SERVICIO DE SALUD TALCAHUANO
SUBDIRECCIÓN ADMINISTRATIVA
ÁREA DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN
HOSPITAL DE TOMÉ

TOMÉ, 28 OCTUBRE 2025

VISTOS:

Considerando el Decreto Fuerza Ley N° 01/24.04.2006 del MINSAL; el D.F.L. N° 29/2004 sobre Estatuto Administrativo; la Ley N° 19.880 sobre Bases de los Procedimientos Administrativos; la Resolución N° 6/2019 de Contraloría sobre exención de toma de razón en materias de personal; los Decretos Supremos de Salud N° 140/2005 y N° 38/2005 que aprueban los Reglamentos Orgánicos de los Servicios de Salud y de los Establecimientos de Salud de Menor Complejidad; la Resolución Exenta N° 2778/2023 del SSThno; la Resolución Exenta N° 1251/2023 que aprueba la Política General de Seguridad de la Información del Hospital de Tomé; el COMGES 2025; y el Ordinario N° 943/2025 del Subsecretario de Redes Asistenciales sobre implementación de controles críticos de seguridad de la información según ISO/IEC 27001:2022; que, conforme al D.S. N° 285/2022 y la Ley N° 21.663 de Ciberseguridad, el Hospital de Tomé se encuentra incluido en la lista preliminar de **Operadores de Importancia Vital (OIV)**; y que, mediante la Providencia N° DHT-6553 y el oficio N° 0106 clasificado como secreto, se instruye evacuar un Informe Técnico Fundado respecto del cumplimiento de los criterios del artículo 4° del D.S. N° 285/2022, se da curso a la presente comunicación.

CONSIDERANDO:

1. Que la adecuada clasificación y manejo de la información es esencial para garantizar la confidencialidad, integridad y disponibilidad de los activos de información del Hospital de Tomé.
2. Que el Hospital de Tomé requiere establecer lineamientos claros sobre la gestión, almacenamiento, transmisión, etiquetado, y destrucción de la información institucional, de acuerdo con los estándares ISO/IEC 27001 e ISO/IEC 27002, y complementado con el esquema Traffic Light Protocol (TLP) 2.0 para información externa.
3. Que la correcta clasificación de la información permite identificar los niveles de sensibilidad y riesgo, asegurando que cada activo reciba el tratamiento y medidas de seguridad apropiadas según su criticidad.
4. Que la presente política abarca a todos los funcionarios, personal a honorarios y terceros que tengan acceso a los sistemas o información del Hospital de Tomé, independientemente del soporte físico o digital de la información.
5. Que la implementación de esta política contribuye a cumplir con la Ley N° 19.628, Ley N° 20.285, Ley N° 21.663 y otras normas relacionadas con protección de datos, ciberseguridad y transparencia, alineando el manejo de la información a buenas prácticas internacionales y estándares institucionales.

RESUELVE EXENTA N° 2120

1. **APRUEBASE** la Política de Clasificación y Manejo de la Información del Hospital de Tomé, que establece lineamientos, responsabilidades y procedimientos para la identificación, clasificación, protección, almacenamiento, transmisión, etiquetado, duplicación y destrucción de los activos de información institucional, en concordancia

con normas nacionales, estándares internacionales y buenas prácticas de seguridad de la información.

2. **DISPONGASE** que la presente política sea aplicada por todos los servicios, unidades, funcionarios, personal a honorarios y terceros que tengan acceso a la información del Hospital de Tomé, asegurando la correcta gestión de los activos de información, el cumplimiento de los niveles de confidencialidad (Secreta, Reservada, Uso Interno, No Clasificada) y la aplicación complementaria del Traffic Light Protocol (TLP) 2.0 en los contextos pertinentes.
3. **ENCARGUESE** al Comité de Seguridad de la Información y al Encargado de Seguridad de la Información (CISO) la supervisión, control y actualización periódica de la política y procedimientos asociados, incluyendo la validación de clasificaciones, la trazabilidad de accesos, y la gestión de incidentes de seguridad relacionados con el manejo de información.
4. **DEJASE CONSTANCIA** que los responsables de cada activo de información, normalmente las jefaturas de unidad, área o servicio, deberán aplicar la política en sus procesos, manteniendo inventario actualizado de activos, garantizando la protección de la información según su criticidad, y reportando cualquier incidente o incumplimiento a las autoridades competentes.
5. **ESTABLECESE** que la presente resolución entra en vigor a partir de su publicación, y que cualquier modificación futura deberá efectuarse mediante resolución exenta de la autoridad competente, asegurando la coherencia con las normativas legales y estándares internacionales aplicables.

"ANÓTESE Y COMUNÍQUESE"

LEC/CCU/ccu
N° INT. 03/28.10.2025
DISTRIBUCIÓN:

- Subdirección Administrativa H. Tomé
- Subdirección Médica H. Tomé
- Oficina de Partes Hospital de Tomé
- CR. Apoyo Diagnóstico
- Área Recursos Físicos
- Área Gestión y Desarrollo de las Personas
- CR. Atención Cerrada
- CR. Atención Abierta
- CR. Emergencia

FIRMA DIRECTOR HOSPITAL DE TOMÉ ELECTRONICA

Firmado por Aníbal Antonio Cea Henríquez
Fecha 28/10/2025 15:09:38 CLST

POL03-25-0003

POLITICA PARA LA CLASIFICACIÓN Y MANEJO DE INFORMACIÓN

Sistema de Gestión de Seguridad de la Información – Hospital de Tomé

Versión Oficial Actual 1 – Julio 2025

Contenido

1 PRÓPOSITO

Esta Política tiene por objeto clasificar los activos de información para garantizar una eficaz gestión de su seguridad, protegiendo la información y documentación sensible del Hospital de Tomé para prevenir su divulgación y acceso por parte de personas o instituciones no autorizadas.

2 ALCANCE O AMBITO DE APLICACIÓN

El alcance de este documento se aplica a todos los recursos computacionales del Hospital de Tomé y sus áreas dependientes que tengan acceso a Internet, en las cuales se implemente esta política.

Es aplicable a todo tipo de información independiente del soporte en el que se encuentre, por ejemplo: documentos, sistemas de información, redes, sistemas de comunicaciones móviles, sistemas de información, dispositivos móviles, nubes, correo, correo de voz, comunicaciones de voz en general, multimedia, servicio postal, etc., y cualquier otro elemento sensible, como, por ejemplo, cheques en blanco, facturas.

Es aplicable a todos los funcionarios (planta, contrata, reemplazos y suplencia), así como al personal a honorarios y terceros (Proveedores, compra de servicios, entre otros), que presenten servicios para el Hospital de Tomé.

Esta política abarca los siguientes controles definidos en la norma NCh-ISO 27002:2013, denominada "Tecnologías de la Información – Técnicas de seguridad – Código de prácticas para los controles de seguridad de la información" y, en específico:

- A.08.01.02 Propiedad de los activos
- A.08.01.03 Uso aceptable de los activos
- A.08.02.01 Clasificación de la Información
- A.08.02.02 Etiquetado de la Información
- A.08.02.03 Manejo de Activos
- A.18.01.03 Protección de registros

3 MARCO NORMATIVO Y DOCUMENTOS RELACIONADOS

- Marco Normativo
  - NCh-ISO27001:2013: Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de la seguridad de la información – Requisitos.
  - Ley N° 19.628, de Protección de vida privada y datos personales.
  - Ley N° 19.799, de firmas y documentos electrónicos.
  - Ley N° 19.927, de Delitos de Pornografía Infantil.
  - Ley N° 20.285 regula el principio de transparencia de la función pública y el derecho de acceso a la información de los órganos de la Administración del Estado.
  - Ley N° 21.180, de Transformación Digital del Estado.
  - Ley N° 21.459, que Establece normas sobre Delitos Informáticos, deroga la Ley N°19.223 y modifica otros cuerpos legales con el Objeto de Adecuarlos al Convenio de Budapest.
  - Decreto N° 83, 2004, Ministerio Secretaría General de la Presidencia, que aprueba norma técnica para los órganos de la administración del estado sobre seguridad y confidencialidad de los documentos electrónicos.
  - El Marco Jurídico referido a los Sistemas de Seguridad de la Información (SSI), publicado en el portal del CSIRT del Ministerio del Interior.
    - Decretos Supremos y Normas Internacionales de Seguridad de la Información y Ciberseguridad:
    - Leyes relacionadas

- **Documentos Relacionados**
  - Procedimiento gestión derechos de acceso y devolución de activos.
  - Política Seguridad de la Red.

4 ROLES Y RESPONSABILIDADES

El adecuado manejo y protección de la información es crucial para garantizar la seguridad y confidencialidad de los datos del Hospital de Tomé. En este sentido, se establecen diferentes roles y responsabilidades dentro de la institución, cada uno con sus funciones específicas para garantizar un entorno seguro y protegido. A continuación, se describen los principales roles y sus responsabilidades.

- **Comité de Seguridad de la Información**:
  - Definir lineamientos estratégicos sobre la gestión de la información y validar las políticas y procedimientos relacionados.
  - Resolver situaciones complejas o excepcionales sobre el acceso, uso o clasificación de la información.
  - Supervisar el cumplimiento general de la política y proponer mejoras a nivel institucional
  - Apoyar en la gestión de incidentes de seguridad de nivel 3 (Urgentes).
- **Encargado de Seguridad de la Información**:
  - Apoyar técnicamente la implementación de medidas de seguridad y controles de acceso a los sistemas de información.
  - Aplicar soluciones tecnológicas que refuercen la protección de los datos según su clasificación (cifrado, respaldo, control de acceso, entre otros)
  - Garantizar la disponibilidad, integridad y confidencialidad de los activos de información bajo su responsabilidad.
  - Detectar y reportar vulnerabilidades o brechas relacionadas con el manejo de la información.
- **Jefes de Unidades / Área**:
  - Identificar y declarar los activos de información relevantes de su unidad, con el apoyo del Encargado de Seguridad de la Información.
  - Aplicar la clasificación correspondiente a la información que gestionan, conforme a lo definido en la política.
  - Asegurar que los funcionarios bajo su supervisión conozcan y cumplan las normas y procedimientos relativos al manejo de la información.
  - Evaluar y aprobar necesidades de acceso a información clasificada en su área.
- **Funcionarios y personal en general**:
  - Conocer y aplicar las normas de clasificación y manejo seguro de la información según el nivel que le corresponda.
  - Proteger la información a la que acceden en el ejercicio de sus funciones, evitando su divulgación o uso indebido.
  - Informar a su jefatura o al Encargado de Seguridad de la Información ante cualquier sospecha o incidente relacionado con la seguridad de los datos.
  - Participar en actividades de capacitación sobre manejo y clasificación de la información.

5 DIRECTRICES

5.1 Responsables de los activos de información

Los responsables de proceso de los activos de información son las Jefaturas de Unidad, Área o Servicio del Hospital de Tomé. Estas jefaturas tienen la responsabilidad principal de asegurar la adecuada gestión, protección y clasificación de la información generada, almacenada y utilizada en el ámbito de sus respectivas unidades, en conformidad con lo establecido en la presente política y la normativa vigente.

En específico, les corresponde:

- Identificar y declarar los activos de información relevantes de su unidad, en coordinación con el Encargado de Seguridad de la Información.
- Aplicar la clasificación correspondiente a la información que gestionan, conforme a los criterios definidos en esta política.
- Asegurar que los funcionarios bajo su supervisión conozcan, comprendan y cumplan las normas y procedimientos relativos al manejo y protección de la información.
- Evaluar, aprobar y solicitar los requerimientos de acceso a la información clasificada dentro de su área de responsabilidad, resguardando que dichos accesos sean otorgados bajo el principio de necesidad de conocer.

Adicionalmente, deberán realizar acciones periódicas de revisión de la clasificación y restricciones de acceso aplicables a los activos de información bajo su custodia. Estas revisiones deben considerar los principios de seguridad de la información, las políticas institucionales de control de acceso y las disposiciones legales y regulatorias vigentes, con el fin de asegurar que los activos mantengan un nivel de protección adecuado a su criticidad y sensibilidad.

5.2 Gestión de inventario y activos de información

Es fundamental que todos los activos de información del Hospital de Tomé se encuentren debidamente identificados, inventariados y clasificados, de modo que se determine su importancia relativa y se apliquen los niveles adecuados de protección.

5.2.1 Responsabilidad sobre los Activos

Cada activo debe tener un responsable claramente definido, quien será el encargado de su identificación, clasificación y administración. Este responsable, normalmente la jefatura de la unidad, área o servicio correspondiente deberá elaborar y mantener actualizado un inventario de los activos de información bajo su custodia. Este inventario deberá contener la información básica que permita evaluar las características, criticidad y nivel de protección requerido para cada activo.

5.2.2 Contenido mínimo del inventario

El inventario de activos de información deberá contener, como mínimo, los siguientes campos:

- **Nombre del Activo:** Identificación única del activo dentro del proceso al que pertenece.
- **Proceso Asociado:** Nombre del proceso institucional al cual se encuentra vinculado el activo.
- **Tipo de Activo:** Clasificación general del activo, según las siguientes categorías:
    - **Información:** Datos almacenados o procesados, ya sea en formato físico o electrónico, tales como bases de datos, contratos, manuales,

acuerdos de confidencialidad, planes de continuidad, procedimientos, reportes de auditoría, entre otros.
    - **Software:** Aplicaciones, sistemas operativos, herramientas de desarrollo, utilitarios, interfaces, etc.
    - **Recurso Humano:** Personas que, por su conocimiento, experiencia o función crítica, son consideradas activos clave para el proceso.
    - **Servicio:** Servicios de tecnología o comunicación, tales como internet, plataformas en la nube institucional, intranet, o recursos compartidos.
    - **Hardware:** Equipamiento informático y de comunicaciones que, por su criticidad, son considerados activos de información, sin limitarse a activos fijos.
    - **Otros:** Cualquier activo que no encaje en las categorías anteriores, pero que deba ser valorado por su relevancia dentro del proceso.
- **Ubicación:** Localización física y/o lógica del activo.
- **Administrador de Sistema:** Nombre de la unidad interna o entidad externa responsable de la creación o custodia del activo.
- **Dueño de Proceso:** Nombre de la unidad interna responsable del uso del sistema, sus procesos y datos.

5.2.3 Clasificación y Criticidad

La propiedad y clasificación de la información deben ser determinadas y documentadas para cada activo inventariado, en base a los siguientes criterios:

- **Clasificación de la información**: Determinación del nivel de protección requerido en función de las propiedades de:
    - Confidencialidad
    - Integridad
    - Disponibilidad
- **Criticidad del Activo**: Evaluación del valor del activo según el impacto potencial sobre las propiedades anteriores. Se definen tres niveles:
    - Alta: Cuando dos o mas propiedades con clasificadas como de alta importancia
    - Media: Cuando al menos una propiedad tiene un nivel alto o medio.
    - Baja: Cuando tolas las propiedades son clasificadas como de bajo impacto
- **Niveles de Protección**: A partir del nivel de criticidad determinado, se deben aplicar los controles mínimos de seguridad necesarios, de acuerdo con las buenas prácticas institucionales y los estándares definidos en esta Política.

5.2.4 Ciclo de vida del Activo

Cada activo debe ser gestionado durante todo su ciclo de vida, el cual comprende desde su identificación o incorporación inicial, pasando por su uso operativo, mantenimiento o actualización, hasta su disposición final mediante eliminación, descarte, reciclaje o traspaso, asegurando en todo momento la aplicación de medidas de seguridad acordes a su clasificación.

5.2.5 Propiedad de la Información

Todos los datos e información institucional deben contar con un propietario formal, quien será el responsable de su clasificación según los niveles definidos en la sección **5.2.3 Clasificación de la Información** de esta política.

En caso de activos no inventariados o documentos de carácter transitorio o no oficial (como borradores o anteproyectos), y que no cuenten con un responsable explícito

asignado, la responsabilidad de aplicar las medidas de seguridad adecuadas recae sobre el creador de la información. Este deberá velar por su protección y uso adecuado durante su tratamiento, almacenamiento o transmisión respetando las Políticas institucionales vigentes.

5.3 Clasificación de la Información

La información se clasifica de acuerdo con su estado y nivel de confidencialidad siendo:

5.3.1 Estado

- **En Transito**: Se refiere a la información para uso exclusivo del Hospital de Tomé, que está siendo transferida o desplazada de un lugar a otro, ya sea físicamente o a través de medios electrónicos. Tal como son los respaldos a los actos administrativos. Por ejemplo: Actas, minutos, circular interna, correos electrónicos, entre otros.
- **Producto Final**: Hace referencia a los documentos que soportan información y que han alcanzado su versión final y definitiva. Estos documentos se consideran productos terminados y listos para su distribución, publicación o uso oficial. Tal como son las leyes, reglamentos, resoluciones, decretos, ordinarios en cualquier medio de soporte.

5.3.2 Confidencialidad

La dimensión de Confidencialidad evalúa el grado de restricción que debe aplicarse al acceso y difusión de la información, en función de su sensibilidad, obligaciones legales y el posible impacto negativo de su divulgación no autorizada.

5.3.3 Sistema de clasificación de la Información

El Hospital de Tomé adopta como sistema oficial de clasificación de la información aquel basado en el criterio de confidencialidad, conforme a lo establecido en la normativa chilena vigente, en particular la Ley N° 20.285 sobre Acceso a la Información Pública, la Ley N° 19.628 sobre Protección de la Vida Privada, y los estándares internacionales ISO/IEC 27001 e ISO/IEC 27002. Este sistema establece los siguientes niveles de clasificación:

- **SECRETO**
- **RESERVADO**
- **USO INTERNO**
- **NO CLASIFICADA**

Cada nivel implica una serie de controles específicos en cuanto a almacenamiento, acceso, transmisión, destrucción y etiquetado, definidos en la presente política.

Sin perjuicio de lo anterior, y considerando la necesidad de interoperabilidad con entidades externas en materia de ciberseguridad (como CSIRT-Gob, MINSAL o CERT internacionales), el Hospital de Tomé reconoce la utilidad del **Esquema de Semáforo TLP (Traffic Light Protocol)**, versión 2.0, para regular el **alcance de la difusión de la información compartida con terceros**.

Por tanto, cuando se requiera compartir información en contextos de ciberseguridad, comunicaciones interinstitucionales o cooperación con organismos especializados, el **Responsable de Seguridad de la Información (CISO)** deberá complementar la clasificación interna con el nivel TLP correspondiente, conforme a las definiciones del protocolo TLP 2.0:

- **TLP:ROJO**
- **TLP:AMBAR** (incluyendo variantes como **AMBAR+ESTRICTO**)
- **TLP:VERDE**
- **TLP:BLANCO**

Este uso será complementario y no reemplaza la clasificación institucional, la cual seguirá siendo obligatoria para todo el tratamiento interno de la información. El uso del TLP se limitará a contextos de difusión externa o coordinación en incidentes, asegurando que se mantenga coherencia y proporcionalidad con los controles definidos por el nivel de confidencialidad de cada activo.

5.3.3.1 Nivel de Clasificación SECRETO

- **TLP Asociado**: **TLP:ROJO**
- **Color:** RGB (255,0,51), Hexadecimal (#ff0033)
- **Descripción / Criterio de Clasificación**: Información extremadamente sensible cuyo acceso está limitado a personas específicas. Su divulgación puede causar un alto impacto legal, reputacional, operativo o económico.
- **Restricción de Acceso y Difusión**: Solo puede ser compartida con las personas directamente involucradas en un contexto específico (reunión, incidente, comité) Prohibido todo reenvío o divulgación posterior.

5.3.3.2 Nivel de Clasificación RESERVADO

- **TLP Asociado**: **TLP: AMBAR+ESTRICTO**
- **Color:** RGB (255,192,0), Hexadecimal (#ffc000)
- **Descripción / Criterio de Clasificación**: Información sensible de carácter interno cuya divulgación puede generar riesgos graves para el hospital. Abarca datos protegidos por la Ley 20.2825 y Ley 19.628.
- **Restricción de Acceso y Difusión**: Puede compartirse solo dentro del Hospital de Tomé, y únicamente con personas autorizadas y con necesidad de conocer (Justificada). Prohibido compartir fuera de la institución.

5.3.3.3 Nivel de Clasificación USO INTERNO

- **TLP Asociado**: **TLP:AMBAR**
- **Color:** RGB (255,192,0), Hexadecimal (#ffc000)
- **Descripción / Criterio de Clasificación**: Información institucional de uso interno que, si bien no es altamente sensible, su divulgación no autorizada podría generar inconvenientes o comprometer parcialmente la operación.
- **Restricción de Acceso y Difusión**: Puede compartirse con funcionarios y terceros autorizados bajo necesidad de conocer. Se prohíbe su divulgación externa sin autorización del responsable del activo.

5.3.3.4 Nivel de Clasificación NO CLASIFICADA (Pública)

- **TLP Asociado**: **TLP: VERDE**
- **Color:** RGB (51,255,0), Hexadecimal (#33FF00)
- **Descripción / Criterio de Clasificación**: Información sin restricciones de acceso, cuyo uso o difusión no implica perjuicio para el hospital. Incluye aquella información disponible por transparencia activa o pasiva. Esta clasificación "No Clasificada" es el por defecto para referirse a documentación pública y se recomienda como buena practica agregar TLP:VERDE de manera complementaria, para indicar que es información de carácter Pública.
- **Restricción de Acceso y Difusión**: Puede ser difundida libremente a través de los canales oficiales (OIRS, Sitio Web, Solicitudes de Transparencia) respetando normativa vigente.

5.3.3.5 Nivel NO CLASIFICADA

- **TLP Asociado**: **TLP:BLANCO**
- **Color:** RGB (255,255,255), Hexadecimal (#ffffff)
- **Descripción / Criterio de Clasificación**: Información aún no etiquetada ni clasificada formalmente. Incluye borradores, documentos transitorios u olvidados del inventario. Es importante indicar que esta clasificación la ley la interpreta como la clasificación por defecto de la información, por ende, si es necesario se recomienda complementar con TLP:BLANCO indicando inequívocamente que no esta clasificada, pero que no es precisamente de carácter público.
- **Restricción de Acceso y Difusión**: Deben tratarse como activos de información no publicables hasta su correcta clasificación. Su difusión sin evaluación previa está restringida.

5.3.3.6 Consideraciones sobre la información pública y no clasificada

En el marco de la Ley N° 20.285 sobre Acceso a la Información Pública y su principio de transparencia, se establece que toda información en poder del Estado es pública, salvo que haya sido clasificada conforme a una norma legal expresa como secreta o reservada, o restringida por otras disposiciones legales.

Por tanto, en el Hospital de Tomé, se entenderá que:

- La información que no se encuentre clasificada expresamente como SECRETA, RESERVADA o de USO INTERNO, será considerada como NO CLASIFICADA.
- Esta información puede incluir contenido de carácter público, y su acceso no estará restringido salvo que una normativa específica lo disponga.
- La categoría NO CLASIFICADA no implica la ausencia de gestión o protección básica, ya que esta información igualmente debe manejarse con orden, trazabilidad y conforme a los procedimientos institucionales.
- En caso de duda sobre si una información debe clasificarse o no, se deberá consultar al Encargado de Seguridad de la Información, quien podrá recomendar su clasificación preventiva o aplicar medidas transitorias.

Nota: La clasificación de una información puede evolucionar con el tiempo. Si una información NO CLASIFICADA comienza a incluir antecedentes sensibles o estratégicos, deberá ser revaluada por el responsable del activo de información para aplicar la clasificación correspondiente.

5.3.3.7 Aplicación práctica del TLP 2.0

Toda información oficial deberá llevar su nivel de clasificación indicado explícitamente, y en caso de uso de documentos o comunicaciones:

- Correo Electrónico: Indicar el nivel de Clasificación al inicio del asunto (*ej: RESERVADO – Informe de Gestión de Riesgos o No Clasificada TLP:BLANCA Borrador de Política*)
- En documentos: Indicar el nivel Clasificación en el encabezado de cada hoja, alineado a la derecha, con tipografía de al menos 11 puntos y el color correspondiente.
- En conversaciones verbales: si no se indica explícitamente un nivel de Clasificación, se asumirá como **No Clasificada** por defecto.
- En canales digitales como Chats: puede establecerse una Clasificación por defecto en el reglamento del canal según la naturaleza del mismo.

Importante

- La aplicación del protocolo TLP no reemplaza la legislación nacional, sino que la complementa con estándares de ciberseguridad ampliamente reconocidos
- Toda clasificación debe ser evaluada y validada por el responsable del activo y el Encargado de Seguridad de la Información
- La incorrecta clasificación o uso indebido de información puede ser sancionada según el reglamento interno y la normativa legal vigente.

5.4 Almacenamiento de Información

El almacenamiento de los activos de información debe cumplir con medidas de seguridad proporcionales a su nivel de clasificación, con el fin de evitar accesos no autorizados, pérdidas, modificaciones indebidas o divulgaciones no intencionadas. Estas medidas aplican tanto al soporte físico como digital, y deben considerar las especificaciones del fabricante para los medios de almacenamiento, así como las normativas vigentes sobre protección de datos y ciberseguridad.

I. Información clasificada como Secreta o Reservada - (TLP:ROJO / TLP:AMBAR+ESTRICTO)

a. Cuando no esté en uso, especialmente durante horario inhábil o ausencia prolongada del funcionario, toda información SECRETA o RESERVADA debe permanecer almacenada en un lugar seguro y con acceso restringido a fin de evitar su exposición a personas no autorizadas.
b. Esta prohibido almacenar información de este nivel en el disco duro u otro componente del computador personal institucional o portátil sin autorización expresa del dueño del activo de información y sin contar con un sistema de control de acceso individualizado, como autenticación por usuario y contraseña
c. Todo almacenamiento digital de esta información debe realizarse únicamente en sistemas institucionales con respaldo seguro, cifrado (según criticidad), y monitoreo activo por parte del área de TI o el Encargado de Seguridad de la Información
d. Los medios de respaldo físico (pendrive, discos duros, entre otros) que contengan este tipo de información deben estar protegidos en lugares cerrados, registrados e inventariados, y solo ser utilizados cuando sea estrictamente necesario.

II. Información clasificada como USO INTERNO - (TLP:AMBAR)

a. La información de uso interno, aunque de menor sensibilidad, no debe almacenarse en equipos que posean accesos genéricos o compartidos.
b. Solo se permitirá su almacenamiento en dispositivos institucionales que cuenten con cuentas de usuario personalizadas y protegidas con contraseña, y bajo la responsabilidad directa del funcionario o unidad propietaria del activo.
c. El cifrado de este tipo de información será recomendable, especialmente si se traslada o almacena temporalmente fuera del entorno de red institucional.

III. Información No Clasificada (TLP: VERDE)

a. La información clasificada como No clasificada con TLP:Verde puede almacenarse en sistemas abiertos o compartidos, siempre que se respeten los estándares de integridad, disponibilidad y la normativa de transparencia vigente.

IV. Información No clasificada (TLP:BLANCO)

a. La información no clasificada con TLP: Blanco deberá tratarse, de forma preventiva, como información no publicable, y su almacenamiento debe seguir medidas básicas de resguardo hasta que se determina su clasificación formal.

Como consideración general, todo equipo o sistema donde se almacene información institucional debe estar protegido por medidas técnicas como antivirus, actualizaciones periódicas, acceso autenticado (idealmente centralizado) y, de ser requerido, cifrado en disco.
La responsabilidad sobre el almacenamiento seguro recae tanto en el dueño del activo como en los funcionarios que accedan o manipulen dicha información.

El uso de medios personales (USB, Discos Externos no Institucionales, cuentas en la Nube privadas como Google Drive, OneDrive, entre otras que sean usadas para almacenar información institucional clasificada está prohibido, salvo autorización expresa documentada y con medidas de control adicionales, para lo cual se deberá asegurar el cumplimiento de normativas vigentes de ciberseguridad.

5.5 Servicio de Almacenamiento

El Área de Tecnologías de la Información del Hospital de Tomé declara que los servicios asociados a la **Nube Institucional** —implementada mediante recursos compartidos del dominio institucional (Active Directory) tienen como finalidad principal **facilitar la transferencia y el trabajo colaborativo de la información**, **no constituyendo un medio de almacenamiento permanente o de respaldo oficial**

Por lo tanto:

- La responsabilidad del almacenamiento seguro y definitivo de la información recae en los usuarios y/o propietarios de los activos de información, quienes deberán generar copias adecuadas y almacenarlas conforme a las disposiciones de esta política y los mecanismos definidos por la institución.
- Toda información contenida en la Nube Institucional se entenderá como información clasificada bajo el nivel USO INTERNO, por lo que deberá cumplir con las medidas de seguridad correspondientes, especialmente las relacionadas con el control de acceso individualizado.
- No se permitirá el acceso genérico o sin trazabilidad a los recursos compartidos, debiendo todo acceso ser otorgado nominalmente, vinculado a una cuenta de usuario institucional y con autenticación segura.
- El uso de la Nube Institucional no reemplaza los procedimientos establecidos para el almacenamiento seguro de información clasificada, especialmente en los casos de información SECRETA o RESERVADA, los cuales requieren sistemas y ubicaciones de resguardo con medidas adicionales de seguridad, las cuales pueden ser consultadas con el Área de TI de la Institución.

5.6 Tratamiento de la Información según su clasificación y confidencialidad (TLP 2.0)

De acuerdo con los principios definidos en esta política y conforme a las buenas prácticas internacionales recogidas en las normas ISO/IEC 27001 e ISO/IEC 27002, todo activo de información del Hospital de Tomé debe ser tratado según

su clasificación de seguridad, incluyendo su estado (físico o digital) y nivel de confidencialidad conforme al esquema principal indicado en puntos anteriores y complementado con el Traffic Light Protocol cuando se tratase de información externa que se requiera precisar.

Este tratamiento implica la aplicación de medidas de seguridad en diferentes ámbitos del ciclo de vida de la información, tales como el almacenamiento, transmisión, duplicación, destrucción, acceso, etiquetado, entre otros. Las medidas deben ser proporcionales al nivel de confidencialidad asignado, con el fin de garantizar la protección contra accesos no autorizados, alteraciones o pérdidas.

5.6.1 TLP:ROJO (SECRETA)

La información clasificada como SECRETA requiere un nivel máximo de protección. Su almacenamiento deberá realizarse exclusivamente en medios digitales cifrados o en soportes físicos guardados en cajas fuertes o gabinetes con cerradura, accesibles únicamente por personal autorizado. Está prohibido copiarla o transmitirla, salvo autorización expresa del dueño del activo, y en tal caso deben emplearse medios institucionales con registro de trazabilidad, cifrado de extremo a extremo y autenticación robusta.

El envío por correo electrónico solo está permitido a través de cuentas institucionales con cifrado y previa autorización, mientras que el uso de redes públicas está restringido a conexiones mediante VPN autorizadas.

El uso de dispositivos portátiles, como USB o discos externos, deberá contar con cifrado y control de inventario. La destrucción de esta información debe realizarse mediante mecanismos certificados, como trituración física o borrado seguro conforme al estándar DoD 5220.22-M.

Los documentos físicos deberán estar claramente etiquetados con su clasificación, indicando destinatario y unidad responsable. El acceso, tanto físico como lógico, debe ser controlado, revisado periódicamente y contar con mecanismos de autenticación multifactor.

5.6.2 TLP:AMBAR+ESTRICTO (RESERVADA)

La información RESERVADA debe mantenerse en dispositivos institucionales protegidos mediante contraseñas de usuario individuales y autenticación segura. Se recomienda su cifrado, en especial si será almacenada en dispositivos móviles o compartida dentro de la red. El copiado está restringido al personal autorizado, y toda transmisión debe realizarse mediante medios institucionales con cifrado o autenticación, evitando canales no validados como redes sociales o aplicaciones personales.

Su almacenamiento en medios físicos debe realizarse en espacios seguros y con acceso limitado. El envío por correo electrónico es permitido solo desde cuentas institucionales a destinatarios autenticados. La destrucción deberá hacerse mediante métodos que impidan la recuperación de la información, como trituración o borrado seguro.

Todo documento o dispositivo deberá incluir su nivel de clasificación. El acceso a esta información debe ser registrado y supervisado por las jefaturas correspondientes.

5.6.3 TLP:AMBAR (USO INTERNO)

La información clasificada como USO INTERNO puede ser almacenada en computadores institucionales que cuentes con accesos personalizados, no siendo admisible su almacenamiento en dispositivos con cuentas genéricas. La encriptación es opcional, pero se recomienda para contenidos críticos. Su transmisión se permite mediante canales institucionales, como correo electrónico o sistemas de nube, siempre que estos cuenten con control de acceso.

Se permite su duplicación con fines operativos, evitando la proliferación innecesaria de copias. Los dispositivos digitales utilizados deben ser institucionales y mantenerse bajo resguardo. En cuanto a la destrucción, bastará con aplicar los mecanismos establecidos en las políticas internas del hospital.

Es recomendable etiquetas físicamente los documentos o medios que contengan este tipo de información, y los accesos deben revisarse de forma periódica, al menos semestralmente

5.6.4 TLP:VERDE (No Clasificada)

La clasificación **TLP:VERDE** corresponde a información oficial pública, pero cuya distribución está dirigida a una comunidad específica, como el personal del Hospital de Tomé, el Servicio de Salud Talcahuano u otras entidades del sector público con relación funcional o colaborativa. No está sujeta a confidencialidad estricta, pero su circulación debe realizarse bajo formatos controlados y con trazabilidad institucional.

Esta información puede ser compartida mediante medios oficiales (intranet, correos institucionales, cartelería interna, documentos firmados digitalmente), pero no puede ser modificada, distorsionada o redistribuida fuera de su contexto original sin autorización expresa del responsable del proceso.

- **Almacenamiento:** Permitido en recursos compartidos del Directorio Activo, nube institucional o medios físicos protegidos. No requiere cifrado, pero sí debe gestionarse con acceso personalizado y sin compartir mediante medios personales.
- **Copiado y transmisión:** Permitidos en el entorno institucional y a terceros autorizados. No se requiere cifrado, pero sí validación del medio y trazabilidad de su origen (por ejemplo, logos, pie institucional, versión y vigencia).
- **Correo electrónico:** Puede enviarse desde cuentas institucionales. Se recomienda evitar el reenvío masivo sin supervisión del área emisora.
- **Destrucción:** Se deben aplicar medios razonables de eliminación al finalizar su ciclo de vida (borrado digital, papelera, reciclado).
- **Etiquetado:** Se debe etiquetar su clasificación, la cual debe ser visible en el encabezado del documento.
- **Control de acceso:** Se gestiona en ambientes abiertos, pero con trazabilidad administrativa y claridad sobre la autoría.

5.6.5 TLP:BLANCO (No Clasificada)

La información clasificada como **TLP:BLANCO** corresponde a contenidos que no han sido objeto de clasificación formal como Secreta, Reservada o de Uso Interno, pero que forman parte del ecosistema institucional y, por tanto, deben ser gestionadas con resguardo mínimo y profesional. Puede incluir minutas de trabajo, agendas, borradores, documentos de circulación interna no oficial, información operativa no sensible, entre otros.

Si bien esta información no posee restricciones de confidencialidad específicas, podría evolucionar hacia un estado clasificado, por lo que su tratamiento requiere de

medidas proporcionales de resguardo, para evitar filtraciones, alteraciones indebidas o uso no autorizado.

- **Almacenamiento:** Permitido en dispositivos o nube institucionales, siempre bajo cuentas identificables y acceso personalizado. No se recomienda el uso de dispositivos personales o almacenamiento en medios no institucionales.
- **Copiado y transmisión:** Permitidos dentro del entorno institucional. No requiere cifrado, pero sí debe evitarse su distribución masiva innecesaria o su almacenamiento en dispositivos compartidos sin control, se debe representar a la imagen institucional.
- **Destrucción:** Se recomienda la eliminación segura mediante papelera digital, borrado lógico o eliminación física según aplique, especialmente si contiene antecedentes operativos acumulados.
- **Etiquetado y control de acceso:** No requiere etiquetado obligatorio, pero se recomienda como una buena práctica, pero debe gestionarse dentro de entornos institucionales con acceso autenticado. Su divulgación fuera del hospital debe contar con autorización del responsable del proceso si afecta la imagen institucional o involucra decisiones administrativas en curso.

5.6.6 Consideración sobre controles adicionales

Los controles descritos anteriormente constituyen las medidas mínimas requeridas para el tratamiento seguro de los activos de información del hospital. Sin perjuicio de ello, los Dueños de Proceso podrán establecer controles adicionales que estimen pertinentes, siempre que estos se encuentren alineados con la clasificación de la información, esta política y la normativa vigente. Dichos controles deberán ser proporcionales, documentados y evaluados en conjunto con el Encargado de Seguridad de la Información cuando se estime necesario.

5.6.7 Etiquetado y comunicación de la clasificación en soportes y medios

Para asegurar la correcta aplicación de las medidas de seguridad y el tratamiento adecuado de los activos de información, es fundamental identificar de forma clara el nivel de clasificación asignado, independiente del medio en que la información se encuentre almacenada, transmitida o expuesta. A continuación, se establecen las directrices mínimas para la etiquetación y comunicación del nivel de clasificación según el tipo de soporte o canal:

- **Documentos Electrónicos:** Todos los documentos electrónicos generados por la institución deben tener en cada una de sus páginas el nivel de clasificación del documento, el cual deberá ser concordante en todo el documento y deberá implementarse en un lugar visible (por ejemplo, encabezado).
- **Correo Electrónico:** Cuando se transmita información clasificada por este medio, el nivel de clasificación deberá indicarse en el asunto del correo. (por ejemplo, [Uso Interno] – Manual Organizacional)
- **Soportes de Almacenamiento Electrónico (como discos duros, pendrives, tarjetas de memoria, etc.):** Todo medio físico que contenga información clasificada deberá estar etiquetado de forma visible en su superficie externa, con la indicación clara del nivel de clasificación correspondiente.
- **Información Transmitida Oralmente:** En reuniones, conversaciones telefónicas u otros medios orales de comunicación institucional, el nivel de clasificación debe ser comunicado explícitamente antes de revelar el contenido de la información, especialmente si se trata de información Secreta, Reservada o de Uso Interno.
- **Activos de Información Impresos Sin Etiqueta:** En caso de encontrarse un documento impreso que no cuente con una etiqueta visible de clasificación y no indique su TLP, este deberá ser tratado provisionalmente como información No Clasificada en todos sus niveles de seguridad (Confidencialidad, Integridad y

Disponibilidad). Esta situación debe ser informada de inmediato al responsable de Información o Jefatura correspondiente, para que se aplique la clasificación adecuada y se adopten las salvaguardas necesarias conforme a esta política.

Estas medidas buscan garantizar que el personal del Hospital de Tomé cuente con información clara y accesible sobre la naturaleza de los activos que manipula, minimizando los riesgos de filtración, mal manejo o divulgación indebida.

6 MECANISMO DE DIFUSIÓN.

La comunicación de la presente política se efectuará de manera que el contenido de la documentación sea accesible y comprensible para todos los usuarios, a lo menos se deberá hacer difusión mediante los siguientes canales:

- Portal Mesa de Servicio TI, Sección Ayuda, Seguridad
- Correo Informativo.

7 PERÍODO DE REVISIÓN.

La presente política deberá ser revisada cada dos años o cuando ocurran cambios significativos para garantizar que:

- Sigue siendo adecuado para su propósito y preciso.
- Refleja los cambios en las tecnologías.
- Está alineado con legislación vigente, los estándares internacionales y mejores prácticas.

8 EXCEPCIONES AL CUMPLIMIENTO DE LA POLÍTICA

En situaciones excepcionales, el Jefe de TIC, el CISO o el Comité de Seguridad de la Información tendrán la facultad de evaluar y establecer condiciones específicas para la excepción al cumplimiento de las directrices establecidas en esta política, siempre que tales excepciones no infrinjan la legislación vigente ni comprometan la seguridad de la información.
Cada excepción deberá ser debidamente documentada, y se deberá iniciar un proceso de revisión de la política en el que se determinará si es necesario incorporar directrices adicionales o realizar modificaciones específicas.

9 HISTORIAL Y CONTROL DE VERSIONES

Versión	Fecha	Pág. o Sección modificada	Motivo del cambio