Desarrollo de un modelo de un SGSI (Sistema de Gestión de la Seguridad de la Información) para el Hospital Clínico de la Universidad de Valparaíso.

Problema

El uso de las Tecnologías de la Información dentro de las organizaciones del sector de salud ha ido aumentando rápidamente, permitiendo optimizar y mejorar la prestación de sus servicios, convirtiéndose en una herramienta valiosa dentro del proceso de atención médica. En la actualidad uno de los activos más importantes que poseen las organizaciones es la información; sin embargo, en muchas ocasiones no cuentan con políticas adecuadas para protegerla, generando vulnerabilidades que pueden ser aprovechadas por las amenazas existentes en el entorno y por ende afectar a la integridad, confidencialidad y disponibilidad de los activos de información.

El Hospital Clínico de la UV, es una institución orientada a brindar servicios ambulatorios y hospitalarios con altos estándares de calidad, con profesionales médicos de excelencia en todas las especialidades, además cuenta con una infraestructura física moderna y con lo último en tecnología.

Por la falta de conocimiento de las normativas de seguridad de la información, esta expuesto a vulnerabilidades y riesgos en lo concerniente a la seguridad informática. Debido al alto grado de importancia que tiene esto último, el significativo impacto en la continuidad operacional, la posible fuga de información sensible y las sanciones económicas y legales a la que puede verse expuesto el hospital, es menester que este último cuente con un modelo de Gestión de Seguridad de la Información que oriente a las personas responsables o técnicos afines sobre las mejores prácticas o mecanismos tecnológicos para salvaguardar la información contra amenazas y ataques tanto internos como externos.

OBJETIVOS

OBJETIVO GENERAL

Proponer un Modelo de Gestión de Seguridad de la Información Hospital Clínico UV; que permita garantizar la integridad, disponibilidad y confidencialidad de la información, mediante el uso de la norma ISO 27799:2008, ISO/IEC 27005:2008 e ISO/IEC 27002:2013.

OBJETIVOS ESPECÍFICOS

Realizar una revisión bibliográfica de las normativas sobre confidencialidad de la información para el sector salud y de la metodología de las normas ISO 27001:2013; que permita establecer lineamientos adecuados para el desarrollo del modelo de Sistema de Gestión de Seguridad de la Información aplicable al sector de salud.

Realizar el levantamiento de información de la situación actual del Hospital Clínico UV, para la identificación de los dispositivos lógicos y físicos que comprometan la seguridad de la información.

Plantear un modelo de Sistema de Gestión de Seguridad de la Información (SGSI) para el Hospital Clínico UV; seleccionando los controles de seguridad de información más importantes que garanticen la confidencialidad, integridad y disponibilidad de la información.

ALCANCE

Proponer un modelo de Sistema de Gestión de Seguridad de la Información para el Hospital Clínico UV que permita garantizar la integridad, disponibilidad y confidencialidad de la información, basado en la norma ISO 27001:2013

Antecedentes

En Valparaíso, el Hospital Clínico de la UV presta sus servicios desde el año 2000, enfocándose en brindar un servicio de calidad y mejores prácticas al servicio del paciente, con asesoramiento y programas de acompañamiento para este último. Otorgando la mejor atención con profesionales altamente calificados y equipamiento tecnológico de última generación para cubrir todas las necesidades del usuario.

El hospital cuenta con una unidad de emergencia que funciona las 24 horas al día, además de un área de hospitalización, cirugía, neonatología, laboratorio clínico, imageonología y apoyo terapéutico.

Misión

Brindar un servicio de salud de calidad, orientado siempre a la satisfacción de las necesidades de nuestros pacientes, con un completo equipo profesional y humano orientado a la responsabilidad social.

Visión

Ser sinónimo de excelencia en servicios de salud a nivel nacional, mejorando la calidad de vida de los pacientes y su entorno familiar.

OBJETIVOS INSTITUCIONALES

Objetivo general

- Brindar al público en general servicios de salud con calidad y calidez apuntando siempre a la mejora continua y a la satisfacción del paciente y su entorno familiar.

Objetivos específicos

- Darse a conocer a través de la buena atención prestada a sus pacientes y su excelente equipo médico.
- Ampliar la infraestructura clínica para poder ofrecer mejores y más servicios médicos a la ciudadanía.
- Garantizar la seguridad ocupacional de todos los usuarios de el hospital tanto internos como externos fomentando un ambiente de trabajo seguro y saludable.

UNIDAD DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES

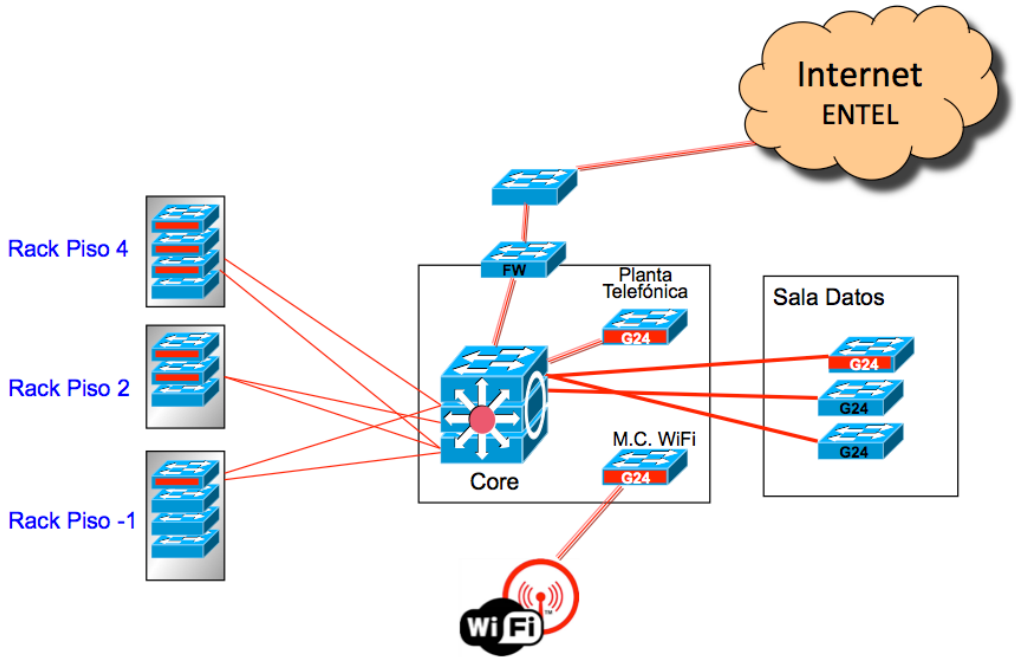
La Unidad de Gestión de Tecnologías de la Información y Comunicaciones (TIC) del Hospital Clínico UV, se encuentra conformado 5 profesionales del área de Tecnología de la información y una secretaria. Dentro del organigrama la unidad de TIC se encuentra como un departamento y es considerado al mismo nivel que Administración y RRHH; entre las principales funciones que tiene son:

- Gestión de niveles de Servicio
- Ingeniería de Sistema
- Administración Red Lógica
- Monitoreo de Servicios
- Comunicaciones (VPN, Audio, Video, Telefonía IP)
- Soporte de servicios
- Respaldo
- Administración Sala Servidores
- Administración de BD
- Desarrollo de aplicaciones
- Prueba de programas
- Confección de manuales
- Soporte de aplicaciones
- Mejoramiento de aplicaciones
- Atención Usuarios
- Administración Red Física
- Mantención equipos
- Instalación y configuración de software
- Evaluación Técnica (HW y SW)
- Mantenimiento de la PABX IP.
- Inventario de los equipos tecnológicos computacionales y comunicacionales.

Infraestructura

Red de Datos

Actualmente la red de datos del Hospital Clínico de la UV es controlada por el proveedor de servicios de comunicaciones ENTEL, con una velocidad de 1 Gbps. Se cuenta con un router Cisco Asa 550 proporcionado por el proveedor; además, se cuenta con una red WIFI soportada por Cisco AP y concentradores Cisco 2950



Equipos

A nivel de equipos en el Hospital Clínico de la UV, se cuenta con el siguiente número de estaciones de trabajo:

Área	**Estaciones de trabajo**
Gerencia	1
Dirección médica	6
Dirección administrativa	1
Dirección contable – financiera	2

Además, se cuenta con dispositivos de telefonía, impresoras y servidores que se listan en la siguiente tabla:

Equipo	**Descripción**	**Cantidad**
Central telefónica Analógica	Alcatel Lucent Opentouch	1
Router Inalámbrico	Cisco	1
Impresora – Escáner	Samsung ML-1665; Epson EcoTank L220	3
Portátiles	Dell	4
Computadoras de escritorio	All in One HP, core i7 1Tb + 8gb RAM+ Sistema Operativo Windows 10	5
Servidor de página web	Servidor HP Elite 8300, Procesador Intel Core i7-3770 (3.5 GHz) 7º Generación.	1
Servidor AD	Servidor HP Elite 8300, Procesador Intel Core i7-3770 (3.5 GHz) 7º Generación.	1
Servidor Correo electrónico Linux Redhat	Servidor HP Elite 8300, Procesador Intel Core i7-3770 (3.5 GHz) 7º Generación.	1
Servidor Web Linux Redhat	Servidor HP Elite 8300, Procesador Intel Core i7-3770 (3.5 GHz) 7º Generación.	1
Servidor de Aplicaciones	Servidor HP Elite 8300, Procesador Intel Core i7-3770 (3.5 GHz) 7º Generación.	1
Endoscopio	Olympus CV140	1

Ecógrafo	Hitachi Medical Systems: F37	1
Monitor de signos vitales	Storz Electronic Laparoflator 26012	1
Impresora de placas radiográficas	CARESTREAM DRYVIEW 5950	1
Datafono	Verifone Vx510	1
Reloj Biométrico	BIOTRACK BT-BTIME	1
Grabador de vídeo digital	DVR ST-4KITAHD7016A-1M	1

Aplicaciones

El Hospital Clínico de la UV, utiliza diferentes aplicaciones para la gestión de sus operaciones. En la siguiente tabla se listan las diferentes aplicaciones que permiten prestar los servicios médicos:

Aplicación	**Tipo de aplicación**	**Comentarios**
Office	Paquete Office Herramienta de ofimática	
Microsoft Windows	SO	
Microsoft Windows server	SO	
Kaspersky Lab	Antivirus	
SysLabs	SW para laboratorios clínicos	
Aplica	SW contable, financiero y administrativo	ERP
Ginkgo CADx	Herramienta para análisis de datos de imagen médica	Framework de visualización y gestión de imagen
Amide 3D	Herramienta para análisis de datos de imagen médica	Herramienta de análisis de datos de imagen médica
Apache	Servidor web	Portal corporativo

ANÁLISIS FODA DE LA UNIDAD DE GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES

Para diagnosticar el estado del Departamento de Tecnologías de la Información y Comunicaciones (TIC) del Hospital Clínico UV, se realiza una discusión y debate en base a algunas preguntas, esto permite identificar las diferentes Fortalezas, Oportunidades, Debilidades y Amenazas con respecto a la implementación del SGSI.

Algunas de las preguntas que se analizan en la discusión son las siguientes:

1. ¿Para la implementación de proyectos informáticos dentro del Hospital Clínico UV existe apoyo de la alta dirección?

2. A su consideración, ¿existe trabajo en equipo entre las diferentes áreas del Hospital para la realización de proyectos?

3. Por parte del personal de la Unidad de TIC, ¿existe disponibilidad para auto capacitación (aprender/aprender)?

4. A su consideración, ¿el soporte técnico y tiempo de respuesta por la Unidad de TIC es satisfactorio?

5. ¿Existe un uso correcto de los recursos informáticos por parte del personal del Hospital?

6. Considera usted que obtener una certificación ISO 27001 para Hospital Clínico UV, ¿mejoraría la confidencialidad, integridad y disponibilidad de la información de los pacientes y el personal?

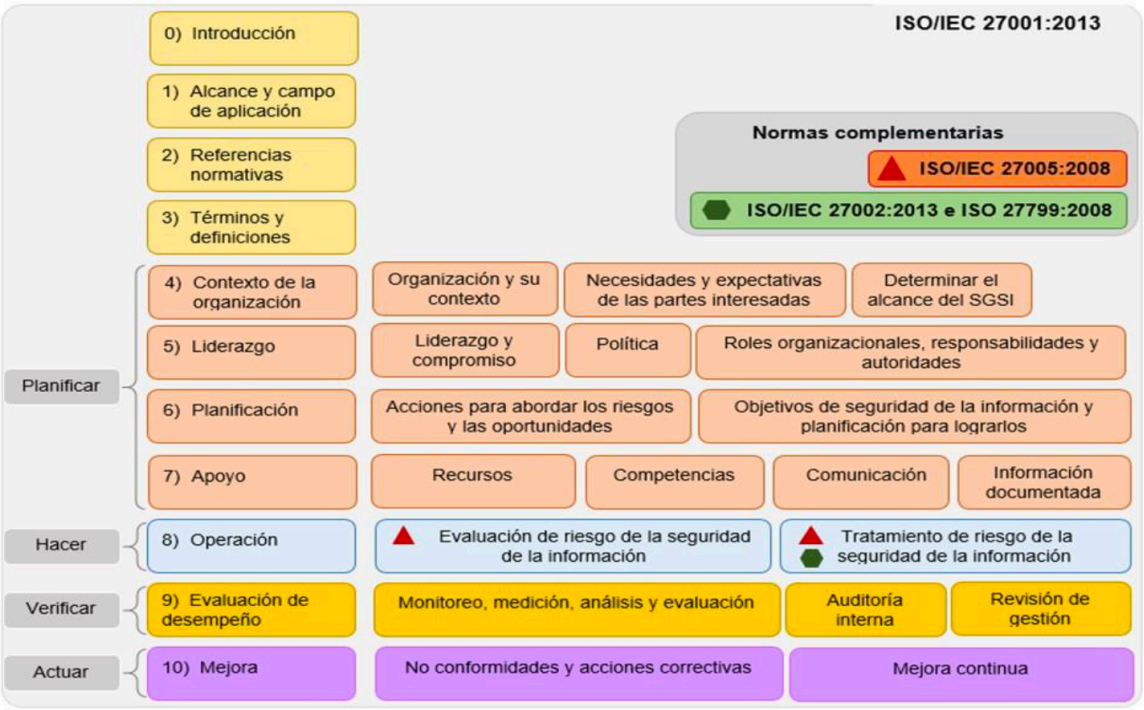
7. ¿Existe documentación sobre solución a incidentes relacionados con seguridad de la información del Hospital Clínico UV?

8. ¿Considera usted importante la existencia de políticas y procedimientos sobre seguridad de la información para resguardar la información del Hospital?

9. ¿Tiene conocimiento sobre el impacto en las instituciones del sector salud al sufrir ataques o infiltraciones de seguridad de la información?

MODELO DE GESTIÓN DEL SISTEMA DE SEGURIDAD DE LA INFORMACIÓN PARA EL HOSPITAL CLINICO UV

El uso de las normas ISO/IEC 27001:2013, ISO/IEC 27005:2008, ISO/IEC 27002:2013 e ISO 27799:2008; permiten crear un modelo de un Sistema de Gestión de Seguridad de la Información para el Hospital Clínico UV. Dicho modelo abarca procesos y actividades dirigidas a salvaguardar la información de los pacientes de el hospital y sus trabajadores ante cualquier amenaza que se presente, preservando su confidencialidad, integridad y disponibilidad de la información.



INSTRUMENTOS DE RECOLECCION DE INFORMACION

Para el desarrollo del modelo de Sistema de Gestión de Seguridad de la Información, se establece que los mecanismos e instrumentos para la recolección de la información del Hospital Clínico UV son:

- Focus group.
- Observaciones.
- Entrevistas con funcionarios y sobre todo con el personal de Tecnología de la información y comunicaciones (TIC).

También, se utilizará las diferentes fuentes de información, tales como normas, marcos de referencia, tesis, libros, textos, revistas, entre otros.

ANÁLISIS DEL CONTEXTO DE LA ORGANIZACIÓN

En la presente fase se realiza un análisis y descripción de la situación actual del Hospital Clínico UV, tratando de comprender su perspectiva, procesos internos, dependencias, requisitos tanto internos como externos y las motivaciones para la implantación de un SGSI.

DETERMINAR EL ALCANCE DEL SGSI

Se determinará qué elementos formarán parte del Sistema de Gestión de Seguridad de la Información, generalmente identificando los procesos de negocio sobre los que se aplicará el sistema; para determinar el alcance del SGSI del Hospital Clínico UV debe considerar por ejemplo lo siguiente:

- “Los asuntos externos e internos de la organización que son importantes para su objetivo y que afecte su capacidad para lograr los resultados esperados de su Sistema de Gestión de la Seguridad de la Información” (ISO/27001).

- "Comprender las necesidades y expectativas de las partes interesadas, tomando en consideración que los requisitos de las partes interesadas pueden incluir requerimientos legales y regulatorios, así como obligaciones contractuales” (ISO/27001).

- Interferencias y dependencias entre las actividades realizadas por la organización del sector salud y aquellas realizadas por otras organizaciones adyacentes o proveedores.

- “El alcance estará disponible como información documentada” (ISO/27001), por lo cual debe existir un documento que servirá como evidencia donde se especificará el alcance del Sistema de Gestión de Seguridad de la Información y que contenga la aprobación y respaldo de Gerencia del Hospital Clínico UV.

ÁREAS DEL HOSPITAL CLÍNICO UV

Gerencia:

- Representar a la institución legalmente.
- Autorizar el ingreso del personal necesario.
- Establecer objetivos a corto y largo plazo.
- Autorizar la compra de insumos para la institución.
- Tomar decisiones respecto a sanciones al personal por incumplimiento de normas.
- Desarrollar estrategias para mantener la buena imagen de el hospital.
- Identificar, analizar y resolver los problemas que se presenten en la institución.
- Tomar decisiones en favor de la institución.

Dirección Administrativa

Recursos Humanos:

- Planear, organizar, dirigir y controlar los programas, estrategias y acciones a desarrollar para el óptimo aprovechamiento de las habilidades del personal.
- Proponer medidas técnico-administrativas para el mejor funcionamiento de los recursos existentes.
- Supervisa y distribuye las actividades del personal.
- Velar por el cumplimiento de las normas y procedimientos de higiene y seguridad laboral, establecidos por la organización.
- Elaborar y controlar el proceso de reclutamiento, selección, ingreso e inducción del personal.
- Proyectar y coordinar programas de capacitación y entrenamiento para los empleados.
- Coordinar y controlar el proceso de desvinculación del personal.

Servicios generales:

- Dar cumplimiento a las políticas y normas de seguridad e higiene emitidas.
- Mantenimiento de equipos médicos.
- Limpieza y seguridad de las instalaciones.
- Mantener el orden e higiene de los materiales o enseres utilizados.
- Informar del deterioro de los equipos médicos e instalaciones de el hospital.
- Brindar apoyo en las tareas administrativas de la Institución.
- Tratamiento de reciclaje de desechos infecciosos.

- Suministrar, controlar y conservar en buen estado físico y logístico interno de la Institución.

Dirección Financiera.

Contabilidad

- Realizar un listado de los insumos médicos y administrativos faltantes.
- Realizar las cotizaciones.
- Pago a proveedores.
- Facturación de servicios médicos.
- Control de inventario (Laboratorio, Farmacia, Emergencia, Consultorios).
- Preparar los registros para realizar las declaraciones.
- Recibir, examinar, clasificar y codificar los documentos contables.
- Archivar documentos contables.
- Mantener actualizados los registros contables.

Finanzas

- Registro de ingresos, gastos y control de inventarios.
- Pago a empleados de la institución.
- Realizar el cierre del ejercicio al finalizar el periodo.
- Verificar y consolidar saldos contables.
- Asesorar a gerencia en la toma de decisiones financieras.
- Llevar un adecuado control de los activos fijos de el hospital y su respectiva depreciación.
- Elaborar de Conciliaciones Bancarias.

Consulta médica:

- Brindar un servicio ambulatorio para pacientes con una cita asignada de los diferentes tipos de diagnósticos que posee el hospital: Medicina General, Otorrinolaringología, Ginecología y Pediatría

Servicios Médicos:

- Brindar a los pacientes un eficiente servicio médico de las diferentes atenciones que presta el hospital:
- Hospitalización
- Quirófano
- Emergencia
- Farmacia
- Servicios de diagnóstico (Imagenología)

Departamento de TI

- Gestión de niveles de Servicio
- Ingeniería de Sistema
- Administración Red Lógica
- Monitoreo de Servicios
- Comunicaciones (VPN, Audio, Video, Telefonía IP)
- Soporte de servicios
- Respaldo
- Administración Sala Servidores
- Administración de BD
- Desarrollo de aplicaciones
- Prueba de programas
- Confección de manuales
- Soporte de aplicaciones
- Mejoramiento de aplicaciones
- Atención y soporte usuarios
- Administración Red Física
- Mantención equipos
- Instalación y configuración de software
- Evaluación Técnica (hw y sw)
- Mantenimiento de la PABX IP.
- Inventario de los equipos tecnológicos computacionales y comunicacionales.

DEFINICIÓN DE LA POLÍTICA Y OBJETIVOS DE LA SEGURIDAD DE LA INFORMACIÓN

La definición de los objetivos y políticas para el proceso de implementación del Sistema de Gestión de Seguridad de la Información permitirá establecer un sentido de dirección general para el Hospital Clínico UV. Por medio de esta fase se logrará establecer los objetivos de el hospital en el ámbito de la seguridad de la información y los mecanismos para alcanzar dichos objetivos.

Al definir la política del Sistema de Gestión de Seguridad de la Información, se deberían tomar en cuenta los siguientes aspectos:

- “Establecer los objetivos del SGSI en base a los requerimientos organizacionales y las prioridades de seguridad de la información de la organización” (ISO/27001).
- “Establecer el enfoque general y la guía de acción para lograr los objetivos del SGSI” (ISO/27001).

- Considerar los requerimientos del Hospital Clínico UV, legales o regulatorios y las obligaciones contractuales relacionadas con la seguridad de la información.
- Establecer el contexto de la gestión del riesgo dentro de el hospital.
- “Determinar los criterios de evaluación de los riesgos y definir una estructura de evaluación del riesgo” (ISO/27001).
- Obtener la aprobación de la Gerencia del Hospital Clínico UV.
- El entregable de la presente fase es un documento que describe los objetivos y política del Sistema de Gestión de Seguridad de la Información y de igual manera aprobada por la Gerencia del Hospital Clínico UV.

DEFINIR LOS RECURSOS, COMPETENCIAS, COMUNICACIÓN Y DOCUMENTACIÓN

El Hospital Clínico UV deberá determinar y proporcionar los recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continua del Sistema de Gestión de la Seguridad de la Información. De igual manera, deberá establecer procesos internos para la elección de personal médico y administrativo que permita “asegurar que estas personas sean competentes basados en una educación, capacitación o experiencia adecuada” (ISO/27001).
Los responsables de la implementación deberán definir los procedimientos de comunicación interna y externa pertinentes al Sistema de Gestión de Seguridad de la Información; así como también la creación, actualización y control de la información documentada.

ESTABLECER ACCIONES PARA ABORDAR LOS RIESGOS Y LAS OPORTUNIDADES

En la presente fase se debe determinar los riesgos y oportunidades que necesitan ser cubiertos para asegurar que el Sistema de Gestión de la Seguridad de la Información pueda lograr el resultado esperado. Para lo cual se debe realizar actividades que tienen relación con “la evaluación y el tratamiento del riesgo de la seguridad de la información” (ISO/27001).

En lo que se refiere a la evaluación del riesgo, la norma ISO/IEC 27001:2013 establece que la “organización debe definir y aplicar un proceso de evaluación de riesgo de la seguridad de la información” que establezca y mantenga los criterios de riesgo de la seguridad de la información, así como también asegurar que las evaluaciones de riesgo de la seguridad de la información, producen resultados consistentes, válidos y comparables, una y otra vez; “el entregable de esta fase es la información documentada acerca del proceso de evaluación de riesgo de la seguridad de la información”. Dicha documentación deberá contener las siguientes actividades:

Inventario de activos de información

Se deben identificar los activos que dan soporte a los procesos de negocio del Hospital Clínico UV en el alcance del Sistema de Gestión de la Seguridad de la Información y cuantificar su valor en términos de confidencialidad, integridad y disponibilidad. “Tomando en consideración que se define como activo todo aquello que tiene valor para la organización y que por lo tanto debe ser protegido” (ISO/27005).
La identificación de los activos se debería llevar a cabo con un nivel adecuado de detalle, que proporcione información suficiente para la valoración del riesgo, de igual manera se debería identificar al propietario de cada activo, para asignarle la responsabilidad y rendición de cuentas sobre éste. “El propietario del activo puede no tener derechos de propiedad sobre este último, pero tiene la responsabilidad de su producción, desarrollo, mantenimiento, uso y seguridad, según corresponda” (ISO/27005). El entregable de esta actividad es un documento con el inventario de los activos de información de los principales procesos de la organización dentro del alcance del Sistema de Gestión de la Seguridad de la Información.
Para la identificación de los activos, se debe tomar en cuenta los tipos de activos que existen en el Hospital Clínico UV tanto los activos primarios y de soporte. A continuación, se muestra una clasificación de estos.

- Los activos primarios:
    - Servicios médicos y procesos del negocio
    - Información / Datos
- Los activos de soporte de todos los tipos:
    - Hardware
    - Software
    - Redes de comunicaciones
    - Personas
    - Sitio / Instalaciones
    - Estructura de la organización

Realizar una valoración de los activos

La valoración de los activos sirve para determinar el impacto que el deterioro, falla o pérdida de estos tiene sobre la confidencialidad, disponibilidad e integridad de la información del Hospital Clínico UV. Para ello se deberá aplicar una escala de valor a los activos y de esa manera poder relacionarlos apropiadamente; “El propietario del activo con frecuencia es la persona más idónea para determinar el valor que el activo tiene para la organización” (ISO/27005).
Nota: Ver planilla Excel de activos

Identificar amenazas

En esta etapa se deben identificar las amenazas asociadas a cada uno de los procesos de negocio del Hospital Clínico UV, activos de información, probabilidad de ocurrencia y vulnerabilidades ante dichas amenazas, lo que permitirá estimar el

impacto de la materialización de cualquier falla de seguridad de la información dentro de el hospital.

En la planilla Excel de activos, pestaña “Amenazas”, se describe los diferentes tipos y ejemplos de amenazas comunes aplicables al modelo de Sistema de Gestión de Seguridad de la Información, así como también su código para identificarlas posteriormente.

Valorización de amenazas

Valor	Categoría	Descripción
5	Catastrofico	Riesgo cuya materialización puede generar pérdidas financieras ($) que tendrán un impacto catastrófico en la organización y/o comprometen totalmente la imagen de la organización.
4	Mayores	Riesgo cuya materialización puede generar pérdidas financieras ($) que tendrán un impacto importante en la organización y/o comprometen fuertemente la imagen de la organización.
3	Moderadas	Riesgo cuya materialización puede generar pérdidas financieras ($) que tendrán un impacto moderado en ela organización y/o comprometen moderadamente la imagen de la organización
2	Menores	Riesgo cuya materialización puede generar pérdidas financieras ($) que tendrán un impacto menor en la organización y/o comprometen de forma menor la imagen de la organización
1	Insignificantes	Riesgo cuya materialización no genera pérdidas financieras ($) ni compromete de ninguna forma la imagen de la organización.

Identificación de las vulnerabilidades

Se procede a identificar las vulnerabilidades de los activos por las distintas fuentes que las pueden originar, utilizando como guía algunos de los dominios de la norma ISO 27002 y una lista de vulnerabilidades proporcionadas por la Norma ISO/IEC 27005 que se detalla en la planilla Excel asociada a este ejemplo.

Evaluación de la probabilidad de incidentes

Después de identificar y valorizar las amenazas e incidentes es necesario evaluar la probabilidad de cada escenario y el impacto de que ocurra. Se deberán tomar en consideración la frecuencia con la que ocurren las amenazas y la facilidad con que las vulnerabilidades pueden ser explotadas.
La valoración cuantitativa del 1 al 5 permitirá indicar que tan probable es que una amenaza se concrete con una o varias de las vulnerabilidades encontradas.

Valor	Categoría	Descripción
5	Casi Certeza	Riesgo cuya probabilidad de ocurrencia es muy alta, es decir, se tiene un alto grado de seguridad que éste se presente en el año en curso. (90% a 100%).
4	Probable	Riesgo cuya probabilidad de ocurrencia es alta, es decir, se tiene entre 66% a 89% de seguridad que éste se presente en el año en curso.
3	Moderado	Riesgo cuya probabilidad de ocurrencia es media, es decir, se tiene entre 31% a 65% de seguridad que éste se presente en el año en curso.
2	Improbable	Riesgo cuya probabilidad de ocurrencia es baja, es decir, se tiene entre 11% a 30% de seguridad que éste se presente en el año en curso.
1	Muy Improbable	Riesgo cuya probabilidad de ocurrencia es muy baja, es decir, se tiene entre 1% a 10% de seguridad que éste se presente en el año en curso.

Establecer un nivel de estimación del riesgo

Para cada activo de información del Hospital Clínico UV se calcula el riesgo, “que será una combinación de la probabilidad de un escenario de incidente y sus consecuencias” (ISO 27005).
La calificación del riesgo se realizará haciendo una multiplicación entre la probabilidad del incidente tratado (pestaña vulnerabilidades planilla Excel) y el impacto en caso de materializarse (pestaña amenazas planilla Excel), a continuación, se muestra el nivel de estimación de riesgo a utilizar:

ID	Nivel de Probabilidad	Nivel de Impacto	Valor	Severidad
55	5	5	25	Extremo
54	5	4	20	Extremo
53	5	3	15	Extremo
52	5	2	10	Alto
51	5	1	5	Alto
45	4	5	20	Extremo
44	4	4	16	Extremo
43	4	3	12	Alto
42	4	2	8	Alto
41	4	1	4	Moderado
35	3	5	15	Extremo
34	3	4	12	Extremo
33	3	3	9	Alto
32	3	2	6	Moderado
31	3	1	3	Bajo
25	2	5	10	Extremo
24	2	4	8	Alto
23	2	3	6	Moderado
22	2	2	4	Bajo
21	2	1	2	Bajo
15	1	5	5	Alto
14	1	4	4	Alto
13	1	3	3	Moderado
12	1	2	2	Bajo
11	1	1	1	Bajo

Realizar una identificación de los controles existentes

Posterior al proceso de identificar y valorizar las amenazas, se debe realizar la identificación de los controles existentes en la organización que permitan brindar de alguna manera confidencialidad, integridad y disponibilidad a la información para evitar trabajo o costos innecesarios en la implementación de un Sistema de Gestión de Seguridad de la Información, por ejemplo, en la duplicación de los controles.
Para la identificación de los controles existentes o planificados, las siguientes actividades pueden ser útiles:

- Revisión de los documentos que contengan información sobre los controles.
- Verificación con las personas responsables de la seguridad de la información.

REALIZAR EL TRATAMIENTO DE RIESGO DE LA SEGURIDAD DE LA INFORMACIÓN

Luego de completar la evaluación de riesgos, el Hospital Clínico UV “deberá definir y aplicar un proceso de tratamiento de riesgo de la seguridad de la información”. Dentro de las estrategias de llevar el tratamiento del riesgo están:

- Eliminación o evitación: Consiste en eliminar la amenaza eliminando la causa que puede provocarla.
- Transferencia: Esta posibilidad busca trasladar las consecuencias de un riesgo a una tercera parte junto con la responsabilidad de la respuesta.
- Mitigación: Busca reducir la probabilidad o las consecuencias de sucesos adversos a un límite aceptable antes del momento de activación. Es importante que los costos de mitigación sean inferiores a la probabilidad del riesgo y sus consecuencias. Para llevar a cabo la mitigación de riesgos es necesario: seleccionar, implantar, y verificar los controles y establecer indicadores. La selección de los controles se podrá realizar utilizando como referencia la Norma ISO 27002:2013
- Aceptación: Se utiliza cuando se decide no actuar contra el riesgo antes de su activación. La aceptación puede ser activa, cuando se incluye un plan de contingencia que será ejecutado si el riesgo se presenta, o pasiva, cuando no requiere de ninguna acción, únicamente se realiza la gestión del riesgo.

Para el tratamiento del riesgo se debe “determinar todos los controles que son necesarios para implementar las opciones de tratamiento de riesgo de la seguridad de la información escogida” (ISO/27001). Los controles seleccionados permitirán garantizar que cada aspecto del activo, que se valoró con cierto riesgo, quede cubierto y auditable. Estos controles se toman de la ISO 27002:2013; sin embargo, la norma ISO 27001:2013 aclara que “los controles propuestos no son exclusivos y podrían adoptarse otros tipos de controles”.
Además, se debe considerar que, en el proceso de implementación de un Sistema de Gestión de Seguridad de la Información, siempre existen riesgos residuales, los cuales deben ser evaluados y categorizados como aceptables o no aceptables. La aceptación de dichos riesgos residuales debe estar realizado por un comité de seguridad de la información el cual decidirá que controles deben ser implementados en el futuro. El resultado de esta fase es el documento denominado declaración de aplicabilidad el cual detallará los proyectos propuestos a implementar, dicho documento debe tener la aceptación y compromiso de la Gerencia y del encargado de la Unidad de TICs.

El objetivo del Plan de Tratamiento del Riesgo es definir cuál es la estrategia de tratamiento de riesgo, selección de controles, herramientas, información documentada, responsable de implementar los controles, lo que permitirá garantizar:

- Un funcionamiento efectivo y eficiente de la organización.
- Controles internos efectivos.
- Conformidad con las leyes y reglamentos vigentes.

DEFINIR ACTIVIDADES DE CONTROL

La definición de actividades surge a partir del análisis de riesgos y el resumen de los controles a implementar, priorizando la implementación de los que aporten mejoras en la seguridad en el menor plazo. Cabe indicar que estos deben estar dirigidos a mitigar amenazas mencionadas en el Anexo C de la ISO 27005.

Implantación de políticas de seguridad de la información

Ejemplos de dominios a cubrir: Políticas de seguridad, control de acceso, seguridad de las operaciones y seguridad de las comunicaciones.

Objetivo: Implantar el conjunto de políticas de seguridad de la información, que dirija y entregue un marco normativo y de comportamiento del Hospital Clínico UV en su conjunto, para el cumplimiento del Sistema de Gestión de la Seguridad de la Información.

Descripción: Las políticas de seguridad de la información contienen las directrices y lineamientos que regirán la seguridad de la información en el Hospital y las responsabilidades y obligaciones de todos los colaboradores y terceros que tengan acceso a la información del Hospital Clínico UV.