**Tarea Gobernanza de Datos**

Integrantes:

Martín Hernández - .  
Sofía López - .  
Benjamín Zárate -20.882.488-0 - [benjamin.zarate@alumnos.uv.cl](mailto:benjamin.zarate@alumnos.uv.cl)

El **Sistema de Gestión de Seguridad de la Información (SGSI)** es un componente esencial para garantizar la protección de los activos de información en cualquier organización, especialmente en instituciones de salud como el **Hospital Clínico de la Universidad de Valparaíso (UV)**. En un entorno hospitalario, la seguridad de la información es fundamental no solo para proteger datos sensibles de pacientes y personal, sino también para asegurar la continuidad de los servicios médicos y la confianza de los usuarios.

Este informe tiene como propósito principal desarrollar, implementar y mantener un SGSI eficaz que cumpla con las normativas internacionales ISO 27001, ISO 27002, ISO 27005 e ISO 27799, las cuales proporcionan directrices y mejores prácticas para la gestión de la seguridad de la información. A través de un enfoque estructurado, el hospital busca cumplir con los requisitos legales y regulatorios, proteger la confidencialidad, integridad y disponibilidad de la información, y garantizar que los procesos de gestión de la información sean robustos frente a riesgos de seguridad.

El presente informe se organiza en una serie de pasos que abarcan todos los aspectos necesarios para la implementación de un SGSI, comenzando por la definición del **alcance**, el **análisis del contexto organizacional**, y la **elaboración de la política de seguridad de la información**, seguida de la **identificación de activos**, **amenazas y riesgos**, así como la **creación de un plan de tratamiento** y un **conjunto de controles**. Además, se contemplan las actividades de comunicación, capacitación y la revisión continua de la seguridad del sistema, asegurando la mejora continua del **SGSI**.

A través de la implementación efectiva de estas estrategias, el **Hospital Clínico UV** podrá no solo cumplir con las normativas vigentes, sino también proporcionar un entorno seguro que proteja la información de pacientes y empleados, garantizando una gestión eficiente de los recursos informáticos en todo el hospital.

Este documento constituye un paso crucial en la formalización de un sistema de gestión de seguridad robusto y alineado con las mejores prácticas internacionales, siendo esencial para la protección de la información crítica y la mitigación de riesgos en la institución.

**1. Definir el Alcance del SGSI**

La definición del alcance es uno de los primeros pasos esenciales en la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) conforme a la norma ISO/IEC 27000. El alcance establece las fronteras dentro de las cuales el SGSI operará, especificando qué procesos, activos de información, sistemas y ubicaciones estarán cubiertos, así como cualquier exclusión de la gestión de la seguridad de la información.

**1.1. Descripción General de la Organización**

El **Hospital Clínico de la Universidad de Valparaíso** (en adelante, el "**Hospital UV**") es una institución dedicada a la atención médica de pacientes en diversas especialidades. Además de brindar atención clínica, también realiza investigaciones y actividades académicas en el área de salud. El hospital maneja una cantidad significativa de información sensible, incluyendo datos de pacientes, investigaciones científicas y registros médicos, lo que hace que la gestión de la seguridad de la información sea crítica para proteger la confidencialidad, integridad y disponibilidad de estos datos.

**1.2. Identificación de Activos Críticos**

El SGSI del Hospital UV debe cubrir los activos críticos asociados con el manejo y almacenamiento de información sensible, tales como:

* **Datos de pacientes**: Información personal, médica y de tratamientos, tanto en formato electrónico como físico.
* **Sistemas electrónicos**: Todos los sistemas de gestión hospitalaria, incluyendo los sistemas de información clínica, administración de pacientes, historia clínica electrónica (HCE), telemedicina, y sistemas de soporte a decisiones clínicas.
* **Infraestructura tecnológica**: Servidores, estaciones de trabajo, dispositivos móviles utilizados por el personal médico, administrativo y de soporte, y las redes internas y externas.
* **Recursos humanos**: Personal médico, administrativo, de soporte técnico y de seguridad de la información, que tiene acceso a los datos críticos y participa en su manejo.
* **Servicios externos**: Proveedores de servicios externos que colaboran en áreas como almacenamiento en la nube, soporte técnico o comunicaciones.

**1.3. Procesos Críticos**

El alcance del SGSI debe considerar los siguientes procesos críticos que el hospital realiza a diario:

* **Atención de pacientes**: El manejo de la información médica de los pacientes, incluyendo diagnósticos, tratamientos, y cualquier otra información relevante que se gestione en las unidades clínicas.
* **Gestión administrativa**: La administración de la información relacionada con los recursos humanos, financieros y operacionales del hospital.
* **Investigación y docencia**: La gestión de datos relacionados con investigaciones médicas y académicas, que también deben cumplir con requisitos éticos y de confidencialidad.
* **Tercerización de servicios**: Todos los servicios contratados a terceros que impliquen el acceso a información sensible, como servicios de software en la nube, almacenamiento externo de datos y outsourcing de servicios de TI.

**1.4. Definir los Límites Geográficos**

El alcance del SGSI abarcará las siguientes ubicaciones:

* **Sede principal del Hospital UV**: La sede central que incluye todas las unidades clínicas, administrativas y el centro de investigación.
* **Sedes satélites o filiales**: Si existen unidades secundarias o centros médicos periféricos que gestionen información de pacientes o administrativos del hospital, también deberán ser considerados dentro del alcance.
* **Infraestructura remota**: En caso de que el hospital utilice servicios externos de nube o equipos de trabajo remoto (telemedicina, consultas en línea), estos deben ser incluidos dentro del alcance del SGSI.

**1.5. Inclusiones y Exclusiones del SGSI**

**Inclusiones**:

* Todos los **sistemas electrónicos** que gestionen datos de pacientes, tanto de registros médicos como de información administrativa y financiera.
* Todos los **procesos de manejo de datos sensibles** que impliquen la entrada, procesamiento, almacenamiento, transmisión y eliminación de la información de los pacientes.
* Las **infraestructuras tecnológicas** críticas del hospital, incluyendo servidores, redes internas, equipos informáticos y de almacenamiento de datos.
* Los **proveedores externos** que tengan acceso a la infraestructura tecnológica y datos sensibles del hospital, como los proveedores de servicios de soporte de TI, almacenamiento en la nube y otros servicios críticos.

**Exclusiones**:

* Sistemas o procesos no críticos para la operación hospitalaria, tales como **gestión de compras no relacionadas con equipos médicos**, **sistemas de cafetería**, o **gestión de inventarios generales** que no manejen datos sensibles.
* **Infraestructura externa no gestionada directamente** por el hospital, como centros de datos que no estén directamente involucrados en la gestión de información del hospital.

**1.6. Restricciones y Factores Externos**

Existen ciertos factores que pueden limitar la implementación completa del SGSI dentro del alcance definido. Algunos de estos factores pueden incluir:

* **Limitaciones tecnológicas**: Recursos tecnológicos disponibles que pueden restringir la capacidad del hospital para aplicar controles de seguridad adecuados en algunos sistemas más antiguos o de menor criticidad.
* **Presión de tiempo y presupuesto**: El SGSI deberá ser implementado dentro de las limitaciones presupuestarias y de tiempo establecidas por la dirección del hospital.
* **Cumplimiento normativo**: La organización debe asegurarse de que el SGSI cumpla con todas las leyes locales e internacionales aplicables, como las leyes de protección de datos personales (por ejemplo, la Ley 19.628 en Chile sobre protección de la vida privada).

**1.7. Validación y Aprobación del Alcance**

El alcance del SGSI debe ser revisado y aprobado por la alta dirección del Hospital UV para garantizar que cubra todas las áreas relevantes, que todos los procesos clave estén incluidos y que las exclusiones sean justificables.

**2. Realizar un Análisis del Contexto de la Organización**

El análisis del contexto de la organización es una parte fundamental en la implementación del Sistema de Gestión de Seguridad de la Información (SGSI) según la norma ISO/IEC 27001:2022. Este análisis permite comprender los factores internos y externos que afectan la seguridad de la información y establecer un enfoque adecuado para mitigar riesgos, cumplir con requisitos legales y satisfacer las necesidades de los stakeholders. En el caso del **Hospital Clínico de la Universidad de Valparaíso (HCUV)**, el análisis del contexto se enfoca en identificar los elementos clave que influyen en la gestión de la seguridad de la información en sus actividades diarias.

**2.1. Factores Externos**

Los factores externos se refieren a aquellos elementos fuera del control directo del HCUV, pero que afectan o influyen en las decisiones sobre la seguridad de la información. Estos incluyen:

* **Entorno legal y regulatorio**: El HCUV debe cumplir con normativas nacionales e internacionales de protección de datos, como la **Ley 19.496 sobre Protección de Datos Personales** en Chile y las regulaciones internacionales como el **Reglamento General de Protección de Datos (GDPR)** de la Unión Europea, dado que puede manejar información de pacientes internacionales. Estas normativas requieren salvaguardar la privacidad de la información personal y de salud de los pacientes, así como mantener un manejo transparente y ético de los datos.
* **Requisitos del sector salud**: En el ámbito sanitario, el manejo seguro de la información es crucial no solo por razones de privacidad, sino también para garantizar la calidad del servicio y la atención de los pacientes. Existen normativas específicas en cuanto a la gestión de historiales médicos y los sistemas de salud electrónicos que deben ser seguidas para asegurar la integridad y disponibilidad de la información médica.
* **Tecnologías emergentes**: La evolución constante de la tecnología, como la **inteligencia artificial**, la **telemedicina** y la **gestión digital de la salud**, implica que el HCUV debe adaptarse a nuevas plataformas tecnológicas que pueden introducir vulnerabilidades en la seguridad de la información, al mismo tiempo que proporcionan oportunidades para mejorar la calidad del servicio.
* **Amenazas externas**: Factores como el **cibercrimen**, los **ataques de ransomware** y las **filtraciones de datos** son amenazas que el HCUV debe considerar. Además, los **desastres naturales** o situaciones de **emergencia sanitaria global** como la pandemia del COVID-19 pueden afectar la disponibilidad de los sistemas de información y requerir planes de contingencia adicionales.

**2.2. Factores Internos**

Los factores internos son aquellos que están bajo el control de la organización y que influyen directamente en su capacidad para gestionar la seguridad de la información. En el contexto del HCUV, los factores internos incluyen:

* **Estructura organizacional**: El HCUV está compuesto por un equipo diverso de profesionales de la salud, administrativos, técnicos y personal de TI que interactúan con diferentes sistemas de información. La alta dirección debe comprometerse con la seguridad de la información, implementando una cultura organizacional que valore la protección de datos. La comunicación entre las distintas áreas del hospital debe ser fluida y eficiente para garantizar que las políticas de seguridad sean comprendidas y seguidas en todos los niveles.
* **Recursos tecnológicos**: El HCUV posee una infraestructura tecnológica compuesta por servidores, sistemas de almacenamiento de datos, plataformas de gestión de pacientes y redes de comunicación que deben ser protegidas adecuadamente. Sin embargo, la organización enfrenta desafíos en la actualización constante de sus tecnologías, debido a la rapidez con la que evolucionan los sistemas de TI y las ciberamenazas. La capacitación de personal de TI en prácticas de seguridad de la información también es esencial para garantizar un manejo adecuado.
* **Cultura organizacional**: La cultura dentro del hospital influye significativamente en la gestión de la seguridad de la información. La formación y concienciación del personal médico y administrativo sobre la importancia de proteger los datos sensibles de los pacientes es clave para la implementación exitosa del SGSI. Se debe fomentar una cultura de seguridad activa y no reactiva.
* **Procesos y procedimientos internos**: El HCUV dispone de una serie de procedimientos internos relacionados con la gestión de pacientes, el manejo de la información médica, los procesos administrativos, la gestión de inventarios y la toma de decisiones en situaciones críticas. Cada uno de estos procesos implica la manipulación de información sensible, por lo que es fundamental identificar los controles de seguridad apropiados para cada área.

**2.3. Partes Interesadas (Stakeholders)**

Las partes interesadas son aquellas personas o entidades que tienen un interés en la protección de la información en el HCUV. Esto incluye:

* **Pacientes**: Los pacientes son los principales interesados, ya que sus datos personales y médicos deben ser protegidos con el más alto nivel de seguridad para garantizar su privacidad y confianza en el sistema de salud.
* **Personal de salud y administrativo**: Médicos, enfermeros, técnicos, administrativos y otros empleados del hospital tienen acceso a sistemas que contienen información sensible. Es crucial que todos ellos comprendan la importancia de la seguridad de la información y sigan las políticas establecidas.
* **Autoridades sanitarias y reguladoras**: Organismos gubernamentales y reguladores del sector salud, como el Ministerio de Salud de Chile, que exigen el cumplimiento de las normativas locales e internacionales de privacidad y seguridad de datos.
* **Proveedores y socios comerciales**: Empresas que brindan servicios o productos al HCUV, como proveedores de software, plataformas tecnológicas o servicios de almacenamiento de datos, tienen un impacto directo sobre la seguridad de la información. La organización debe asegurarse de que estos proveedores cumplan con los mismos estándares de seguridad.
* **Comunidad académica y de investigación**: El HCUV también está vinculado a la academia y la investigación médica, y la protección de datos relacionados con estos proyectos es esencial para garantizar la integridad de los estudios y el cumplimiento de las normativas éticas.

**2.4. Evaluación de Riesgos y Oportunidades**

Es necesario identificar y evaluar los riesgos que podrían comprometer la seguridad de la información, como ciberataques, negligencia humana, desastres naturales, entre otros. Del mismo modo, es importante identificar oportunidades que puedan mejorar la gestión de la seguridad de la información, como la adopción de nuevas tecnologías, la mejora en los procesos internos o la capacitación del personal.

**2.5. Requisitos y Expectativas de las Partes Interesadas**

El HCUV debe considerar los requisitos y expectativas de todas las partes interesadas en cuanto a la seguridad de la información. Esto incluye el cumplimiento de las regulaciones de privacidad, la garantía de la disponibilidad continua de los sistemas críticos y la protección de la información sensible contra accesos no autorizados.

**2.6. Contexto de Riesgo**

El análisis del contexto también debe incluir la identificación de los posibles eventos que puedan generar riesgos para la seguridad de la información, como los siguientes:

* **Pérdida de datos**: A través de fallos tecnológicos o de procedimientos inadecuados.
* **Accesos no autorizados**: Por parte de personal interno o externo.
* **Fugas de información**: Debido a un manejo inapropiado de los datos personales de los pacientes o de los registros médicos.
* **Interrupciones en los servicios**: Debido a ataques informáticos o desastres naturales.

**3. Política de Seguridad de la Información - Hospital Clínico UV**

**3.1. Objetivo:** El objetivo principal de esta política es establecer los principios y directrices para la gestión de la seguridad de la información dentro del Hospital Clínico UV. Su propósito es proteger la información sensible, garantizar la confidencialidad, integridad y disponibilidad de la misma, y minimizar los riesgos asociados a la seguridad de la información, asegurando así la correcta gestión y protección de los datos críticos del hospital.

**3.2. Alcance:** Esta política se aplica a todos los activos de información y procesos asociados al Hospital Clínico UV, incluyendo:

* **Sistemas de Información**: Todo software, hardware y redes utilizadas para la gestión y almacenamiento de la información.
* **Personal**: Incluyendo personal médico, administrativo, de TI y cualquier tercero o proveedor con acceso a sistemas de información.
* **Datos**: Toda la información, tanto digital como física, gestionada por el hospital, que incluye registros médicos, datos de pacientes, personal, y toda la información relacionada con la gestión hospitalaria.

**3.3. Procedimientos:**

* **Identificación y Clasificación de la Información**: El hospital establecerá procedimientos para identificar y clasificar los activos de información en función de su nivel de confidencialidad, criticidad e impacto para la organización. Esta clasificación servirá como base para definir las medidas de protección y los controles necesarios.
* **Evaluación de Riesgos**: Se implementará un proceso continuo de identificación, evaluación y tratamiento de riesgos asociados a la seguridad de la información. La evaluación será llevada a cabo al menos una vez al año o en caso de cambios significativos en los procesos o infraestructura.
* **Control de Accesos**: Los accesos a la información se limitarán a aquellos individuos que necesiten conocerla para cumplir con sus funciones. Todos los accesos deberán ser registrados y monitorizados.
* **Protección de Datos**: Los datos sensibles, incluyendo los registros de pacientes, serán protegidos mediante cifrado en tránsito y reposo, asegurando su integridad y confidencialidad.
* **Respuesta ante Incidentes**: En caso de incidentes de seguridad, se definirá un protocolo claro de respuesta para mitigar el impacto, restaurar los servicios afectados y tomar medidas correctivas para prevenir futuros incidentes.
* **Monitoreo Continuo**: Se implementará un sistema de monitoreo que permita detectar posibles incidentes de seguridad en tiempo real, incluyendo el uso de herramientas de auditoría y seguimiento de eventos.

**3.4. Responsabilidades:**

* **Gerencia**: La alta dirección del Hospital Clínico UV es responsable de proporcionar los recursos necesarios para la implementación y mantenimiento del SGSI, asegurando que todas las actividades se alineen con los objetivos organizacionales y las normativas aplicables.
* **Responsable del SGSI**: El responsable del SGSI será el encargado de coordinar todas las acciones relacionadas con la seguridad de la información, garantizar la implementación efectiva de los controles y la evaluación continua de los riesgos.
* **Usuarios**: Todos los empleados, proveedores y terceros que interactúan con los sistemas de información del hospital tienen la responsabilidad de cumplir con esta política y seguir los procedimientos establecidos para la protección de la información.
* **Terceros y Proveedores**: Los proveedores externos que gestionen información del hospital deberán cumplir con las mismas políticas de seguridad establecidas, asegurando que no se comprometa la seguridad de la información en el proceso de gestión.

**3.5. Compromiso:** El Hospital Clínico UV se compromete a:

* Proteger la confidencialidad, integridad y disponibilidad de la información crítica para la operación del hospital.
* Cumplir con los requisitos legales y normativos aplicables a la seguridad de la información, incluyendo la normativa ISO/IEC 27001:2022.
* Fomentar una cultura organizacional que valore la seguridad de la información, sensibilizando y capacitando regularmente al personal.

**3.6. Cumplimiento:** La implementación de esta política será supervisada por el responsable del SGSI. El cumplimiento será obligatorio para todos los miembros de la organización. Los incumplimientos de las normas de seguridad de la información se sancionarán conforme a la normativa interna del hospital, que podrá incluir desde medidas correctivas hasta la finalización de la relación laboral o contractual con el responsable del incumplimiento.

**3.7. Revisión:** La política de seguridad de la información será revisada al menos una vez al año, o cuando ocurra un cambio significativo en la infraestructura tecnológica, en los riesgos asociados o en las regulaciones aplicables. La revisión estará a cargo del Responsable del SGSI, quien evaluará la efectividad de las medidas implementadas y propondrá mejoras.

**4. Identificar y Valorar los Activos de Información**

En este punto se identifican los activos de información más importantes para la organización, como bases de datos, sistemas de gestión hospitalaria y registros médicos. Posteriormente, se realiza una valoración de su importancia según su confidencialidad, integridad y disponibilidad, con el fin de priorizar la protección de los activos críticos.

**5. Identificar Amenazas, Vulnerabilidades y Riesgos**

Se procede a identificar las amenazas externas e internas que podrían afectar la seguridad de la información en el hospital, tales como ataques cibernéticos, errores humanos o fallos tecnológicos. Además, se evalúan las vulnerabilidades existentes en los sistemas y procesos actuales, lo que nos permite estimar los riesgos y sus posibles impactos en la institución.

**6. Definir un Plan de Tratamiento del Riesgo**

Basado en la identificación y valoración de riesgos, se debe diseñar un plan de tratamiento para mitigar, transferir o aceptar los riesgos identificados. El plan incluye la asignación de recursos, la definición de plazos y la implementación de acciones correctivas para reducir el impacto de los riesgos en la organización.

**7. Definir las Actividades de Control**

En este paso, se desarrollan y definen los controles que deben implementarse para mitigar los riesgos identificados. Los controles abarcan aspectos técnicos, físicos y administrativos, e incluyen tanto medidas preventivas como correctivas para garantizar la seguridad de la información dentro del Hospital Clínico.

**8. Crear Procesos de Comunicación y Capacitación**

La seguridad de la información no solo depende de los controles técnicos, sino también de la cultura organizacional. Por eso, se deben establecer procesos de comunicación efectivos y programas de capacitación continua para todos los empleados, garantizando que cada miembro del hospital esté alineado con las políticas de seguridad y conozca las mejores prácticas para manejar la información de manera segura.

**9. Desarrollar la Documentación del SGSI**

Es fundamental documentar todo el SGSI para asegurar su operatividad y facilitar su seguimiento y revisión. Esto incluye la creación de manuales, procedimientos, registros y políticas que definan claramente los roles, responsabilidades y procesos de seguridad de la información, asegurando la consistencia en la gestión de la seguridad a largo plazo.