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

TOMÉ, 30 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 gestión de las relaciones con proveedores externos 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 contratación, supervisión, responsabilidades, obligaciones contractuales, acceso a información y seguridad de la información en relación con proveedores y personal externo.
3. Que la correcta aplicación de esta política asegura que los proveedores cumplan con las normativas, estándares ISO/IEC 27001:2022 y 27002:2022, y otros requerimientos legales y regulatorios, incluyendo la Ley N° 19.628, Ley N° 20.285, Ley N° 21.180, Ley N° 21.459, y Ley N° 21.663.
4. Que la presente política abarca a todos los funcionarios, personal a honorarios y terceros que interactúan con proveedores, así como al personal de empresas proveedoras que presta servicios en el Hospital de Tomé, asegurando el cumplimiento de controles de seguridad y buenas prácticas de ciberseguridad.
5. Que la implementación de esta política contribuye a formalizar los compromisos de seguridad en los contratos de proveedores, definir roles y responsabilidades, establecer niveles de servicio, auditoría y mecanismos de control, así como garantizar la correcta finalización de la relación contractual y la protección de activos de información.

RESUELVE EXENTA N° 2139

1. **APRUÉBASE** la Política de Gestión de Seguridad para las Relaciones con los Proveedores del Hospital de Tomé, que establece lineamientos, responsabilidades y procedimientos para la contratación, supervisión, auditoría y finalización de servicios

de proveedores externos, en concordancia con normas nacionales, estándares internacionales y buenas prácticas de seguridad de la información.

2. **DISPÓNGASE** que todos los proveedores, colaboradores y personal externo que preste servicios para el Hospital de Tomé cumplan estrictamente con los lineamientos establecidos en esta política, incluyendo:
    a) Requisitos de seguridad en productos y servicios.
    b) Cláusulas contractuales de seguridad de la información.
    c) Responsabilidades contractuales y sanciones por incumplimiento.
    d) Acuerdos de Nivel de Servicio (SLA) relativos a la seguridad.
    e) Certificación y auditoría de servicios contratados.
    f) Procedimientos de finalización de la relación contractual.
    g) Cumplimiento con la Política General de Seguridad de la Información.
    h) Uso apropiado de recursos, equipos y sistemas.
    i) Confidencialidad, protección de datos personales y propiedad intelectual.
    j) Intercambio seguro de información.
3. **ENCÁRQUESE** a la Jefatura de Abastecimiento, Administradores de Contratos y Encargado de Seguridad de la Información la supervisión, aplicación, monitoreo, y control de cumplimiento de la política, así como la gestión de incidentes, auditorías y medidas correctivas en caso de incumplimiento.
4. **DEJASE CONSTANCIA** que el personal de proveedores y cualquier colaborador externo deberá firmar un compromiso de adhesión a la política y cumplir con todos los lineamientos, directrices y procedimientos establecidos, reportando incidentes y asegurando la correcta gestión de los activos de información.
5. **ESTABLÉCESE** que la presente resolución entra en vigor a partir de su publicación, y 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 Recurso Físicos
- Área Gestión y Desarrollo de las Personas
- CR. Atención Cerrada
- CR. Atención Abierta
- CR. Emergencia

Firmado por Aníbal Antonio Cea Henríquez
Fecha 29/10/2025 17:58:01 CLST

POL03-25-0005

POLITICA DE SEGURIDAD PARA LAS RELACIONES CON LOS PROVEEDORES

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

Versión Oficial Actual 1 – Agosto 2025

CONTENIDO

1 PROPÓSITO.

La Política de Gestión de Seguridad para las Relaciones con los Proveedores establece un marco normativo para la contratación y gestión de servicios externos en el ámbito de la seguridad de la información, aplicable a los proveedores del Hospital de Tomé, así como a sus colaboradores y cualquier personal externo que desempeñe funciones en representación del Hospital. Su propósito es asegurar que todos los proveedores y personal externo, en el desempeño de sus actividades y acceso a la información, sistemas y recursos de la institución, cumplan con las normativas de seguridad, preservando la confidencialidad, integridad y disponibilidad de la información de la organización.

2 ALCANCE O ÁMBITO DE APLICACIÓN.

Esta política aplica a todas las actividades realizadas para el Hospital de Tomé por personal de empresas proveedoras, incluyendo aquellos servicios prestados a través de contratos de provisión de servicios. Comprende tanto el acceso a información y sistemas del Establecimiento como la interacción con cualquier recurso de la organización en el contexto de sus funciones, asegurando el cumplimiento de los estándares y controles de seguridad establecidos.

Esta política abarca los siguientes controles de Seguridad de la Información:

Alcance de Dominios y Controles de Seguridad de la Información		
Estándar	ID Control	Nombre del Control
ISO 27002:2022	5.19	Seguridad de la información en las relaciones con los proveedores
	5.20	Abordar la seguridad de la información dentro de los acuerdos de proveedores

3 MARCO NORMATIVO Y DOCUMENTOS RELACIONADOS.

- **Marco Normativo**
  - ISO 27001:2022 Tecnología de la información – Técnicas de seguridad – Sistemas de gestión de la seguridad de la información – Requisitos.
  - ISO 27002:2022 sobre Seguridad de la información, ciberseguridad y protección de la privacidad: controles de seguridad de la información.
  - El Marco Jurídico referido a los Sistemas de Seguridad de la Información (SSI), publicado en el portal del CSIRT del Ministerio del Interior.
- **Leyes relacionadas:**
  - Ley N° 19.628, de Protección de vida privada y datos personales.
  - Ley N° 19.799, de firmas y documentos electrónicos.

- Ley N° 19.880, que establece bases de los procedimientos administrativos que rigen los actos de la organización del Estado.
- 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, que establece directrices para la modernización de los procesos y servicios digitales en instituciones públicas. "Ley 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.
- Ley N° 21.663, que proporciona un marco para asegurar la ciberseguridad de infraestructuras críticas. "Ley Marco de Ciberseguridad".

- Decretos Supremos y Normas Internacionales de Seguridad de la Información y Ciberseguridad:
  - 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.
  - Decreto 273, de 2022, Ministerio del Interior, que establece la obligación de reportar incidentes de ciberseguridad a los organismos del Estado al CSIRT de gobierno.
  - El Decreto N° 533 establece el marco regulatorio en ciberseguridad para las instituciones públicas en Chile.
  - El Decreto Supremo N° 7 establece una Norma Técnica de Seguridad de la Información y Ciberseguridad, en concordancia con la Ley Nº 21.180 sobre Transformación Digital del Estado.

4 ROLES Y RESPONSABILIDADES

Jefe de Abastecimiento y Administradores de Contratos:

- Revisar y asegurar el cumplimiento de esta política, incluyendo la incorporación de cláusulas que obliguen el cumplimiento de la política de seguridad de la información del Hospital de Tomé en los contratos con proveedores externos.
- En todos los contratos se debe establecer la reserva del derecho de veto sobre el personal del proveedor que incumpla con las obligaciones de seguridad de la información que prevea el contrato y las políticas de seguridad del Hospital de Tomé, incluyendo las previstas en este instrumento.
- Prever normas de propiedad intelectual en los contratos que consideren la titularidad de las obras desarrolladas a nombre del Hospital de Tomé, salvo que se trate de Software o Infraestructura como servicio, la indemnidad del Hospital de Tomé frente a infracciones a derechos de terceros por parte del proveedor, entre otras.

- Aplicar a los proveedores, cuando proceda, las sanciones que corresponda, en el caso de infringirse los lineamientos de esta política,

División Jurídica:

- Revisar y asegurar que los contratos con proveedores incluyan cláusulas de confidencialidad, de seguridad de la información, y la consideración de un régimen infraccional por el incumplimiento de las obligaciones de resguardo de los datos y sistemas del Hospital de Tomé.
- Apoyar en la gestión de incidentes legales relacionados con incumplimientos de seguridad por parte de proveedores, colaborando en la elaboración de acciones legales o sanciones pertinentes.
- Garantizar que los acuerdos de servicio con terceros cumplan con las normativas y regulaciones legales vigentes, en especial aquellas relacionadas con la protección de datos y la ciberseguridad.

Proveedores:

- Cumplir y hacer cumplir estrictamente las normas de seguridad descritas en esta política, así como con los requisitos del Sistema de Gestión de Seguridad de la Información (SGSI) y el marco legal aplicable, sancionando a los infractores.
- Garantizar que todo el personal que emplee en la provisión de los servicios conoce y se encuentra obligado al cumplimiento de las obligaciones de seguridad de la información que se prevean en el contrato y en las políticas vigentes en el Hospital de Tomé.
- Reportar oportunamente a la Unidad de Seguridad de la Información cualquier incidente de seguridad de la información que pueda afectar la continuidad de los servicios comprometidos en el contrato, la seguridad de los datos y/o sistemas del Hospital de Tomé.

Personal Externo que Presta Servicios para el Hospital:

- Cumplir rigurosamente con las normas de seguridad especificadas en esta política, en la documentación del SGSI y en el marco normativo aplicable.

Usuarios Internos:

- El personal del Hospital de Tomé que interactúa con personal de proveedores debe adherirse estrictamente a las políticas y normas de seguridad pertinentes, considerando el perfil de cada proveedor y su nivel de acceso a los sistemas e información de la organización.

Encargado de Seguridad de la Información:

- Administrar y gestionar cualquier incidente de seguridad relacionado con incumplimientos de esta política y adoptar las acciones correctivas necesarias.

5 DIRECTRICES DE LA POLÍTICA:

5.1 Requisitos de seguridad en productos y servicios:

Establecer requisitos claros y específicos de ciberseguridad que deben cumplir los productos, sistemas, y servicios que se contraten a los proveedores. Estos requisitos estarán alineados con las políticas de seguridad de la información y ciberseguridad del Hospital de Tomé, así como con las cláusulas de seguridad incluidas en los contratos de TIC, los que se comunicarán de forma clara a todos los proveedores, distribuidores, colaboradores y socios comerciales involucrados.
Dichos requisitos incluirán estándares de seguridad específicos, normativas regulatorias, y cualquier otra medida de protección de la información acorde a los niveles de sensibilidad de los datos que manejarán, así como a los riesgos de los sistemas involucrados.

5.2 Cláusulas contractuales en materia de seguridad de la información:

Para formalizar compromisos en seguridad de la información y ciberseguridad, se establece la obligatoriedad de incluir **"Cláusulas de Protección de Datos y Seguridad de la Información para Contratos de Tecnologías"** en todos los contratos y convenios de tecnologías de la información. Estas cláusulas deben contemplar medidas de seguridad específicas, obligaciones de protección de datos y, en casos pertinentes, condiciones de privacidad. Se implementarán mecanismos de control y auditoría para monitorear el cumplimiento de estas cláusulas durante la ejecución de los contratos, permitiendo la identificación y gestión de cualquier desviación o incumplimiento. Además, se exigirá la notificación inmediata al Hospital de Tomé de cualquier incidente de seguridad relacionado, junto con un plan de acción correctiva.

5.3 Responsabilidades relativos a la seguridad:

Definir contractualmente la responsabilidad de cada proveedor en relación con todos los aspectos de seguridad requeridos para su función, incluyendo sanciones en caso de incumplimiento.
Los proveedores deben adherirse a las siguientes responsabilidades específicas:

- **Control de Acceso a Información Sensible:** Asegurar que solo el personal autorizado acceda a información sensible, mediante medidas de autenticación robustas y controles de acceso adecuados.
- **Realización y Gestión de Copias de Seguridad:** Establecer una política de respaldo de datos adecuada, incluyendo la periodicidad de las copias, el almacenamiento seguro de las mismas, pruebas funcionales recurrentes y un procedimiento claro para la recuperación de información en caso de incidente.
- **Supervisión y Control de Logs de Seguridad:** Configurar y mantener registros detallados (logs) de las actividades de acceso y operaciones

críticas en los sistemas del Hospital de Tomé. Estos registros deben estar sujetos a auditoría y conservarse conforme a los periodos requeridos por la normativa vigente.

- **Activación y Mantenimiento de Sistemas de Seguridad:** Asegurar la implementación y monitoreo continuo de sistemas de seguridad tales como antimalware, firewalls, y cifrado de comunicaciones. Estos sistemas deben mantenerse actualizados y en cumplimiento con las políticas de seguridad de la organización para prevenir y mitigar posibles vulnerabilidades.

5.4 Definir los Acuerdos de Nivel de Servicio (o SLA en inglés) relativos a la seguridad:

Para garantizar la calidad y las garantías del servicio adquirido, es fundamental establecer Acuerdos de Nivel de Servicio (SLAs) con los proveedores. Estos acuerdos deben especificar claramente las expectativas y los parámetros de rendimiento del servicio, y deben incluir, pero no limitarse a, los siguientes aspectos:

- **Tasas de Error Permitidas:** Definir el umbral aceptable de errores o fallos en el servicio, especificando métricas claras que permitan evaluar el desempeño del proveedor y su compromiso con la calidad.
- **Disponibilidad del Servicio:** Establecer un porcentaje de disponibilidad mínima del servicio, especificando las horas de operación y el tiempo máximo de inactividad permitido, así como las condiciones que se consideran excepciones a esta disponibilidad.
- **Tiempos de Respuesta y Resolución de Incidentes:** Definir los tiempos máximos de respuesta y resolución para diferentes tipos de incidentes, diferenciando entre incidentes críticos, mayores y menores, para asegurar que se manejen con la urgencia adecuada.
- **Definición de Canales de Contacto:** Especificar los canales oficiales a través de los cuales los usuarios pueden comunicarse con el proveedor, incluyendo teléfonos, correos electrónicos y plataformas de soporte, así como la disponibilidad de esos canales.
- **Proceso de Escalado y Notificación ante Incidentes:** Establecer un procedimiento claro para la escalación de incidentes que no se resuelven dentro de los tiempos establecidos, junto con los métodos de notificación requeridos para mantener informados a los usuarios sobre el estado del incidente.
- **Procedimientos para la Resolución de Problemas e Incidencias:** Detallar los pasos que el proveedor seguirá para resolver problemas e incidencias, incluyendo el diagnóstico inicial, la implementación de soluciones temporales, y el seguimiento para evitar que se repitan los problemas.

Estos SLAs deben ser revisados y acordados por ambas partes antes de la firma del contrato, y su cumplimiento será monitoreado de forma regular para garantizar la satisfacción del Hospital de Tomé y el mantenimiento de estándares de calidad en los servicios contratados.

Frente a dudas el Área de TI del Hospital de Tomé pone a disposición un servicio de **asesoría TI** que puede ser accedido desde la Mesa de Servicio TI.

5.5 Certificación de los servicios contratados:

Para servicios de alta criticidad (Definido en SGSI, Registro Clínico Electrónico, Sistema de Laboratorio, Sistema de Imagenología y Sistema de Directorio Activo), es fundamental exigir que los proveedores cuenten con certificaciones en gestión de la seguridad de la información. Estas certificaciones aseguran que el proveedor cumple con estándares reconocidos internacionalmente en calidad y seguridad, alineándose con las necesidades de Hospital de Tomé en cuanto a protección de activos de información institucionales.

Específicamente, se recomienda que los proveedores cuenten con certificaciones como ISO/IEC 27001 para la gestión de la seguridad de la información o equivalentes, que demuestren su compromiso con la confidencialidad, integridad, y disponibilidad de la información.

Además, los proveedores deberán garantizar la actualización periódica de estas certificaciones, conforme a los últimos estándares y mejores prácticas en seguridad.

Tratándose de servicios en la nube, se debe contar con certificaciones adicionales como SOC 2 o ISO/IEC 27017, que regulan la seguridad en ambientes de cloud computing.

Las certificaciones serán un requisito obligatorio en la selección de proveedores y deseable con puntaje en activos no críticos y deberán ser auditadas periódicamente para asegurar el cumplimiento continuo de los niveles de seguridad acordados.

5.6 Auditoría y control de los servicios contratados:

Con el fin de garantizar la calidad del servicio contratado en todo momento, es necesario establecer la factibilidad de monitorizar, revisar y auditar los aspectos relacionados con la ciberseguridad del servicio proporcionado por los proveedores. Esta práctica podría extenderse a lo largo de toda la cadena de suministro.

5.7 Finalización de la relación contractual:

Para preservar la seguridad de la información al término de un contrato, es esencial definir y ejecutar las siguientes acciones con el proveedor para garantizar la protección y correcta disposición de los activos y datos de Hospital de Tomé:

- **Devolución de Activos**: Inventariar y recuperar todos los activos físicos y digitales proporcionados al proveedor, incluyendo equipos, dispositivos de almacenamiento, documentación, y cualquier otro recurso asignado durante la relación contractual.

- **Eliminación de Permisos de Acceso**: Revocar todos los accesos a sistemas, redes, plataformas, y cualquier otro recurso del Hospital de Tomé a los que el proveedor o sus colaboradores hayan tenido acceso.
- **Borrado y Destrucción de Información Sensible**: Asegurar la eliminación segura y definitiva de toda la información sensible almacenada en los sistemas del proveedor, según los estándares de eliminación de datos seguros. Este proceso deberá estar documentado y ser verificable.
- **Migración de la Información**: Establecer un procedimiento de portabilidad de datos para transferir la información a un nuevo proveedor, garantizando la continuidad del servicio y la integridad de los datos.
- **Propiedad Intelectual**: Formalizar y aclarar la propiedad de todos los desarrollos, documentación, y cualquier otra creación intelectual producida durante la relación contractual, de acuerdo con los términos acordados, incluyendo derechos de autor y licencias de uso, si es aplicable.

5.8 Cumplimiento con la Política General de Seguridad de la Información del Hospital de Tomé:

Todo personal externo que preste servicios debe cumplir rigurosamente con la Política General de Seguridad de la Información y Ciberseguridad del Hospital de Tomé, acatando sus directrices y participando activamente en su implementación según sus funciones y competencias.

- **Responsabilidad en el Cumplimiento**: Los proveedores y colaboradores serán responsables por cualquier incumplimiento de las políticas y normas de seguridad de la información, tanto por parte de su personal directo como de subcontratistas. Esto incluye cumplir con todos los controles y medidas de seguridad establecidos en la política del Hospital de Tomé, independientemente del tipo de contrato o relación laboral.
- **Compromiso Documentado**: Se debe asegurar que todos los proveedores y colaboradores externos firmen un compromiso de adhesión a la Política General de Seguridad de la Información o en su defecto un Certificado de Confidencialidad que se deberá firmar antes del inicio de las funciones, en el que declaren conocer y aceptar las consecuencias en caso de incumplimiento.
- **Sanciones**: Las sanciones y medidas a aplicar en caso de incumplimientos serán definidas y aplicadas conforme a las condiciones contractuales y a la legislación vigente, asegurando que se tomen las acciones necesarias para mitigar cualquier riesgo asociado a violaciones de seguridad.

5.9 Prestación de servicios en Hospital de Tomé:

Los proveedores solo podrán realizar actividades para el Hospital de Tomé que estén formalmente amparadas en el contrato de provisión de servicios correspondiente. De este modo, todas las actividades desarrolladas por personal de empresas proveedoras se ajustarán estrictamente a los términos contractuales que vinculan al Hospital de Tomé con dichos proveedores.

- **Cumplimiento de Normas, Directrices, Políticas y Procedimientos**: El personal de empresas proveedoras deberá llevar a cabo sus actividades de acuerdo con lo estipulado en el contrato y siguiendo todas las normas y procedimientos de seguridad definidos por el Hospital de Tomé para la prestación del servicio.
- **Relación y Actualización del Personal**: La empresa proveedora presentará periódicamente al Hospital de Tomé una lista detallada del personal involucrado en la provisión de los servicios, sus perfiles, funciones y responsabilidades. Cualquier cambio, alta, baja, o reasignación de funciones deberá ser notificado de inmediato, manteniendo actualizada esta relación para asegurar la coherencia con los términos del contrato.
- **Derecho de Veto de Personal Infractor**: En caso de incumplimiento, el Hospital de Tomé se reserva el derecho de veto sobre el personal externo infractor y podrá imponer las sanciones pertinentes a la empresa proveedora.
- **Capacitación en Seguridad de la Información**: La empresa proveedora garantizará que todo su personal asignado al Hospital de Tomé cuenta con la formación y capacitación adecuada para el servicio provisto, tanto en conocimientos específicos como en prácticas generales de seguridad de la información. Se exigirá un compromiso explícito de cumplimiento de las Políticas de Seguridad del Hospital de Tomé.
- **Restricciones al uso de activos de Información**: Todo intercambio de información entre el establecimiento y los proveedores se entenderá como parte del contrato de servicios y estará restringido al cumplimiento de los fines específicos definidos en el contrato. Cualquier otro uso de la información está expresamente prohibido.
- **Definición de Activo de Información**: Para efectos de esta política, los activos de información incluyen no solo los datos, sino también las personas, activos intangibles como marcas, modelos, proyectos, la tecnología y el equipamiento que los respaldan. Esto garantiza que los recursos asociados al servicio están protegidos y operan de acuerdo con los lineamientos de seguridad establecidos.

5.10 Confidencialidad de la información:

El personal externo que tenga acceso a información del Hospital de Tomé debe asumir que toda información, por defecto, es confidencial (TLP:Ambar+Estricto – Política para la Clasificación y Manejo de la Información), salvo aquella expresamente divulgada a través de medios públicos oficiales del Hospital de Tomé.

Protección de Datos Confidenciales: Queda estrictamente prohibido que los proveedores revelen, modifiquen, destruyan, o usen indebidamente la información en cualquier formato, sin importar su soporte, sin autorización previa y expresa del Hospital de Tomé

Vigencia de las Obligaciones de Confidencialidad: Las obligaciones de confidencialidad y uso adecuado tendrán carácter indefinido y se mantendrán vigentes aun después de finalizadas las actividades del proveedor para el Hospital de Tomé, sin que sea lícita su difusión por el proveedor salvo autorización previa y expresa de Establecimiento.

Minimización y Protección de Informes en Papel: Los proveedores deberán reducir al mínimo los documentos en formato físico que contengan información confidencial, almacenándolos en áreas seguras y fuera del alcance de terceros.

Adopción de medidas de seguridad acordes a la criticidad del activo de información: La información debe ser clasificada según su nivel de sensibilidad, cumpliendo con los controles necesarios para preservar su integridad, disponibilidad y confidencialidad, en consistencia con la criticidad de la información. Ver Política para la Clasificación y Manejo de la Información del Hospital de Tomé.

Uso Temporal de Información Confidencial: El personal de la empresa proveedora que acceda temporalmente a información confidencial debido a sus funciones debe devolver todos los soportes que la contengan al finalizar sus tareas o la relación contractual con el Hospital de Tomé, sin ningún derecho de posesión, titularidad, o copia de la información.

Sanciones por Incumplimiento: El incumplimiento de cualquiera de estas obligaciones se sancionará conforme a la legislación vigente y a los términos contractuales estipulados.

Protección de Datos Personales:

Para proteger adecuadamente los Datos de Carácter Personal almacenados en sistemas electrónicos, el personal externo deberá cumplir con los siguientes lineamientos:

- **Creación y Destrucción de Ficheros Temporales**: Se permite la creación de archivos temporales con datos personales únicamente cuando sean necesarios para el trabajo. Estos ficheros no deben almacenarse en unidades locales y deben ser eliminados al concluir su finalidad específica.
- **Restricción de Almacenamiento Local**: No se permitirá el almacenamiento de datos personales en unidades locales de los equipos.
- **Control de Soportes de Datos Personales**: La salida de soportes que contengan datos personales fuera de las instalaciones debe estar autorizada por el responsable de la información. Estos soportes deben inventariarse, identificarse claramente y almacenarse en áreas de acceso restringido a personal autorizado. Toda información sensible debe estar protegida con clave y sistemas de encriptación.
- Lo anterior si no esta bajo el control de algún administrador TI, debe ser reportado al Encargado de Seguridad de la Información el cual podrá auditar cuando estime conveniente.

5.11 Propiedad intelectual:

Todo proveedor deberá dar estricto cumplimiento a los derechos de propiedad intelectual y garantizará el cumplimiento de las restricciones legales al uso del material protegido. Queda estrictamente prohibido el uso de programas informáticos que no cuenten con licencia. Asimismo, queda prohibido el uso, reproducción, cesión, transformación o comunicación pública de cualquier tipo de obra o invención protegida por la propiedad intelectual sin la debida autorización.

Consecuentemente, el incumplimiento de esta circunstancia no podrá acarrear ningún tipo de responsabilidad para el Hospital de Tomé, debiendo el proveedor hacerse cargo de cualquier reclamo que efectuaren terceros en esta materia.

Todos los bienes y activos de propiedad intelectual del proveedor se mantendrán bajo la titularidad, salvo acuerdo expreso y por escrito que disponga lo contrario. Sin embargo, las obras cuyo desarrollo encargue el Hospital de Tomé, serán de titularidad del establecimiento, debiendo constar esta circunstancia en los contratos respectivos. En el caso de que el proveedor contrate licencias de uso de programas computacionales, para la provisión de los servicios, deberá hacerlo a nombre del Hospital de Tomé y, una vez concluido este contrato, quedando prohibido al proveedor su uso posterior sin el consentimiento expreso de ésta.

Cualquier información que la institución contratante ponga a disposición del proveedor, ya sea en la fase de licitación, adjudicación o ejecución del contrato, se considerará de titularidad de la institución contratante y se regirá por lo dispuesto en el acápite de confidencialidad.

5.12 Intercambio de información:

Ninguna persona debe ocultar o manipular su identidad en ninguna circunstancia.

En relación con el intercambio de información dentro del marco del contrato de provisión de servicios que se suscriba con los proveedores, se considerarán no autorizadas las siguientes actividades:

- Transmisión o recepción de material protegido por derecho de autor, en infracción de la Ley de Protección Intelectual.
- Transmisión o recepción de toda clase de material pornográfico, mensajes o de una naturaleza sexual explícita, declaraciones discriminatorias raciales y cualquier otra clase de declaración o mensaje clasificable como ofensivo, denigrante o ilegal.
- Transferencia de ficheros a terceras partes no autorizadas de material de la Organización o material que es de alguna u otra manera confidencial.

- Transmisión o recepción de ficheros que infrinjan la normativa sobre protección de datos de carácter personal o directrices del Hospital de Tomé.
- Transmisión o recepción de juegos y/o aplicaciones no relacionadas con las actividades de Hospital de Tomé.
- Participación en actividades de Internet, como grupos de noticias, juegos u otras que no estén directamente relacionadas con el servicio, queda prohibida. El acceso a plataformas y sitios web que no estén relacionados con las funciones laborales y objetivos de la entidad/organización está sujeto a restricciones y no será tolerado durante el horario de trabajo.
- Todas las actividades que puedan dañar la buena reputación del Hospital de Tomé están prohibidas en Internet y en cualquier otro lugar.

Toda salida de información que contenga datos de carácter personal (tanto en soportes informáticos como en papel o por medios electrónicos) sólo podrá ser realizada por personal autorizado y con el debido permiso.
Si el tratamiento de datos de carácter personal se realiza fuera de las instalaciones del Hospital de Tomé, dicho tratamiento deberá contar con la autorización expresa del dueño o responsable del fichero. Además, se deberá garantizar en todo momento el nivel de seguridad correspondiente al tipo de información tratado.
La transmisión de datos de carácter personal, a través de redes de telecomunicaciones se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice la confidencialidad y trazabilidad, con el objetivo que la información no sea inteligible ni manipulada por terceros.

Lo anterior será auditable si se estima necesario, especialmente en los casos de activos críticos.

5.13 Uso apropiado de los recursos:

Todo contrato considerará la obligación de informar periódicamente al Hospital de Tomé sobre el nivel de cumplimiento de los estándares de seguridad de los activos con los que proporciona el servicio.

El proveedor se compromete a utilizar los recursos dispuestos para la provisión del servicio de acuerdo con las condiciones para las que fueron diseñados e implantados.

Los recursos que el Hospital de Tomé pone a disposición del personal externo, independientemente del tipo que sean (informáticos, datos, software, redes, sistemas de comunicación, etc.), están disponibles exclusivamente para el cumplimiento de las obligaciones y propósito de la operativa para la que fueron proporcionados. El Hospital de Tomé se reserva el derecho de implementar mecanismos de control y auditoría que verifiquen el uso apropiado de estos recursos.

Todos los equipos del proveedor que se conecten a la red de producción del Hospital de Tomé deberán ser de las marcas y modelos autorizados por el área de Tecnologías de la Información del Hospital de Tomé. El proveedor pondrá a disposición del Establecimiento dichos equipos para que este último les instale el software homologado y los configure adecuadamente.

Cualquier fichero introducido en la red del Hospital de Tomé o en cualquier equipo conectado a ella a través de soportes automatizados, Internet, correo electrónico o cualquier otro medio, deberá cumplir los requisitos establecidos en la normativa vigente, en las Políticas de Seguridad del Establecimiento y, en especial, las referidas a propiedad intelectual, protección de datos de carácter personal y protección contra programas maliciosos.

Al finalizar el contrato, el proveedor deberá restituir al Hospital de Tomé todos los activos físicos y destruir o restituir todos los activos de información, sin retraso injustificado. Además, todos los dispositivos electrónicos, como ordenadores personales en los que el Establecimiento haya instalado algún software, serán llevados al Área de TI del Hospital o Proveedor para formatear el disco duro al término del servicio prestado al Hospital de Tomé.
Se prohíbe expresamente:

- El uso de los recursos proporcionados por el Hospital de Tomé para actividades no relacionadas con el propósito del servicio.
- La conexión a la red de producción del Hospital de Tomé de equipos y/o aplicaciones que no estén especificados como parte del Software o de los Estándares de los Recursos Informáticos propios del Establecimiento o bajo supervisión del Área de Tecnologías de la Información del Hospital.
- Introducir en los Sistemas de Información o en la Red del establecimiento, contenidos obscenos, amenazadores, inmorales u ofensivos.
- Introducir voluntariamente en la red del Hospital de Tomé cualquier tipo de malware (programas, macros, applets, controles ActiveX, etc.), dispositivo lógico, dispositivo físico o cualquier otro tipo de secuencia de órdenes que causen o sean susceptibles de causar cualquier tipo de alteración o daño en los recursos informáticos lo que incluye elementos tipo Proxys. Todo el personal con acceso a la red del Hospital de Tomé tendrá la obligación de utilizar los programas antivirus y sus actualizaciones para prevenir la entrada en los Sistemas de cualquier elemento destinado a destruir o corromper los datos informáticos.
- Intentar obtener sin autorización explícita otros derechos o accesos distintos a aquellos que el Hospital de Tomé les haya asignado.
- Intentar acceder sin autorización explícita a áreas restringidas de los Sistemas de Información del Hospital de Tomé.
- Intentar distorsionar o falsear los registros "log" de los Sistemas de Información del Establecimiento.
- Intentar descifrar sin autorización explícita las claves, sistemas o algoritmos de cifrado y cualquier otro elemento de seguridad que intervenga en los procesos telemáticos del Hospital.

- Poseer, desarrollar o ejecutar programas que pudieran interferir sobre el trabajo de otros usuarios, dañar o alterar los Recursos Informáticos de la Institución.
- Intentar destruir, alterar, inutilizar o cualquier otra forma de dañar los datos, programas o documentos electrónicos de responsabilidad del Hospital de Tomé.

5.14 Responsabilidades del usuario:

Los proveedores de servicios deberán asegurarse de que todo el personal que desarrolla labores para el Hospital de Tomé respete los siguientes principios básicos dentro de su actividad informática:

- Cada persona con acceso a información del Establecimiento es responsable de la actividad desarrollada por su identificador de usuario y todo lo que de él se derive. Por lo tanto, es imprescindible que cada persona mantenga bajo control los sistemas de autenticación asociados a su identificador de usuario, garantizando que la clave asociada sea únicamente conocida por el propio usuario, no debiendo revelarse al resto del personal bajo ningún concepto.
- Los usuarios no deberán utilizar ningún identificador de otro usuario, aunque dispongan de la autorización del propietario.
- Los usuarios conocen y aplican los requisitos y procedimientos existentes en torno a la información manejada.
- Los usuarios no deberán conectarse a sistemas desde redes externas sin una razón justificable y que se encuentre debidamente documentada, previo al acceso.

Toda persona con acceso a información responsabilidad del Hospital de Tomé deberá seguir las directivas en relación con la gestión de las contraseñas, ver Política de Seguridad en la Identificación y autenticación de usuarios:

- Seleccionar contraseñas de alta calidad y robustez.
- Solicitar el cambio de la contraseña siempre que exista un posible indicio de compromiso del sistema o de las contraseñas.
- Cambiar las contraseñas periódicamente y evitar reutilizar o reciclar contraseñas antiguas.
- Cambiar las contraseñas por defecto y las temporales en el primer inicio de sesión ("login").
- Evitar incluir contraseñas en los procesos automatizados de inicio de sesión, por ejemplo, aquellas almacenadas en una tecla de función o macro.
- Notificar cualquier incidente de seguridad relacionado con sus contraseñas como pérdida, robo o indicio de pérdida de confidencialidad.
- Cualquier persona con acceso a información de responsabilidad del Hospital de Tomé deberá velar porque los equipos queden protegidos cuando vayan a quedar desatendidos.

Toda persona con acceso a información de responsabilidad del Hospital de Tomé deberá respetar al menos las siguientes instrucciones de escritorio limpio, con el fin de proteger los documentos en papel y dispositivos de almacenamiento removibles y reducir los riesgos de acceso no autorizado, pérdida y daño de la información, tanto durante el horario normal de trabajo como fuera del mismo:

- Almacenar bajo llave los documentos en papel y los medios informáticos con información de responsabilidad del Hospital de Tomé, en mobiliario seguro cuando no están siendo utilizados, especialmente fuera del horario de trabajo.
- No dejar desatendidos los equipos asignados a funciones críticas. Cuando sea necesario ausentarse, debe asegurarse de bloquear el acceso al equipo con la combinación de teclas Windows + L.
- Proteger, siempre que se utilice información bajo la responsabilidad del Hospital de Tomé los puntos de recepción y envío de información (correo postal, máquinas de scanner y fotocopiadoras), así como los equipos de duplicado (fotocopiadora y scanner) y los dispositivos de almacenamiento móvil (pendrives, discos ópticos y similares). La reproducción, envío o almacenamiento de información con estos dispositivos será de responsabilidad exclusiva del usuario.
- Retirar, sin retraso injustificado, cualquier información confidencial que sea de responsabilidad de un usuario, una vez impresa.
- Los listados con datos de carácter personal o información confidencial de responsabilidad del Hospital de Tomé deberán almacenarse en lugar seguro al que únicamente tengan acceso personal autorizado.
- Los listados con datos de carácter personal o información confidencial responsabilidad del Hospital de Tomé deberán eliminarse de manera segura una vez que no sean necesarios.
- Las personas con acceso a sistemas y/o información del Hospital de Tomé nunca deberán sin autorización explícita, realizar pruebas para detectar y/o utilizar una supuesta debilidad o incidente de seguridad, en caso de identificarse incidentes o debilidades que puedan suponerse relacionadas con la seguridad de la información. Para ello debe utilizarse el Procedimiento de Gestión de Incidentes de Seguridad de la Información.
- Se prohíbe la captura de tráficos de red por parte de los usuarios, salvo que se estén llevando a cabo tareas de auditoría expresamente autorizadas por el Área de TI del Hospital.
- Ningún dato de carácter personal responsabilidad de la Institución será almacenado en equipos o soportes de información personales de usuario, salvo autorización expresa del responsable del activo de información de que se trate.
- Todo el personal que acceda a la información y/o los sistemas de responsabilidad del Establecimiento deberá seguir las siguientes normas de actuación:
    - Proteger la información confidencial perteneciente o cedida por terceros al Hospital de toda revelación no autorizada, modificación, destrucción o uso incorrecto, ya sea accidental o no.

- Proteger todos los sistemas de información y redes de telecomunicaciones contra accesos o usos no autorizados, interrupciones de operaciones, destrucción, mal uso o robo.
- Contar con la autorización necesaria para obtener el acceso a los sistemas de información y/o la información accedidos.
- Conocer, aceptar y cumplir las Políticas de Seguridad del Hospital de Tomé antes de acceder a la información y/o los sistemas de la Institución.

5.15 Equipos de usuario:

Los proveedores de servicios deben garantizar que todo el equipamiento informático de usuario para acceder a información de responsabilidad del Hospital de Tomé cumple con las siguientes políticas:

- Ningún equipo de usuario dispondrá de herramientas que puedan transgredir el sistema de seguridad y las autorizaciones dentro de los sistemas de la organización.
- Los equipos de usuario se mantienen de acuerdo con las especificaciones del fabricante.
- Todos los equipos de usuario están adecuadamente protegidos frente a malware.

✓ El software antivirus se deberá instalar y usar en todos los ordenadores para reducir el riesgo operacional asociado con los virus u otro software malicioso.
✓ Se mantendrán al día con las últimas actualizaciones de seguridad disponibles.
✓ El software antivirus deberá estar siempre habilitado. Se establecerá una actualización automática de los ficheros de definición de virus.

Se velará especialmente por la seguridad de todos los equipos móviles de usuario que contengan información de responsabilidad del Hospital de Tomé o que permitan acceder a ella de algún modo:

- Adoptar precauciones adicionales al manejo de información fuera de las dependencias del Hospital de Tomé asegurándose de prevenir la visualización no autorizada por parte de terceros.
- Transportando los equipos en fundas, maletines o equipamiento similar que incorpore la apropiada protección frente a golpes.

5.16 Gestión de equipamiento “hardware”:

Los proveedores de servicios deberán asegurarse de que todos los equipos proporcionados por el Hospital de Tomé para la prestación de servicios, independientemente del tipo que sean, se gestionan apropiadamente. Para ello deberán cumplir las siguientes directrices:

- Siempre que un proveedor quiera reasignar algún equipo que haya contenido información de responsabilidad del Hospital de Tomé, deberá devolver temporalmente dicho activo al Área de TI del Establecimiento para que se realicen los procedimientos de borrado seguro necesarios de forma previa a su reasignación.
- En caso de que un proveedor cese en la prestación del servicio, deberá devolver al Área de TI del Hospital todos los equipos que le hayan sido entregado durante el periodo de servicio, tal y como establecen los correspondientes contratos de prestación de servicios. Sólo en el caso de activos de información el proveedor podrá proceder a su eliminación segura, en cuyo caso deberá notificar al Área de TI de dicha eliminación.

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 de la Mesa de Servicio TI
- 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
1			