciéndolas más fiables e incrementando su prestigio. Un certificado mejora la imagen y confianza de una institución entre pacientes y proveedores que, poco a poco, exigen la certificación para abrir y compartir sus sistemas de información con cualquier institución. La exigencia de este certificado es el modo de garantizar un equilibrio en las medidas de seguridad entre las partes.

La contribución particular que proporciona este trabajo, corresponde a la entrega de una metodología para encaminar la implementación de un SGSI, adaptándola a los lineamientos que solicita la norma ISO/IEC 27001 y lo que pretende la UEA en cuánto a la seguridad de la información y la adopción del modelo PDCA en la aplicación de los procesos del SGSI.

A pesar de que la ISO/IEC 27001 entrega directrices que permiten encaminarse en la implantación del SGSI, la norma está un poco desordenada y en muchos puntos no detalla lo suficiente o no entrega ideas enlenteciendo el proceso. Es por ello, que el mayor aporte que tiene este diseño metodológico para implementar un SGSI en la UEA es que, a diferencia de la norma, posee un orden de aplicación que facilita al lector la comprensión de cada etapa y las actividades que se deben llevar a cabo en cada una de ellas. Además, entrega propuestas de herramientas e ideas que permiten tener más opciones al usuario de ella, ya que también se apoya en informes y papers que ejemplifican las actividades.

*6.3. Alcance de las contribuciones*

Esta metodología para la implementación de un SGSI según ISO/IEC 27001 está orientada al proceso de atención de urgencia adulto de la UEA, como una contribución inicial que debe ser revisada y discutida por la Dirección del hospital y todos los funcionarios de la UEA, para que en un futuro próximo pueda ser implementada en sus cuatro etapas del ciclo de mejora continua.

La norma recomienda empezar por un alcance limitado, es por ello que el alcance de esta metodología es la UEA del HCVB, la cual, después de ser implementada, puede abarcar otros procesos de la Unidad u otros servicios clínicos del hospital.

*6.4. Investigaciones futuras*

Al ser un trabajo de aplicación, se sugieren aplicaciones futuras en lugar de investigaciones futuras tales como:

(1) Redefinir el alcance del SGSI a otras Unidades o Servicios Clínicos del hospital.
(2) Redefinir el alcance a otros servicios no clínicos del hospital, servicios de otros hospitales así como también adaptar esta metodología a otras instituciones de salud.
(3) Implementar el SGSI en la UEA, según la metodología propuesta en este trabajo, en conjunto con la Dirección del hospital. Aplicar las fases hacer, verificar y actuar del ciclo PHVA (mejora continua) en su totalidad siguiendo la estructura definida en esta metodología.
(4) Desarrollar un sistema informático que ayude en el control de las medidas intervenidas en la implementación del SGSI.

**Referencias Bibliográficas**

Aenor (2014). ISO/IEC 27001: Seguridad de la información. Recuperado el 14 de mayo del 2015, de: http://www.aenorchile.com/seguridad-de-la-informaci%C3%B3n.aspx

Alcaldía Mayor Bogotá (2015). Proyecto de Implementación SIG. Recuperado el 14 de mayo del 2015, de: http://www.esecentrooriente.gov.co/hco/images/stories/planeacion/gestioncalidad/implementacion%20del%20sig.pdf

Alexander, A. (2007). *Diseño de un sistema de gestión de seguridad de información*. Editorial Alfaomega Colombiana. Bogotá, Colombia.

Atsec (2014). *Atsec, el proveedor de seguridad de la información*. Recuperado el 5 de noviembre del 2014, de: http://www.atsec.com/us/isms-iso-iec-27001-consulting.html

Audisec (2007). *Guía de implantación de un Sistema de Gestión de Seguridad de la información UNE-ISO/IEC 27001:2007 Herramienta Global SGSI*. Recuperado el 15 de octubre del 2014, de: http://www.criptored.upm.es/descarga/GUIA_AUDISEC_GLOBALSGSI.pdf

Bestratén, M., Orriols, R., y Mata, C. (2004). *NTP 679: Análisis modal de fallos y efectos AMFE. Instituto Nacional de Seguridad e Higiene en el trabajo*. Notas Técnicas de Prevención. 679. P 1 - 8. Recuperado el 24 de octubre del 2014, de: http://www.insht.es/InshtWeb/Contenidos/Documentacion/FichasTecnicas/NTP/Ficheros/601a700/ntp_679.pdf

Buitrago, Bonilla, Murillo (2012). *Diseño de una Metodología para la Implementación del Sistema de Gestión de Seguridad de la Información en el sector de Laboratorios de Análisis Microbiológicos*. Tesis de maestría no publicada, Universidad EAN, Bogotá, Colombia.

Calidad y Gestión (2015). *Consultoria Ambiental, Calidad, Seguridad, Inocuidad Alimentaria, Eficiencia Energética: Ciclo PDCA: Estrategia para la mejora continua*. Recuperado el 24 de abril del 2015, de: http://www.calidad-gestion.com.ar/boletin/58_ciclo_pdca_estrategia_para_mejora_continua.html

Camacho, G. (2015). Sistema de Gestión de Seguridad de la Información Hospital Del Sur, Bogotá. Recuperado el 19 de mayo del 2015, de: https://prezi.com/18pgwcjcrnhq/sistema-de-gestion-de-seguridad-de-la-informacion-hospital/

Castro, E. (2013). *Manual Administrativo de Aplicación General en la materia de Tecnologías de la Información y Comunicaciones y de Seguridad de la Información.* Ciudad de México, México. Recuperado el 21 de abril del 2015, de: http://www.hospitaljuarez.salud.gob.mx/interior/NORMATECA/MAAGTIC-SI-HJM_Final.pdf

Dane (2015). Dirección de regulación, planeación, estandarización y normalización: *Metodología de línea base de indicadores*. Recuperado el 1 de junio del 2015, de: http://www.dane.gov.co/files/planificacion/LineaBase/metodologia/metodologia .pdf

Díaz, J. (2010). *Negocios y emprendimiento: Plantilla para aplicar el ciclo PHVA.* Recuperado el 5 de noviembre del 2014, de: http://www.negociosyemprendimiento.org/2010/08/plantilla-para-aplicar-el-ciclo-phva-de.html

Dirección de Presupuestos (2015). *Gobierno de Chile: Indicadores de desempeño*. Santiago, Chile. Recuperado el 4 de mayo del 2015, de: http://www.dipres.gob.cl/572/w3-article-36280.html

Estrategia Digital de Salud 1 (2014). *Departamento de Gestión Sectorial TIC asume el liderazgo para dar cumplimiento al PMG de Seguridad de la Información*. Recuperado el 30 de octubre del 2014, de: http://www.salud-e.cl/prensa/departamento-de-gestion-sectorial-tic-asume-el-liderazgo-para-dar-cumplimiento-al-pmg-pmg-de-seguridad-de-la-informacion/

Estrategia Digital de Salud 2 (2014). *Comité de Seguridad de la Información supervisa la implementación del Plan de Trabajo 2014*. Recuperado el 30 de octubre del 2014, de: http://www.salud-e.cl/prensa/comite-de-seguridad-de-la-informacion-supervisa-la-implementacion-del-plan-de-trabajo-2014/

Estrategia Digital de Salud 3 (2014). *Servicios de Salud, Seremis y Divisiones del MINSAL se capacitan en seguridad de la información*. Recuperado el 30 de octubre del 2014, de: http://www.salud-e.cl/destacados-home/servicios-de-salud-seremis-y-divisiones-del-minsal-se-capacitan-en-seguridad-de-la-informacion/

Gavilanes, V. (2011). *Elaborar una Metodología aplicando la norma ISO/IEC 27001 en la Implementación de un Sistema de Gestión de Seguridad de la Información en el Desitel.* Tesis de licenciatura no publicada, ESPOCH, Riobamba, Ecuador.

Gómez, J. (2014). Enfermero Coordinar Unidad Urgencia. Comunicación personal en octubre y noviembre del año 2014.

Guzmán, A., Moreno, B. (2011). Protocolo categorización de demanda en la red local de Urgencia del Servicio de Salud O'Higgins (SSO), Rancagua, Chile. Recuperado el 23 de octubre del 2014, de: http://www.saludohiggins.cl/attachments/1080_P.%20de%20Categorizacion%20(C1%20a%20C5).pdf

Hospital Carlos Van Buren (2015). *Página web: Unidad de Emergencia Adultos (UEA).* Recuperado el 1 de julio del 2015, de: http://www.hospitalcarlosvanburen.cl/index.php?option=com_content&view=article&id=174&Itemid=94

Hospital Centro Oriente (2015). *Sistema Integrado de Gestión*. Recuperado el 2 de junio del 2015, de: http://www.esecentrooriente.gov.co/hco/

Hospital Del Sur (2015). *Calidad: Sistema Integrado de Gestión.* Recuperado el 2 de junio del 2015, de; http://www.hospitalsur.gov.co/

Hospitales San Roque (2015). *Hospitales San Roque dispone de certificación en las Normas ISO 9001, 14001 y 27001*. Recuperado el 2 de junio del 2015, de: http://hospitalessanroque.com/es/calidad

IEC (2014*). International Electrotechnical Comission: Vision and Mission*. Recuperado el 29 de septiembre del 2014, de: http://www.iec.ch/about/?ref=menu

ISO (2014). *International Organization for Standardization: Standards*. Recuperado el 30 de septiembre del 2014, de: http://www.iso.org/iso/home/standards.htm

ISO/IEC 27000 (2009). *Normativa ISO 27000:2009: Overview and vocabulary*. Recuperado el 21 de octubre del 2014, de: http://www.iso.org/iso/catalogue_detail?csnumber=41933

ISO/IEC 27000 (2014). *El portal de ISO 27000 en español*. Recuperado el 4 de junio del 2015, de: http://www.iso27000.es/sgsi.html

ISO/IEC 27001 (2005). *Estándar internacional. Tecnología de la Información - Técnicas de seguridad Sistemas de gestión de seguridad de la información – Requerimientos*. Recuperado el 2 de septiembre del 2014, de: http://www.academia.edu/11138718/EST%C3%81NDAR_ISO_IEC_INTERNACIONAL_Tecnolog%C3%ADa_de_la_Informaci%C3%B3n_T%C3%A9cnicas_de_seguridad_Sistemas_de_gesti%C3%B3n_de_seguridad_de_la_informaci%C3%B3n_Requerimientos

ISO/IEC 27002 (2015). *El portal de ISO 27002 en español: controles de ISO/IEC 27002*. Recuperado el 12 de mayo del 2015, de: http://www.iso27000.es/iso27002.html

ISO Survey (2013). The ISO Survey of Management System Standard Certifications: *Executive summary*. Recuperado el 9 de septiembre del 2014, de: http://www.iso.org/iso/iso_survey_executive-summary.pdf?v2013

ISO 27001 Survey data (2013). *The ISO 27001 Survey Data, Planilla excel*. Recuperado el 9 de septiembre del 2014, de: http://www.iso.org/iso/home/standards/certification/iso-survey.htm?certificate=ISO/IEC%2027001&countrycode=CL#countrypick

Ley Nº 19.223. Tipifica figuras penales relativas a la informática. Ministerio de Justicia, Santiago, Chile, 7 de junio de 1993.

Ley Nº 19.628. Protección de datos de carácter personal. Ministerio Secretaría general de la presidencia, Santiago, Chile, 28 de agosto de 1999.

Ley Nº 20.584. Derechos y Deberes de las Personas en Atención de Salud; Acciones Vinculadas a la Atención en Salud; (2012). Ministerio de Salud, Subsecretaría de Salud Pública, Santiago, Chile, 24 de abril de 2012.

Logra (2012). *Consultoría para la Estandarización de Procesos de Redes Asistenciales MINSAL: Proceso de Urgencia (UEH)*. Santiago, Chile. Recuperado el 13 de junio del 2015, de: https://www.ssmaule.cl/dig/C%20Gesti%C3%B3n%20A%C3%B1os/CG2014/URGENCIA/3.%20Red%20de%20Urgencia%20(UEH)-FINAL.pdf

Magerit (2012). *Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.* Recuperado el 30 de octubre del 2014, de: https://www.ccn-cert.cni.es/publico/herramientas/pilar5/magerit/Libro_I_metodo.pdf

MINSAL (2014). *Ministerio de Salud: Estrategia Digital de Salud: sistema de seguridad de la información*. Recuperado el 7 de noviembre del 2014, de: http://www.salud-e.cl/category/politicas/seguridad-de-la-informacion/

Olguín, E. (2014). Jefe Departamento Informática Servicio de Salud Valparaíso – San Antonio. Comunicación personal año 2014 y 2015.

Pallas, G. (2009). *Metodología de Implantación de un SGSI en un grupo empresarial jerárquico*. Tesis de maestría no publicada, Universidad de la República, Montevideo, Uruguay.

Pérez, E. (2011). *Activos, ataques, amenazas y vulnerabilidades*. Recuperado el 14 de octubre del 2014, de: http://es.slideshare.net/jonbonachon/activos-ataques-amenazas-y-vulnerabilidades-de-informacin

Poveda, J. (2007). *Gestión y tratamiento de los riesgos: selección de los controles*. Madrid, España. Recuperado el 12 de junio del 2015, de: https://jmpovedar.files.wordpress.com/2011/03/mc3b3dulo-9.pdf

Project Management (2014). *Sistema de Gestión de la Seguridad de la Información: ISO 27001*. Recuperado el 5 de mayo del 2015, de: http://www.pmconsultores.com/portal/content.asp?ContentId=%20667

Soto, K. (2015). Enfermera Supervisora Unidad de Emergencia Adulto (UEA) del Hospital Carlos Van Buren. Comunicación personal año 2015

Toro, M. (2011). *Plan de seguridad de la información ISO 27002 Vs COBIT. Normas y Calidad. ICONTEC*. Cuarta edición. P 26 – 28.

Unidad de Modernización y Gobierno Electrónico (2012). *Seminario de la información: Gestión Seguridad de la Información (SGI), marco normativo*. Santiago, Chile. Recuperado el 22 de octubre del 2014, de: http://es.slideshare.net/modernizacioncl/gestin-seguridad-de-la-informacin-y-marco-normativo-12675211

Universidad Nacional de Colombia (2015). *Plan de Gestión de un SGS*. Recuperado el 28 de mayo del 2015, de: http://datateca.unad.edu.co/contenidos/233003/modulo/modulo-233003-online/capitulo_4_plan_de_gestion_de_un_sgsi.html

Vera, F. (2013). Entrevista programa "Demasiado tarde": *ONG Derechos Digitales*. Recuperado el 3 de octubre del 2015, de: https://www.youtube.com/watch?v=mZiM2iwSqVU

**Glosario**



*Activo:* Cualquier cosa que tenga valor para la organización.

*Análisis de riesgo:* Uso sistemático de la información para identificar fuentes y para estimar el riesgo.

*Confidencialidad:* La propiedad que esa información esté disponible y no sea divulgada a personas, entidades o procesos no-autorizados.

*Disponibilidad:* La propiedad de estar disponible y utilizable cuando lo requiera una entidad autorizada.

*Evaluación del riesgo:* Proceso de comparar el riesgo estimado con el criterio de riesgo dado para determinar la importancia del riesgo.

*Evento de seguridad de la información:* Una ocurrencia identificada del estado de un sistema, servicio o red indicando una posible violación de la política de seguridad de la información o falla en las salvaguardas, o una situación previamente desconocida que puede ser relevante para la seguridad.

*Gestión del riesgo:* Actividades para dirigir y controlar una organización con relación al riesgo.

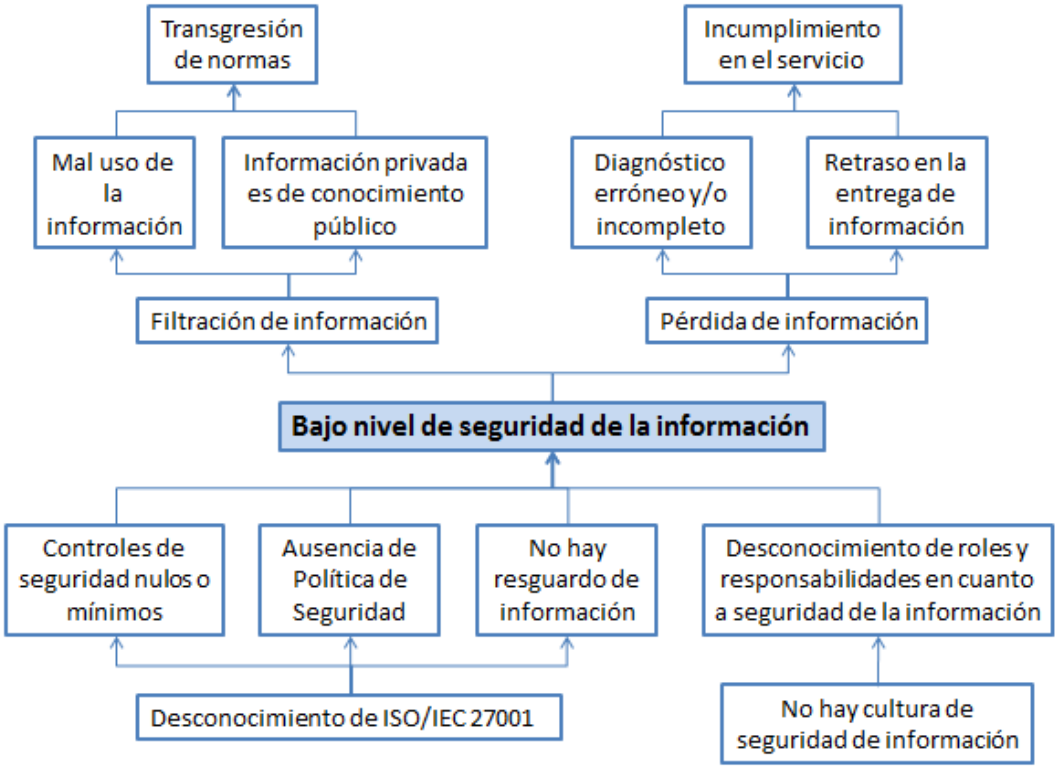
*Incidente de seguridad de la información*: Un solo o una serie de eventos de seguridad de la información no deseados o inesperados que tienen una significativa probabilidad de comprometer las operaciones comerciales y amenazan la seguridad de la información.

*Integridad:* La propiedad de salvaguardar la exactitud e integridad de los activos.

*Seguridad de información:* Preservación de la confidencialidad, integridad y disponibilidad de la información; además, también pueden estar involucradas otras propiedades como la autenticidad, responsabilidad, no-repudio y confiabilidad.

*Sistema de gestión de seguridad de la información SGSI:* Esa parte del sistema gerencial general, basado en un enfoque de riesgo comercial; para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información.

**Anexo 1**
Árbol del problema



## Anexo 2
N° Certificados África y Asia Central y Sur

| AFRICA | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Año** | **2006** | **2007** | **2008** | **2009** | **2010** | **2011** | **2012** | **2013** |
| **País** | **6** | **10** | **16** | **47** | **46** | **40** | **64** | **99** |
| Argelia | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 2 |
| Angola | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 |
| Botswana | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 |
| Burundi | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 |
| República de Congo | 0 | 0 | 0 | 1 | 1 | 0 | 1 | 0 |
| Egipto | 1 | 2 | 3 | 7 | 8 | 6 | 11 | 17 |
| Etiopía | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 |
| Gabón | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 |
| Ghana | 0 | 0 | 0 | 3 | 1 | 3 | 0 | 3 |
| Kenia | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 |
| Lesoto | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 |
| Malawi | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 |
| Mauricio | 0 | 0 | 1 | 2 | 3 | 4 | 8 | 11 |
| Marruecos | 0 | 0 | 2 | 2 | 1 | 5 | 7 | 9 |
| Mozambique | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 |
| Niger | 0 | 0 | 0 | 1 | 2 | 0 | 0 | 0 |
| Nigeria | 0 | 0 | 0 | 0 | 0 | 5 | 9 | 12 |
| Ruanda | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 |
| Sierra Leona | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 |
| Sudáfrica | 5 | 8 | 10 | 14 | 14 | 14 | 22 | 35 |
| Sudán | 0 | 0 | 0 | 2 | 2 | 0 | 1 | 1 |
| Swazilandia | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 |
| República Unida de Tanzania | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 |
| Túnez | 0 | 0 | 0 | 2 | 0 | 1 | 2 | 8 |
| Uganda | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 |
| Zambia | 0 | 0 | 0 | 1 | 2 | 1 | 0 | 0 |
| Zimbabue | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 |

| ASIA CENTRAL Y SUR | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Año** | **2006** | **2007** | **2008** | **2009** | **2010** | **2011** | **2012** | **2013** |
| **País** | **383** | **519** | **839** | **1303** | **1328** | **1497** | **1668** | **2061** |
| Afganistán | 0 | 0 | 0 | 2 | 1 | 5 | 0 | 2 |
| Bangladesh | 0 | 0 | 0 | 2 | 1 | 1 | 9 | 9 |
| India | 369 | 508 | 813 | 1240 | 1281 | 1427 | 1611 | 1931 |
| Kazajstán | 0 | 0 | 3 | 4 | 3 | 3 | 5 | 8 |
| Kirguistán | 0 | 1 | 1 | 2 | 1 | 0 | 0 | 0 |
| Nepal | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 |
| Pakistán | 1 | 4 | 12 | 28 | 18 | 19 | 16 | 17 |
| Sri Lanka | 13 | 6 | 10 | 23 | 21 | 42 | 27 | 37 |
| Tayikistán | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 57 |

## Anexo 3
N° Certificados Europa

| EUROPA | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Año** | **2006** | **2007** | **2008** | **2009** | **2010** | **2011** | **2012** | **2013** |
| **País** | **1064** | **1432** | **2172** | **3563** | **4800** | **5289** | **6379** | **7950** |
| Albania | 0 | 0 | 0 | 0 | 0 | 3 | 2 | 7 |
| Armenia | 0 | 0 | 1 | 0 | 0 | 0 | 3 | 7 |
| Austria | 16 | 23 | 32 | 37 | 54 | 59 | 28 | 75 |
| Bielorrusia | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 1 |
| Bélgica | 4 | 9 | 15 | 19 | 26 | 29 | 31 | 47 |
| Bosnia y Herzegovina | 0 | 0 | 0 | 4 | 4 | 2 | 7 | 9 |
| Bulgaria | 0 | 8 | 23 | 60 | 116 | 132 | 208 | 278 |
| Croacia | 2 | 5 | 10 | 22 | 24 | 32 | 58 | 69 |
| Chipre | 0 | 0 | 0 | 3 | 4 | 5 | 9 | 16 |
| República Checa | 27 | 77 | 88 | 264 | 529 | 301 | 264 | 397 |
| Dinamarca | 3 | 4 | 4 | 9 | 6 | 5 | 7 | 8 |
| Estonia | 0 | 1 | 1 | 1 | 1 | 1 | 2 | 2 |
| Finlandia | 1 | 14 | 13 | 18 | 23 | 27 | 28 | 32 |
| Francia | 5 | 9 | 14 | 15 | 31 | 46 | 66 | 94 |
| Georgia | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 |
| Alemania | 95 | 135 | 239 | 253 | 357 | 424 | 488 | 581 |
| Gibraltar (Reino Unido) | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 |
| Grecia | 3 | 5 | 20 | 28 | 44 | 45 | 49 | 77 |
| Hungría | 54 | 81 | 135 | 146 | 151 | 178 | 199 | 280 |
| Islandia | 10 | 11 | 13 | 16 | 20 | 21 | 20 | 26 |
| Irlanda | 6 | 7 | 10 | 21 | 24 | 30 | 48 | 54 |
| Italia | 175 | 148 | 233 | 297 | 374 | 425 | 495 | 901 |
| Letonia | 0 | 0 | 1 | 2 | 6 | 9 | 9 | 18 |
| Lituania | 0 | 2 | 3 | 7 | 11 | 14 | 19 | 23 |
| Luxembuergo | 1 | 2 | 2 | 2 | 5 | 8 | 7 | 5 |
| Malta | 0 | 1 | 1 | 1 | 2 | 2 | 5 | 7 |
| Moldavia | 1 | 1 | 1 | 2 | 2 | 1 | 1 | 3 |
| Montenegro | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 |
| Paises Bajos | 41 | 41 | 56 | 76 | 97 | 125 | 190 | 316 |
| Noruega | 15 | 22 | 16 | 17 | 25 | 31 | 16 | 26 |
| Polonia | 11 | 45 | 75 | 187 | 229 | 233 | 279 | 307 |
| Portugal | 1 | 4 | 4 | 5 | 17 | 20 | 34 | 58 |
| Rumania | 4 | 16 | 44 | 303 | 350 | 575 | 866 | 840 |
| Federación de Rusia | 5 | 9 | 17 | 53 | 72 | 31 | 27 | 48 |
| República de San Marino | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 |
| Serbia | 0 | 0 | 0 | 3 | 8 | 9 | 25 | 43 |
| Eslovaquia | 4 | 12 | 28 | 50 | 70 | 111 | 127 | 159 |
| Eslovenia | 5 | 12 | 16 | 27 | 33 | 31 | 13 | 49 |
| España | 23 | 93 | 203 | 483 | 711 | 642 | 805 | 799 |
| Suecia | 20 | 55 | 18 | 30 | 30 | 37 | 32 | 49 |
| Suiza | 34 | 32 | 58 | 57 | 61 | 66 | 65 | 111 |
| La ex República Yugoslava de Macedonia | 1 | 1 | 4 | 6 | 7 | 7 | 5 | 9 |
| Turquía | 10 | 27 | 33 | 86 | 117 | 100 | 132 | 181 |
| Ucrania | 1 | 1 | 3 | 5 | 1 | 6 | 7 | 12 |
| Reino Unido | 486 | 519 | 738 | 946 | 1157 | 1464 | 1701 | 1923 |

## Anexo 4
N° Certificados Asia Oriental y Pacífico

| ASIA ORIENTAL Y PACÍFICO | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Año** | **2006** | **2007** | **2008** | **2009** | **2010** | **2011** | **2012** | **2013** |
| **País** | **4210** | **5550** | **5807** | **7394** | **8788** | **9665** | **10422** | **10748** |
| Australia | 59 | 55 | 63 | 55 | 82 | 94 | 113 | 138 |
| Camboya | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 |
| China | 75 | 146 | 236 | 459 | 957 | 1219 | 1490 | 1710 |
| Hong Kong, China | 29 | 36 | 59 | 72 | 78 | 99 | 110 | 124 |
| Macao, China | 2 | 5 | 2 | 7 | 9 | 12 | 13 | 15 |
| Taipei, China | 159 | 256 | 702 | 934 | 1028 | 791 | 855 | 861 |
| Fiji | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 |
| Indonesia | 2 | 3 | 7 | 13 | 22 | 29 | 35 | 48 |
| Japón | 3790 | 4896 | 4425 | 5508 | 6237 | 6914 | 7199 | 7084 |
| Reoública Popular Democrática, Korea | 0 | 0 | 95 | 0 | 1 | 0 | 1 | 0 |
| República de Korea | 50 | 77 | 94 | 174 | 166 | 191 | 230 | 252 |
| Malasia | 18 | 23 | 34 | 38 | 60 | 72 | 100 | 181 |
| Mongolia | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 |
| Myanmar | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 |
| Nueva Zelanda | 1 | 1 | 4 | 5 | 5 | 5 | 5 | 12 |
| Filipinas | 10 | 24 | 27 | 47 | 38 | 59 | 66 | 73 |
| Singapur | 7 | 17 | 36 | 41 | 43 | 68 | 65 | 84 |
| Tailandia | 7 | 9 | 16 | 34 | 39 | 76 | 96 | 125 |
| Viet Nam | 1 | 2 | 7 | 5 | 21 | 36 | 44 | 39 |

## Anexo 5

N° Certificados Medio Oriente y Norteamérica

| MEDIO ORIENTE | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Año** | **2006** | **2007** | **2008** | **2009** | **2010** | **2011** | **2012** | **2013** |
| **País** | **37** | **71** | **128** | **206** | **218** | **279** | **332** | **451** |
| Bahrein | 3 | 5 | 8 | 12 | 8 | 6 | 15 | 20 |
| República Islámica de Irán | 0 | 1 | 1 | 6 | 7 | 13 | 4 | 9 |
| Irak | 0 | 0 | 0 | 10 | 0 | 1 | 0 | 0 |
| Israel | 0 | 24 | 61 | 78 | 86 | 110 | 130 | 185 |
| Jordania | 0 | 1 | 1 | 1 | 2 | 1 | 3 | 2 |
| Kuwait | 4 | 6 | 7 | 10 | 18 | 15 | 17 | 15 |
| Líbano | 1 | 0 | 0 | 1 | 1 | 3 | 3 | 3 |
| Omán | 3 | 4 | 3 | 8 | 9 | 11 | 10 | 11 |
| Palestina | 0 | 0 | 0 | 1 | 1 | 0 | 1 | 1 |
| Katar | 0 | 0 | 1 | 3 | 6 | 9 | 7 | 23 |
| Arabia Saudita | 12 | 15 | 18 | 21 | 23 | 37 | 46 | 59 |
| República Árabe Siria | 0 | 0 | 0 | 2 | 0 | 0 | 0 | 0 |
| Emiratos Árabes Unidos | 14 | 15 | 27 | 53 | 57 | 73 | 96 | 123 |
| Yemen | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 |

| NORTEAMÉRICA | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Año** | **2006** | **2007** | **2008** | **2009** | **2010** | **2011** | **2012** | **2013** |
| **País** | **79** | **112** | **212** | **322** | **329** | **435** | **552** | **712** |
| Canadá | 1 | 5 | 13 | 21 | 26 | 50 | 62 | 66 |
| México | 9 | 13 | 31 | 49 | 56 | 70 | 75 | 80 |
| EE.UU | 69 | 94 | 168 | 252 | 247 | 315 | 415 | 566 |

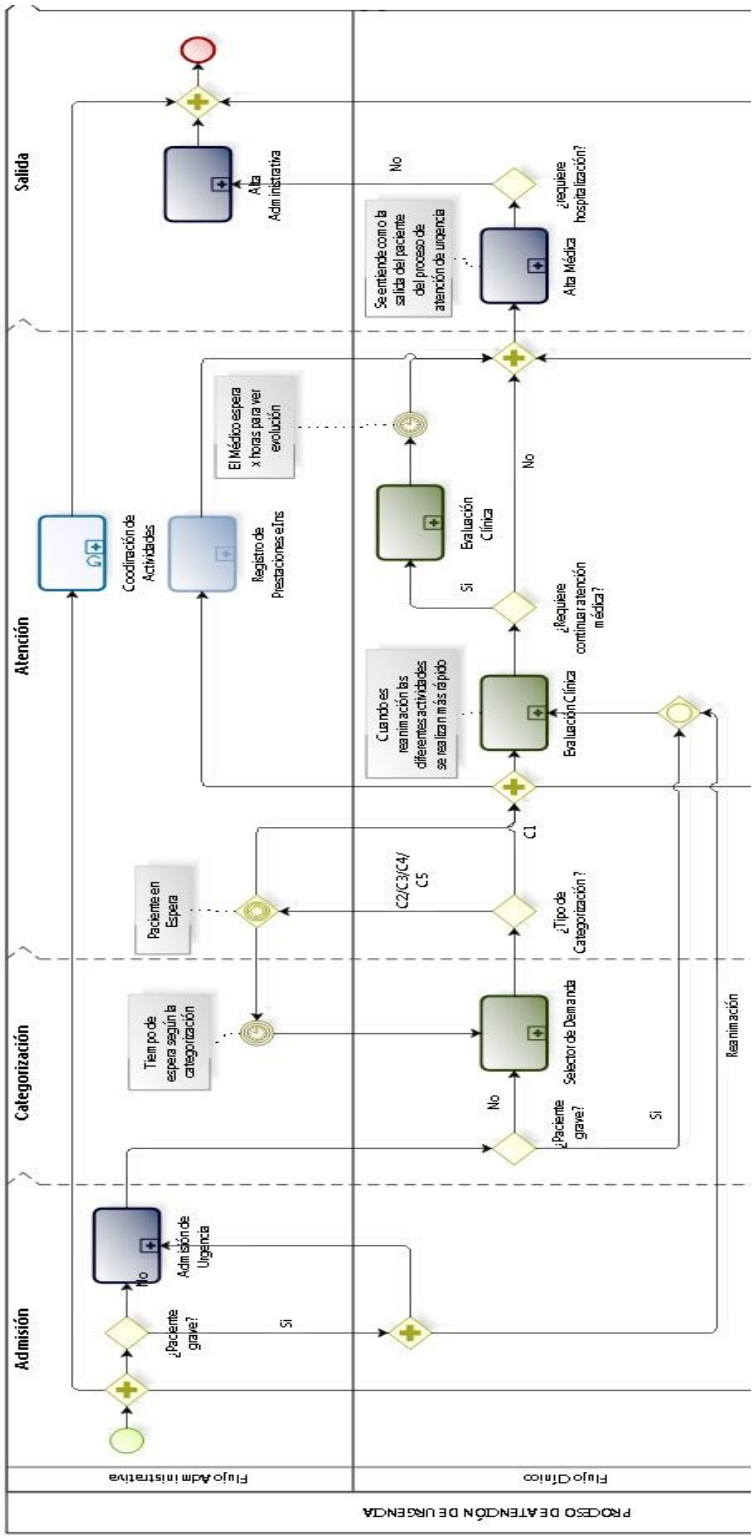
## Anexo 6

N° Certificados por sector industrial el año 2013

| | | 2006 | 2007 | 2008 | 2009 | 2010 | 2011 | 2012 | 2013 |
|---|---|---|---|---|---|---|---|---|---|
| 1 | Agricultura, pesca | 1 | 45 | 1 | 13 | 8 | 14 | 13 | 13 |
| 2 | Minas y canteras | 0 | 1 | 3 | 6 | 2 | 12 | 31 | 34 |
| 3 | Productos alimenticios, bebidas y tabaco | 3 | 14 | 1 | 10 | 6 | 8 | 10 | 24 |
| 4 | Textiles y productos textiles | 0 | 1 | 1 | 3 | 3 | 2 | 12 | 10 |
| 5 | Cuero y productos de cuero | 0 | 0 | 0 | 1 | 2 | 5 | 1 | 2 |
| 6 | Madera y productos de madera | 0 | 0 | 0 | 1 | 3 | 5 | 4 | 4 |
| 7 | Pulpa de madera, papel y productos de papel | 2 | 6 | 6 | 7 | 4 | 7 | 13 | 17 |
| 8 | Editoriales | 1 | 5 | 6 | 10 | 11 | 20 | 18 | 22 |
| 9 | Empresas de impresión | 34 | 84 | 30 | 62 | 78 | 101 | 121 | 148 |
| 10 | Manufactura de coque y productos de petróleo refinado | 3 | 6 | 9 | 8 | 3 | 5 | 4 | 14 |
| 11 | Combustible nuclear | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 2 |
| 12 | Química, productos químicos y fibra | 7 | 3 | 3 | 9 | 9 | 9 | 11 | 24 |
| 13 | Productos farmaceúticos | 0 | 1 | 3 | 4 | 6 | 3 | 0 | 3 |
| 14 | Caucho y plásticos | 7 | 5 | 0 | 10 | 15 | 16 | 16 | 36 |
| 15 | Productos minerales no metálicos | 1 | 3 | 0 | 16 | 16 | 8 | 0 | 5 |
| 16 | Hormigón, cemento, cal, yeso, etc. | 1 | 1 | 1 | 6 | 6 | 14 | 27 | 25 |
| 17 | Metal básico y fabricación de productos de metal | 10 | 5 | 2 | 16 | 25 | 28 | 36 | 50 |
| 18 | Maquinaria y equipamiento | 18 | 10 | 9 | 29 | 31 | 36 | 43 | 52 |
| 19 | Equipamiento eléctrico y óptico | 38 | 58 | 50 | 135 | 221 | 280 | 342 | 289 |
| 20 | Construcción naval | 0 | 0 | 2 | 5 | 3 | 3 | 4 | 8 |
| 21 | Aeroespacial | 0 | 7 | 12 | 22 | 24 | 17 | 22 | 18 |
| 22 | Otro equipamiento de transporte | 1 | 3 | 2 | 4 | 4 | 7 | 4 | 25 |
| 23 | De fabricación no clasificados en otra parte | 4 | 14 | 2 | 5 | 5 | 23 | 8 | 5 |
| 24 | Reciclaje | 2 | 10 | 4 | 11 | 32 | 44 | 61 | 72 |
| 25 | Suministro de electricidad | 8 | 10 | 11 | 20 | 9 | 12 | 15 | 45 |
| 26 | Suministro de gas | 0 | 2 | 2 | 4 | 3 | 2 | 6 | 6 |
| 27 | Suministro de agua | 1 | 1 | 2 | 11 | 13 | 13 | 10 | 23 |
| 28 | Construcción | 55 | 17 | 12 | 127 | 266 | 350 | 409 | 396 |
| 29 | Al por mayor y menor; reparación de vehículos, motocicletas y artículos personales y del hogar | 12 | 38 | 26 | 93 | 164 | 214 | 215 | 224 |
| 30 | Hoteles y restaurantes | 2 | 4 | 0 | 6 | 10 | 32 | 4 | 5 |
| 31 | Transporte, almacenamiento y comunicaciones | 60 | 70 | 63 | 170 | 184 | 241 | 288 | 322 |
| 32 | Intermediación financiera, bienes raíces, arriendo | 47 | 54 | 68 | 148 | 185 | 113 | 138 | 169 |
| 33 | Tecnologías de la información | 890 | 1236 | 1152 | 2086 | 3217 | 3588 | 4558 | 5059 |
| 34 | Servicios de ingeniería | 25 | 33 | 48 | 173 | 122 | 126 | 189 | 211 |
| 35 | Otros servicios | 189 | 204 | 228 | 380 | 579 | 564 | 755 | 849 |
| 36 | Administración pública | 23 | 33 | 79 | 181 | 79 | 106 | 155 | 192 |
| 37 | Educación | 8 | 9 | 25 | 47 | 75 | 65 | 102 | 101 |
| 38 | Salud y trabajo social | 14 | 10 | 61 | 102 | 102 | 145 | 201 | 201 |
| 39 | Otros servicios sociales | 8 | 13 | 16 | 46 | 54 | 75 | 98 | 106 |
| **TOTAL** | | **1475** | **2016** | **1940** | **3987** | **5579** | **6314** | **7945** | **8811** |

**Anexo 7**

Diagrama de proceso de urgencia



## Anexo 8

Encuesta de evaluación seguridad de la información HCVB

| | Ambito | Pregunta | SI/NO | Comentarios |
|---|---|---|---|---|
| 1 | **Política de Seguridad (A.5)** | ¿Han establecido el enfoque de la política en línea con los objetivos que tienen como hospital y el compromiso con la seguridad de la información a través de un documento? | NO | |
| 2 | **Política de Seguridad (A.5)** | Este documento, en el caso de tenerlo, ¿es revisado de forma regular? | NO | |
| 3 | **Organización de la seguridad de la información (A.6)** *Organización Interna* | ¿Se ha establecido un marco referencial a nivel directivo para inciar y controlar la implementación de la seguridad de la información? | NO | |
| 4 | **Organización de la seguridad de la información (A.6)** *Organización Interna* | ¿Existe un comité multidisciplinario el cual tenga designado cada rol de seguridad mediante una resolución? | NO | |
| 5 | **Organización de la seguridad de la información (A.6)** *Organización Interna* | ¿Existe contacto con especialistas o grupos de seguridad externos con la idea de mantenerse informado con las tendencias mundiales, monitorear los estándares y evaluar los métodos? | NO | |
| 6 | **Organización de la seguridad de la información (A.6)** *Entidades Externas* | ¿Están identificados los riesgos que poseen la información y sus medios de procesamiento relacionados con entidades externas? | NO | |
| 7 | **Gestión de activos (A.7)** | ¿Se han identificado los activos de información y los responsables del mantenimiento de sus respectivos controles? | NO | |
| 8 | **Gestión de activos (A.7)** | ¿Existe una clasificación de la información según su necesidad, prioridad y grado de protección esperado en su manejo? | NO | Salvo la información personal y ficha clinica que está protegida por ley |
| 9 | **Seguridad física y ambiental (A.9)** *Áreas Seguras* | ¿Existen perímetros de seguridad física con barreras apropiadas de seguridad y controles de entrada con el fin de proteger áreas que contengan información y medios de procesamiento de información? | SI | |
| 10 | **Seguridad física y ambiental (A.9)** *Seguridad del equipo* | ¿Existe alguna protección, para todos los equipos del hospital, de riesgos tales como: acceso no autorizado; pérdida, daño o robo; fallas en los servicios básicos, condición del cableado? | SI | |
| 11 | **Control de acceso (A.11)** | ¿Procedimientos para controlar la asignación de los derechos (perfiles) para todas las etapas del acceso del usuario a los sistemas y los servicios de información? | SI | Pero no están concentrados en una sola unidad. |
| 12 | **Control de acceso (A.11)** | ¿Los usuarios autorizados se encuentran informados de sus responsabilidades para la mantención de controles de acceso efectivos? | SI | |
| 13 | **Control de acceso (A.11)** | ¿Existen medios de seguridad para que el acceso a las redes por parte del usuario no comprometa la seguridad de los servicios de la red, además de mantener restringido el acceso a los sistemas operativos a los usuarios no autorizados? | SI | Nivel de seguridad básico, no existen herramientas de monitoreo |
| 14 | **Gestión de continuidad comercial (A.14)** | ¿Se ha implementado un proceso de gestión de la continuidad de los servicios prestados por el hospital que minimice el impacto sobre este y que logre recuperar las pérdidas de activos de información hasta un nivel aceptable? | NO | Muy básico |
| 15 | **Gestión de continuidad comercial (A.14)** | Este proceso de gestión ¿cuenta con controles para identificar y reducir los riesgos? Esto además del proceso general de evaluación de riesgos, para permitir la disponibilidad de la información requerida | NO | |

## Anexo 9

Resumen controles y objetivos de control ISO/ IEC 27001 Anexo A

| | | |
|---|---|---|
| **POLITICA DE SEGURIDAD** | | |
| Documento y revisión de la política de seguridad de la información | A.5.1, A.5.1.1 Y A5.1.2 | Aprobar un documento de política de seguridad de la información, hacerlo conocer y revisar para garantizar que siga siendo adecuada, suficiente y eficaz |
| **ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN** | | |
| Compromiso de la dirección con la seguridad de la información | A6.1.1 | La dirección debe apoyar activamente la seguridad dentro de la organización |
| Coordinación y asignación de responsabilidades para la seguridad de la información | A6.1.2 Y A6.1.3 | Las actividades de la seguridad de la información deben ser coordinadas y definir claramente todas las responsabilidades |
| Procesos de autorización para los servicios de procesamiento de información | A6.1.4 | Definir e implementar un proceso de autorización para nuevos servicios de procesamiento de la información |
| Acuerdos sobre confidencialidad | A6.1.5 | Revisar los requisitos de confidencialidad |
| Contacto con las autoridades y con grupos de interés especiales | A6.1.6 Y A6.1.7 | Mantener contactos apropiados con las autoridades pertinentes y con grupos de interés especiales |
| Revisión independiente de la seguridad de la información | A6.1.8 | Revisar el enfoque de la organización para la gestión de la seguridad de la información |
| Identificación de los riesgos relacionados con las partes externas | A6.2.1 | Identificar los riesgos para la información |
| Consideraciones de la seguridad cuando se trata con los clientes y en los acuerdos con terceras partes | A6.2.2 Y A6.2.3 | Todos los requisitos de seguridad se deben considerar antes de dar acceso o hacer acuerdos |
| **GESTIÓN DE ACTIVOS** | | |
| Inventario, propiedad y uso aceptable de los activos | A7.1.1, A7.1.2 Y A.7.1.3 | Todos los activos y la información deben estar identificados y documentados |
| Directrices, etiquetado y manejo de la clasificación de la información | A7.2.1 Y A7.2.2 | La información se debe etiquetas y clasificar teniendo en cuenta la importancia y valor |

| SEGURIDAD DE LOS RECURSOS HUMANOS | | |
|---|---|---|
| Roles y responsabilidades de los empleados, selección y términos y condiciones laborales | A8.1.1, A8.1.2 Y A8.1.3 | Se deben documentar los roles y responsabilidades, verificar los antecedentes de los candidatos a empleados y deben estar de acuerdo con las condiciones del contrato laboral |
| Responsabilidad de la dirección durante la vigencia de la contratación laboral | A8.2.1 | La dirección debe exigir que se aplique la seguridad según las políticas establecidas |
| Educación, formación y concientización sobre la seguridad de la información | A8.2.2 | Todos los empleados y terceros deben recibir formación sobre las políticas |
| Proceso disciplinario | A8.2.3 | Debe existir un proceso disciplinario formal |
| Responsabilidades en la terminación del contrato laboral | A8.3.1 | Asignar las responsabilidades para llevar a cabo la terminación del contrato laboral |
| Devolución de activos | A8.3.2 | Empleados y terceros deben devolver los activos pertenecientes a la organización |
| Retiro de los derechos de acceso | A8.3.3 | Retiro de los derechos de acceso |
| SEGURIDAD FISICA Y DEL ENTORNO | | |
| Perímetro de seguridad física | A9.1.1 | Se deben utilizar perímetros de seguridad, las áreas deben estar protegidas con controles de acceso, aplicar seguridad física, protecciones contra daños por desastres naturales o artificiales y aislar el acceso no autorizado |
| Controles de acceso físico | A9.1.2 | |
| Seguridad de oficinas, recintos e instalaciones | A9.1.3 | |
| Protección contra amenazas externas y ambientales | A9.1.4 | |
| Trabajo en áreas seguras | A9.1.5 | |
| Áreas de carga, despacho y acceso público | A9.1.6 | |
| Ubicación y protección de los equipos | A9.2.1 Hasta A9.2.7 | Los equipos deben estar protegidos y recibir mantenimiento |
| GESTIÓN DE COMUNICACIONES Y OPERACIONES | | |
| Documentación de los procedimientos de operación | A10.1.1 | Los procedimientos de operación se deben documentar y estar disponibles para su uso |
| Gestión del cambio | A10.1.2 | Controlar los cambios en los servicios |
| Distribución de funciones | A10.1.3 | Distribución de funciones |
| Separación de las instalaciones de desarrollo, ensayo y operación | A10.1.4 | Separa las instalaciones para reducir los riesgos de cambios no autorizados |
| Gestión de la prestación del servicio por terceras partes | A10.2.1 Hasta A10.2.3 | Garantizar que los controles, las definiciones del servicio y los niveles de prestación sean implementados, mantenidos y operados por las terceras partes. |
| Planificación y aceptación del sistema | A10.3.1 y A10.3.2 | Hacer seguimiento y adaptación para sistemas de información nuevos |
| Protección contra códigos malicioso y móviles | A10.4.1 y A10.4.2 | Controles de detección, prevención y recuperación. |

| | | |
|---|---|---|
| Respaldo | A10.5 | Hacer copias de respaldo |
| Gestión de la seguridad de las redes | A10.6.1 y A10.6.2 | Mantener las redes y controlar para proteger de amenazas |
| Manejo de los medios | A10.7.1 Hasta A10.7.4 | Establecer procedimientos para manejar los medios removibles |
| Intercambio de la información | A10.8.1 Hasta A10.8.5 | Establecer políticas, procedimientos y controles de intercambio para proteger la información |
| Servicios de comercio electrónico | A10.9 y A10.10 | La información involucrada en el comercio electrónico debe estar protegida contra actividades fraudulentas, disputas o modificaciones no autorizadas. |
| **CONTROL DE ACCESO** | | |
| Requisito del negocio para el control de acceso | A.11.1 | Establecer, documentar y revisar la política de control de acceso. |
| Gestión del acceso de usuarios | A11.2.1 Hasta A11.2.4 | Asegurar el acceso a usuarios autorizados y evitar el acceso de usuarios no autorizados a los sistemas de información |
| Responsabilidad de los usuarios | A11.3.1 Hasta A11.3.3 | Evitar el acceso de usuarios no autorizados, el robo o la puesta en peligro de la información |
| Control de acceso a las redes | A11.4.1 Hasta A11.4.7 | Evitar el acceso no autorizado a los servicios de la red |
| Control de acceso al sistema operativo | A11.5.1 Hasta A11.5.6 | Evitar el acceso al sistema operativo |
| Control de acceso a las aplicaciones y a la información | A11.6.1 y A11.6.2 | Evitar el acceso no autorizado a la información contenida en los sistemas de información |
| Computación móvil y trabajo remoto | A11.7.1 y A11.7.2 | Garantizar la seguridad de la información cuando se utilizan dispositivos de computación móviles y de trabajo remoto |
| **ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN** | | |
| Análisis y especificación de los requisitos de seguridad | A12.1.1 | Especificar en los requisitos para los controles de seguridad las declaraciones sobre los nuevos sistemas de información o mejoras. |
| Procesamiento correcto en las aplicaciones | A12.2.2 Hasta A12.2.4 | Evitar errores, pérdidas, modificaciones o uso inadecuado de la información en las aplicaciones. |
| Controles criptográficos | A12.3.3 y A12.3.2 | Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información |

| | | |
|---|---|---|
| Seguridad de los archivos del sistema | A12.4.1 Hasta A12.4.3 | Garantizar la seguridad de los archivos controlando la instalación de software |
| Seguridad en los procesos de desarrollo y soporte | A12.5.1 Hasta A12.5.5 | Mantener la seguridad del software y de la información del sistema de aplicaciones |
| Gestión de la vulnerabilidad técnica | A12.6.1 | Reducir los riesgos resultantes de la explotación de las vulnerabilidades técnicas publicadas |
| **GESTION DE LOS INCIDENTES DE LA SEGURIDAD DE LA INFORMACIÓN** | | |
| Reporte sobre los eventos y las debilidades de la seguridad de la información | A13.1.1 y A13.1.2 | Los eventos de seguridad de la información se deben informar y todos deben reportar las debilidades observadas |
| Gestión de los incidentes y las mejoras en la seguridad de la información | A13.2.1 Hasta A13.2.3 | Asegurar que se aplica un enfoque para la gestión de los incidentes |
| **GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO** | | |
| Aspectos de seguridad de la información, de la gestión de la continuidad del negocio | A14.1.1 Hasta A14.1.5 | Contrarrestar las interrupciones en las actividades del negocio y proteger sus procesos críticos |
| **CUMPLIMIENTO** | | |
| Cumplimiento de los requisitos legales | A15.1.1 Hasta A15.1.6 | Evitar el incumplimiento de cualquier ley, obligaciones y cualquier requisito de seguridad |
| Cumplimiento de las políticas y normas de seguridad y cumplimiento técnico | A15.2.1 y A15.2.1 | Asegurar que los sistemas cumplan las normas y políticas de seguridad |
| Consideraciones de la auditoría de los sistemas de información | A15.2.1 y A15.2.1 | Maximizar la eficacia de los procesos de auditoría y minimizar la interferencia |

**Anexo 10**
Acta de validación

Universidad de Valparaíso CHILE
Trabajo de Título
Ingeniería Civil Biomédica

**Verificación de entrega de Información y Validación de Recomendaciones en la Metodología para la Implementación de un SGSI**

Yo Karla Ortiz Nuñez con cargo Enfermera Supervisora en el servicio clínico de Urgencia adulto, del Hospital Carlos Van Buren, certifico que se brindó información relevante para esta implementación y valido las recomendaciones realizadas por el alumno en relación a su trabajo de título denominado "Diseño de una metodología para la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en ISO/IEC 27001 en la Unidad de Urgencia del Hospital Carlos Van Buren (HCVB)"

10/06/15
Firma del Profesional

Valparaíso, Junio 2015

**Anexo 11**
Minutas de reuniones