POL03-26-0006

POLÍTICA DE TRABAJO A DISTANCIA

Sistema de Gobernanza de Tecnologías – Hospital de Tomé

Versión Oficial Actual 1 – julio 2026

Responsable		Fecha	Firma
Elaborado	César Cáceres Urrutia Jefe Área Tecnologías de la Información	27/07/2026	

Contenido

1 INTRODUCCIÓN

El Hospital de Tomé, en su calidad de establecimiento público de salud y Organismo de Importancia Vital (OIV), reconoce que el trabajo a distancia constituye una modalidad excepcional de prestación de servicios que puede resultar necesaria para asegurar la continuidad operacional, la disponibilidad de funciones críticas y la eficiencia institucional. Sin perjuicio de los beneficios que esta modalidad puede aportar, su implementación introduce riesgos específicos para la confidencialidad, integridad y disponibilidad de la información institucional, especialmente aquella relacionada con datos personales, datos sensibles y antecedentes clínicos de los usuarios.

En este contexto, la presente Política de Trabajo a Distancia establece los lineamientos de seguridad de la información que deberán observar todos los funcionarios, colaboradores y terceros autorizados que desarrollen funciones fuera de las dependencias institucionales, asegurando que el acceso, tratamiento, almacenamiento y transmisión de la información institucional se efectúe bajo condiciones adecuadas de seguridad y de conformidad con la normativa vigente.

Esta política se fundamenta en los principios establecidos en la Norma ISO/IEC 27001:2022, particularmente en el Control 6.7 "Trabajo a Distancia", el cual establece la necesidad de definir e implementar medidas de seguridad que permitan proteger la información cuando las actividades laborales se desarrollen fuera de las instalaciones de la organización. Asimismo, considera las obligaciones establecidas en la Ley Marco de Ciberseguridad N° 21.663 y su normativa complementaria, atendiendo especialmente a las responsabilidades que recaen sobre los Operadores de Importancia Vital respecto de la gestión de riesgos, resiliencia operacional, continuidad de los servicios esenciales y protección de los activos de información.

Las disposiciones contenidas en este documento complementan las políticas institucionales de Seguridad de la Información, Gestión de Accesos, Uso Aceptable de Activos, Gestión de Incidentes de Seguridad de la Información y Acceso Remoto, constituyendo un marco de cumplimiento obligatorio para toda persona autorizada a desempeñar funciones mediante trabajo a distancia.

2 PROPOSITO.

La presente Política de Trabajo a Distancia tiene por propósito establecer los principios, lineamientos y requisitos de seguridad de la información que regulan el acceso, uso y tratamiento de la información institucional cuando las funciones se desarrollen fuera de las dependencias del Hospital de Tomé, resguardando la confidencialidad, integridad, disponibilidad y trazabilidad de los activos de información institucionales.

Esta política busca garantizar que las distintas modalidades de trabajo a distancia autorizadas por el Hospital de Tomé se desarrollen bajo condiciones adecuadas de ciberseguridad, gestión de riesgos y continuidad operacional, minimizando la exposición a amenazas derivadas del acceso remoto a plataformas, sistemas clínicos, sistemas administrativos e infraestructura tecnológica institucional.

Para efectos de esta política, se consideran comprendidas las siguientes modalidades institucionales de trabajo a distancia:

- **Teletrabajo**: modalidad formal autorizada por la autoridad competente, mediante la cual un funcionario desempeña total o parcialmente su jornada laboral desde un lugar distinto de las dependencias institucionales, conforme a la normativa vigente y a los actos administrativos que la regulen.
- **Hospital Digital**: modalidad asistencial que permite la prestación de servicios clínicos mediante plataformas tecnológicas institucionales autorizadas, incluyendo actividades de atención remota, telemedicina u otras prestaciones digitales definidas por el Ministerio de Salud o el Servicio de Salud Talcahuano.
- **Gestión Administrativa Remota**: modalidad destinada a permitir el acceso remoto a recursos tecnológicos institucionales para la ejecución de actividades específicas de carácter administrativo, técnico, operativo o de soporte, principalmente fuera de la jornada ordinaria de trabajo o frente a contingencias operacionales, sin que ello constituya una modalidad de teletrabajo ni implique el reemplazo de la jornada laboral presencial, este apartado es aplicable a su vez a las operaciones que pueda realizar la Unidad de Hospitalización Domiciliaría del establecimiento.

La presente política constituye el marco institucional que establece las medidas mínimas de seguridad aplicables a todas las modalidades de trabajo a distancia, sin perjuicio de las disposiciones particulares que puedan establecer otras políticas institucionales, procedimientos operacionales, actos administrativos o instrucciones emitidas por el Hospital de Tomé, el Servicio de Salud Talcahuano o el Ministerio de Salud.

3 OBJETIVO ESTRATÉGICO

Establecer un marco institucional de gobernanza para el trabajo a distancia que permita habilitar el acceso remoto seguro a la información, sistemas y servicios del Hospital de Tomé, garantizando la protección de los activos de información, la continuidad de las funciones críticas, la resiliencia operacional y el cumplimiento del marco normativo vigente, en concordancia con los objetivos del Sistema de Gestión de Seguridad de la Información (SGSI) y las obligaciones aplicables a los Operadores de Importancia Vital (OIV).

Para el cumplimiento de este objetivo estratégico, el Hospital de Tomé promoverá que todas las modalidades de trabajo a distancia se desarrollen bajo un enfoque de gestión de riesgos, aplicando controles técnicos, administrativos y organizacionales que permitan:

- Proteger la confidencialidad, integridad, disponibilidad y trazabilidad de la información institucional y de los datos personales y sensibles tratados durante el trabajo a distancia.
- Reducir los riesgos de ciberseguridad asociados al acceso remoto a plataformas, sistemas clínicos, sistemas administrativos y demás activos tecnológicos institucionales.
- Asegurar que los accesos remotos sean autorizados, controlados, monitoreados y auditables, conforme a las políticas institucionales de seguridad de la información.

- Fortalecer la continuidad operacional de los procesos clínicos, asistenciales, administrativos y de soporte que requieran acceso remoto a recursos institucionales.
- Cumplir los requisitos establecidos en la ISO/IEC 27001:2022, la Ley Marco de Ciberseguridad N° 21.663 y demás normativa aplicable en materia de seguridad de la información, protección de datos y resiliencia operacional.
- Fomentar una cultura institucional de ciberseguridad y responsabilidad en el uso de los recursos tecnológicos durante el desarrollo de actividades fuera de las dependencias del establecimiento.

4 ALCANCE O AMBITO DE APLICACIÓN.

La presente Política de Trabajo a Distancia es de aplicación obligatoria para todos los funcionarios, directivos, jefaturas, colaboradores, prestadores de servicios, estudiantes, internos, becarios y terceros que, previa autorización institucional, accedan, procesen, almacenen o transmitan información del Hospital de Tomé desde una ubicación distinta a las dependencias institucionales, utilizando recursos tecnológicos institucionales o personales autorizados.

Las disposiciones contenidas en esta política serán aplicables a todas las modalidades de trabajo a distancia implementadas o autorizadas por el Hospital de Tomé, incluyendo:

- **Teletrabajo**, conforme a la normativa vigente y a los actos administrativos que lo autoricen.
- **Hospital Digital**, para el desarrollo de prestaciones asistenciales mediante plataformas tecnológicas institucionales habilitadas.
- **Gestión Administrativa Remota**, destinada a la ejecución de actividades específicas de soporte, administración, continuidad operacional, mantenimiento, monitoreo, respuesta ante incidentes, contingencias u otras funciones autorizadas que requieran acceso remoto a los recursos institucionales, sin constituir una modalidad de teletrabajo.

Esta política comprende el uso de todos los activos de información que puedan ser utilizados durante el trabajo a distancia, incluyendo, entre otros:

- Equipos computacionales institucionales y dispositivos personales autorizados.
- Equipos móviles institucionales.
- Redes privadas virtuales (VPN) y demás mecanismos de acceso remoto autorizados.
- Plataformas clínicas, administrativas y de apoyo a la gestión.
- Servicios en la nube autorizados institucionalmente.
- Correo electrónico institucional, herramientas de colaboración y comunicación.
- Bases de datos, documentos electrónicos, registros clínicos, datos personales, datos sensibles y demás información institucional.

Las disposiciones establecidas en este documento deberán observarse durante toda la vigencia del acceso remoto autorizado, independientemente del lugar físico desde el cual se desarrollen las actividades, incluyendo domicilios particulares, dependencias de otras instituciones públicas, establecimientos de salud, centros asistenciales, lugares de comisión de servicio u otras ubicaciones previamente autorizadas por el Hospital de Tomé.

Quedan excluidas del alcance de esta política aquellas actividades que no impliquen acceso, procesamiento o tratamiento de información institucional mediante recursos tecnológicos del Hospital de Tomé, sin perjuicio del cumplimiento de las demás políticas institucionales que resulten aplicables.

5 MARCO NORMATIVO Y DOCUMENTOS RELACIONADOS

La presente Política de Trabajo a Distancia se sustenta en el siguiente marco normativo y regulatorio, el cual establece las obligaciones legales, técnicas y administrativas aplicables a la protección de la información, la ciberseguridad, la continuidad operacional y el acceso remoto a los sistemas institucionales del Hospital de Tomé:

5.1 NORMATIVA LEGAL

- **Ley N° 18.834**, sobre Estatuto Administrativo.
- **Ley N° 20.285**, sobre Acceso a la Información Pública.
- **Ley N° 20.584**, que regula los derechos y deberes que tienen las personas en relación con acciones vinculadas a su atención en salud.
- **Ley N° 21.180**, de Transformación Digital del Estado.
- **Ley N° 21.459**, que establece normas sobre Delitos Informáticos.
- **Ley N° 21.663**, Ley Marco de Ciberseguridad, que establece obligaciones para los organismos públicos y los Operadores de Importancia Vital (OIV).
- **Ley N° 21.719**, sobre Protección y Tratamiento de Datos Personales.

5.2 REGLAMENTOS Y NORMATIVA SECTORIAL

- **Decreto Supremo N° 273**, que establece la obligación de reportar incidentes de ciberseguridad.
- **Decreto Supremo N° 285 de 2022**, del Ministerio del Interior y Seguridad Pública, que aprueba el Reglamento sobre Operadores de Importancia Vital (OIV) y los criterios de calificación de Prestadores de Servicios Esenciales.
- **Resolución Exenta N° 50 de 2025**, de la Agencia Nacional de Ciberseguridad (ANCI), mediante la cual el Hospital de Tomé es incorporado en la nómina preliminar de Operadores de Importancia Vital.

5.3 NORMATIVA INSTITUCIONAL Y SECTOR SALUD

- **Política de Teletrabajo del Ministerio de Salud (MINSAL)**.

- **Resolución Exenta N° 754 de 2026**, y sus modificaciones, en lo que resulte aplicable al trabajo a distancia en el sector salud.
- **Resolución N° 1924,** de fecha 20 de julio de 2026, de la Dirección del Servicio de Salud Talcahuano, que aprueba la Política Institucional de Acceso Remoto a Plataformas Institucionales del Servicio de Salud Talcahuano, estableciendo los principios, requisitos y controles para el acceso remoto seguro a los recursos tecnológicos institucionales.
- Políticas, normas, procedimientos e instructivos vigentes del Hospital de Tomé relacionados con Seguridad de la Información, Ciberseguridad, Gestión de Accesos, Gestión de Activos, Gestión de Incidentes y Continuidad Operacional.

5.4 NORMAS Y BUENAS PRÁCTICAS INTERNACIONALES

- **ISO/IEC 27001:2022**, Sistemas de Gestión de Seguridad de la Información (SGSI), con especial consideración del **Control 6.7 "Trabajo a Distancia"**, y demás controles relacionados con la protección de los activos de información, el control de accesos y la seguridad de las operaciones.
- **ISO/IEC 27002:2022**, Código de buenas prácticas para los controles de seguridad de la información, como guía para la implementación de medidas de seguridad aplicables al trabajo a distancia.
- **Protocolo de Seguridad para el Trabajo a Distancia**, emitido por el Equipo de Respuesta ante Incidentes de Seguridad Informática del Gobierno de Chile (CSIRT), como referencia para la adopción de medidas de ciberseguridad en entornos de trabajo remoto.

6 ROLES Y RESPONSABILIDADES

Con el objeto de asegurar una adecuada gestión del trabajo a distancia, las responsabilidades para la autorización, implementación, administración, supervisión y control de los accesos remotos se distribuyen de acuerdo con las competencias de cada unidad organizacional.

6.1 DIRECCIÓN DEL HOSPITAL

Corresponde a la Dirección del Hospital de Tomé:

- Aprobar la presente política y sus modificaciones.
- Velar por el cumplimiento del marco normativo aplicable.
- Promover la disponibilidad de los recursos necesarios para la implementación de controles de seguridad asociados al trabajo a distancia.
- Resolver las situaciones excepcionales que requieran autorización de la Dirección, cuando corresponda.

6.2 UNIDAD DE CALIDAD DE VIDA LABORAL

Corresponde a la Unidad de Calidad de Vida Laboral:

- Administrar el proceso institucional de solicitudes de Teletrabajo.
- Coordinar el funcionamiento de la Comisión de Evaluación de Teletrabajo.
- Mantener los registros de las solicitudes formalizadas por los funcionarios.
- Recepcionar los informes técnicos que correspondan para la evaluación de final.
- Mantener el registro de las autorizaciones, renovaciones, suspensiones y términos de las modalidades de Teletrabajo.
- Comunicar formalmente las resoluciones adoptadas a las unidades involucradas.

6.3 COMISIÓN DE EVALUACIÓN DE TELETRABAJO

Corresponde a la Comisión:

- Evaluar las solicitudes de Teletrabajo considerando criterios técnicos, operacionales, administrativos y de continuidad del servicio.
- Analizar los antecedentes presentados por el funcionario y su jefatura.
- Resolver favorable o desfavorablemente las solicitudes, dejando constancia de los fundamentos de la decisión.
- Establecer condiciones particulares cuando resulte necesario para resguardar la seguridad de la información o la continuidad operacional.

6.4 JEFATURAS DE SERVICIO

Las jefaturas serán responsables de:

- Justificar la necesidad funcional del trabajo a distancia.
- Autorizar las solicitudes de **Gestión Administrativa Remota**, cuando las funciones requieran acceso excepcional a recursos tecnológicos institucionales fuera de la jornada ordinaria o ante contingencias operacionales.
- Supervisar que las actividades desarrolladas mediante trabajo a distancia se ejecuten conforme a las funciones autorizadas.
- Informar oportunamente cuando dejen de existir las condiciones que justificaron el acceso remoto, solicitando su modificación o revocación.

6.5 JEFATURA DEL CONSULTORIO ADOSADO DE ESPECIALIDADES (CAE)

Corresponde a la Jefatura del CAE:

- Evaluar la pertinencia asistencial de las solicitudes relacionadas con la modalidad de **Hospital Digital**.
- Otorgar los vistos buenos para la habilitación de prestaciones clínicas remotas, verificando que se ajusten a los lineamientos establecidos por el Ministerio de Salud y el Servicio de Salud Talcahuano.
- Coordinar con la Unidad de Operaciones TI la habilitación de los accesos tecnológicos requeridos.

6.6 UNIDAD DE OPERACIONES TI

Corresponde a la Unidad de Operaciones TI:

- Evaluar la factibilidad técnica de las solicitudes de trabajo a distancia mediante el servicio institucional definido en el Catálogo de Servicios TI, disponible en Portal de Centro de Servicio TI.
- Verificar que el funcionario cumpla con los requisitos técnicos mínimos para acceder de forma remota a los recursos institucionales.
- Implementar, modificar, suspender y revocar los accesos remotos autorizados.
- Administrar las plataformas tecnológicas de acceso remoto, incluyendo VPN, autenticación, equipos institucionales y demás mecanismos autorizados.
- Mantener registros de las habilitaciones realizadas y de los cambios efectuados sobre los accesos remotos.
- Brindar soporte técnico asociado a las modalidades de trabajo a distancia, si existe factibilidad.

6.7 UNIDAD DE SEGURIDAD DE LA INFORMACIÓN

Corresponde a la Unidad de Seguridad de la Información:

- Definir los controles de seguridad aplicables al trabajo a distancia.
- Supervisar el cumplimiento de la presente política y de las demás políticas institucionales de seguridad de la información.
- Auditar periódicamente los procesos de autorización, habilitación y uso de accesos remotos.
- Monitorear el cumplimiento de los controles de ciberseguridad asociados al trabajo a distancia.
- Emitir recomendaciones y planes de mejora cuando se detecten incumplimientos o desviaciones.
- Coordinar la gestión de incidentes de seguridad de la información relacionados con accesos remotos, cuando corresponda.

6.8 FUNCIONARIOS Y USUARIOS AUTORIZADOS

Toda persona autorizada para desarrollar actividades mediante trabajo a distancia será responsable de:

- Cumplir íntegramente la presente política y la normativa institucional aplicable.
- Utilizar exclusivamente los mecanismos de acceso remoto autorizados por el Hospital.
- Proteger las credenciales de acceso y mantener la confidencialidad de la información institucional.
- Resguardar los equipos y dispositivos utilizados durante el trabajo a distancia.
- Informar inmediatamente a la Mesa de Ayuda TI y a la Unidad de Seguridad de la Información cualquier incidente, pérdida, robo, acceso no autorizado o sospecha de compromiso de la información.
- Abstenerse de instalar software no autorizado o utilizar servicios tecnológicos que no hayan sido aprobados institucionalmente.
- Permitir las actividades de monitoreo, auditoría y verificación que el Hospital estime necesarias para garantizar el cumplimiento de la presente política.

6.9 RESPONSABILIDAD COMPARTIDA

La autorización para desarrollar actividades mediante trabajo a distancia no exime a los funcionarios ni a sus jefaturas de las responsabilidades administrativas, legales y disciplinarias derivadas del uso de la información institucional y de los recursos tecnológicos del Hospital de Tomé. Todas las unidades participantes deberán actuar de manera coordinada para garantizar la protección de los activos de información, la continuidad operacional y el cumplimiento de las obligaciones establecidas para los Operadores de Importancia Vital (OIV).

7 DIRECTRICES DE LA POLÍTICA

7.1 PRINCIPIOS GENERALES DEL TRABAJO A DISTANCIA

Toda modalidad de trabajo a distancia autorizada por el Hospital de Tomé deberá desarrollarse conforme a los principios establecidos en la presente política, con el propósito de resguardar la seguridad de la información, la continuidad operacional de los servicios institucionales y el cumplimiento de las obligaciones legales y regulatorias aplicables.

7.1.1 PRINCIPIOS DE PROTECCIÓN DE LA INFORMACIÓN

Toda información institucional tratada durante el trabajo a distancia deberá resguardarse de manera que se preserve su confidencialidad, integridad, disponibilidad y trazabilidad, aplicando las medidas de seguridad definidas por el Hospital de Tomé.

7.1.2 PRINCIPIO DE RESPONSABILIDAD INDIVIDUAL

Toda persona autorizada para desempeñar funciones mediante trabajo a distancia será responsable del uso adecuado de los activos de información, de las credenciales de acceso asignadas y del cumplimiento de la presente política, así como de las demás normas institucionales relacionadas con seguridad de la información y ciberseguridad.

7.1.3 PRINCIPIO DE MÍNIMO PRIVILEGIO

Los accesos remotos deberán otorgarse únicamente respecto de los sistemas, aplicaciones, servicios y recursos tecnológicos estrictamente necesarios para el cumplimiento de las funciones autorizadas, limitándose al nivel mínimo de privilegios requerido para el desempeño de las labores.

7.1.4 PRINCIPIO DE NECESIDAD DE CONOCER

El acceso a información institucional estará limitado exclusivamente a aquella que resulte indispensable para el ejercicio de las funciones autorizadas, conforme a las responsabilidades del cargo y a las autorizaciones otorgadas por la autoridad competente.

7.1.5 PRINCIPIO DE GESTIÓN DE RIESGOS

Toda modalidad de trabajo a distancia deberá implementarse considerando los riesgos de seguridad de la información asociados al acceso remoto, adoptando controles técnicos, administrativos y organizacionales proporcionales al nivel de riesgo identificado.

7.1.6 PRINCIPIO DE CONTINUIDAD OPERATIVA

El trabajo a distancia deberá contribuir al mantenimiento de la continuidad de los procesos asistenciales, administrativos y de soporte del Hospital de Tomé, sin comprometer la disponibilidad, estabilidad o resiliencia de los servicios institucionales.

7.1.7 PRINCIPIO DE CUMPLIMIENTO NORMATIVO

Las actividades desarrolladas mediante trabajo a distancia deberán ajustarse a la legislación vigente, a las políticas institucionales, a los procedimientos internos y a los estándares de seguridad de la información adoptados por el Hospital de Tomé, especialmente aquellos derivados de su condición de Operador de Importancia Vital (OIV).

7.1.8 PRINCIPIO DE USO EXCLUSIVAMENTE INSTITUCIONAL

Los mecanismos de acceso remoto, los recursos tecnológicos y la información institucional autorizados para el trabajo a distancia deberán utilizarse exclusivamente para el cumplimiento de funciones propias del Hospital de Tomé. Queda prohibido su uso para fines personales, comerciales o cualquier otra actividad ajena al ejercicio de las funciones institucionales.

7.1.9 PRINCIPIO DE DEFENSA EN PROFUNDIDAD

El acceso remoto a los activos de información deberá protegerse mediante múltiples controles de seguridad complementarios, incluyendo mecanismos de autenticación, control de accesos, protección de dispositivos, monitoreo, registro de actividades y demás medidas técnicas que determine el Hospital de Tomé.

7.1.10 PRINCIPIO DE MEJORA CONTINUA

Las medidas de seguridad aplicables al trabajo a distancia serán objeto de revisión y actualización periódica, considerando la evolución de las amenazas de ciberseguridad, los cambios tecnológicos, las modificaciones normativas, los resultados de auditorías, la gestión de incidentes y el proceso de mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI).

7.2 MODALIDADES DE TRABAJO A DISTANCIA

El Hospital de Tomé reconoce distintas modalidades de trabajo a distancia, las cuales responden a necesidades funcionales, asistenciales, operacionales y de continuidad del servicio. Todas ellas deberán cumplir los requisitos establecidos en la presente política y en las demás normas institucionales relacionadas con seguridad de la información, acceso remoto y ciberseguridad.

La autorización de una modalidad de trabajo a distancia no implicará, por sí sola, la habilitación de accesos remotos a los sistemas institucionales, los cuales deberán ser evaluados, autorizados e implementados conforme a los procedimientos y controles definidos por el Hospital de Tomé.

7.2.1 TELETRABAJO

Corresponde a la modalidad mediante la cual un funcionario autorizado desempeña total o parcialmente su jornada laboral desde un lugar distinto de las dependencias institucionales, conforme a la normativa vigente y a los actos administrativos que regulan esta modalidad.

La autorización de Teletrabajo deberá ser evaluada por la Comisión de Teletrabajo, considerando los antecedentes administrativos, operacionales y técnicos correspondientes, previo informe de factibilidad emitido por la Unidad de Operaciones TI.

7.2.2 HOSPITAL DIGITAL

Corresponde a la modalidad destinada a la prestación de servicios asistenciales mediante plataformas tecnológicas institucionales autorizadas, permitiendo la ejecución de atenciones clínicas remotas, telemedicina y demás prestaciones definidas por el Ministerio de Salud, el Servicio de Salud Talcahuano o el Hospital de Tomé.
Las solicitudes relacionadas con Hospital Digital deberán contar con la evaluación y visto bueno de la Jefatura del Consultorio Adosado de Especialidades (CAE), sin perjuicio del cumplimiento de los requisitos técnicos y de seguridad establecidos para el acceso remoto.

7.2.3 GESTIÓN ADMINISTRATIVA REMOTA

Corresponde a la modalidad que habilita el acceso remoto a plataformas y recursos tecnológicos institucionales para la ejecución de actividades específicas de carácter administrativo, técnico, operativo o de soporte, cuya naturaleza requiera ser realizada fuera de las dependencias institucionales o fuera de la jornada ordinaria de trabajo.

Esta modalidad no constituye Teletrabajo ni reemplaza la jornada laboral presencial, teniendo por finalidad facilitar actividades tales como soporte tecnológico, monitoreo de plataformas, respuesta a incidentes, continuidad operacional, mantenimiento programado, labores administrativas extraordinarias u otras funciones previamente autorizadas por la jefatura correspondiente.

Las autorizaciones para Gestión Administrativa Remota deberán ser otorgadas por la jefatura del servicio o unidad solicitante, previa evaluación técnica de la Unidad de Operaciones TI cuando corresponda.

7.2.4 MODALIDADES EXCEPCIONALES

Excepcionalmente, la Dirección del Hospital podrá autorizar modalidades de trabajo a distancia distintas a las señaladas precedentemente, cuando existan razones fundadas de continuidad operacional, contingencias institucionales, emergencias sanitarias, ciberincidentes u otras circunstancias que así lo justifiquen.

En estos casos, deberán implementarse los controles de seguridad de la información que determine la Unidad de Operaciones TI y la Unidad de Seguridad de la Información, de acuerdo con la evaluación de riesgos realizada para cada situación.

7.2.5 REGLAS COMUNES

Independientemente de la modalidad autorizada, todo trabajo a distancia deberá cumplir, como mínimo, las siguientes condiciones:

a) Contar con autorización formal de la autoridad competente.
b) Utilizar exclusivamente mecanismos de acceso remoto autorizados por el Hospital de Tomé.
c) Cumplir los controles de seguridad establecidos en la presente política y en las demás políticas institucionales relacionadas.
d) Mantener la confidencialidad de la información institucional, especialmente aquella clasificada como reservada, confidencial o que contenga datos personales, datos sensibles o información clínica.
e) Estar sujeto a monitoreo, auditoría y revisión por parte de las unidades competentes, conforme a la normativa institucional vigente.
f) Ser suspendido o revocado cuando desaparezcan las condiciones que justificaron su autorización o cuando se detecten incumplimientos a la presente política.

7.3 AUTORIZACIÓN DEL TRABAJO A DISTANCIA

Toda modalidad de trabajo a distancia deberá contar con autorización formal previa y cumplir el procedimiento institucional establecido por el Hospital de Tomé. Ningún funcionario podrá acceder remotamente a plataformas institucionales sin que exista una autorización vigente y la correspondiente habilitación técnica efectuada por la Unidad de Operaciones TI.

Todas las solicitudes deberán gestionarse a través del Catálogo de Servicios TI. En caso de indisponibilidad de la plataforma o existir dificultades técnicas que impidan el ingreso de la solicitud, el requerimiento podrá efectuarse excepcionalmente mediante la Mesa de Servicio, al anexo institucional **+56 41 2725016**, debiendo posteriormente regularizarse el registro correspondiente.

7.3.1 AUTORIZACIÓN DE TELERABAJO

Las solicitudes de Teletrabajo deberán seguir el siguiente proceso:

a) El funcionario ingresará la solicitud de servicio utilizando el catalogo de servicio del Centro de Servicio TI, Categoría "Comunicación y Colaboración", servicio "Trabajo a Distancia"
b) La Unidad de Operaciones TI realizará la evaluación técnica, verificando la factibilidad del acceso remoto, la disponibilidad de equipamiento institucional u homologación de equipo personal (si aplica) y el cumplimiento de los requisitos de seguridad definidos en la presente política.
c) Emitido el informe técnico favorable, éste será remitido a la Unidad de Calidad de Vida Laboral como antecedente para su futura incorporación al proceso de evaluación por parte de la Comisión de Teletrabajo y se responde con copia al solicitante, la fecha de cierre del ticket deberá ser modificada para un máximo de 30 días y quedará en estado "Abierto" a la espera de la respuesta de la comisión.
d) La Comisión resolverá la aprobación o rechazo de la solicitud conforme a sus atribuciones.
e) Una vez autorizada la modalidad, la Comisión deberá enviar el o los certificados utilizando el correo de notificación anterior, lo que permitirá al equipo de Operaciones TI utilizar el catálogo de servicio y realizar las solicitudes de VPN para cada funcionario autorizado al Trabajo a Distancia, generando estos tickets como hijos del ticket original de solicitud. Esto se debe realizar para cada solicitud.

Nota: Es clave que los datos ingresados sean los correctos, dado que a todo evento las comunicaciones futuras, entrega de claves y asistencias serán al usuario final (funcionario).

Nota Adicional: Este servicio de soporte y evaluación técnica solo será válido durante los procesos formales de solicitud de teletrabajo convocados y publicados oficialmente por la Unidad de Calidad de Vida Laboral. No se aceptarán ni gestionarán solicitudes fuera de dichos periodos habilitados, procediendo al cierre y rechazo automático de cualquier requerimiento ingresado extemporáneamente. Lo anterior tiene como objetivo resguardar los plazos operativos (SLA) de la Mesa de Ayuda TI frente a postulaciones anticipadas o fuera de temporada.

7.3.2 AUTORIZACIÓN PARA HOSPITAL DIGITAL

Las solicitudes relacionadas con Hospital Digital deberán cumplir el siguiente procedimiento:

a) El funcionario ingresará la solicitud de servicio utilizando el catálogo de servicio del Centro de Servicio TI, Categoría "Comunicación y Colaboración", servicio "Trabajo a Distancia", utilizando la opción de Modalidad de Trabajo a Distancia "Hospital Digital".
b) La Unidad de Operaciones TI realizará la evaluación técnica, previa validación de Jefatura CAE, verificando la factibilidad del acceso remoto, la disponibilidad de

equipamiento institucional u homologación de equipo personal (si aplica) y el cumplimiento de los requisitos de seguridad definidos en la presente política.

c) En caso de que exista autorización por Jefatura CAE y factibilidad técnica se procederá a generar la solicitud de VPN como Hijo del Ticket Principal. En caso contrario se notificará al solicitante del rechazo.
d) Los datos de la VPN serán entregados directamente al funcionario solicitante.

7.3.3 AUTORIZACIÓN PARA GESTIÓN ADMINSITRATIVA REMOTA

Cuando un funcionario requiera acceso remoto para actividades específicas de soporte, administración, continuidad operacional o labores extraordinarias, deberá presentar la solicitud mediante el Catálogo de Servicios TI del Centro de Servicio TI, Categoría "Comunicación y Colaboración", servicio "Trabajo a Distancia", utilizando la opción de Modalidad de Trabajo a Distancia "Gestión Administrativa".

La Unidad de Operaciones TI verificará la autorización de la jefatura directa y efectuará la evaluación técnica correspondiente antes de habilitar el acceso remoto. Esta modalidad no constituye Teletrabajo ni modifica la jornada laboral del funcionario.

Al igual como las opciones anteriores deberá gestionarse la solicitud de VPN como Hijo del Ticket Principal.

7.3.4 AUTORIZACIONES EXTRAORDINARIAS

En situaciones de emergencia sanitaria, continuidad operacional, incidentes de ciberseguridad, desastres u otras circunstancias excepcionales, la Dirección del Hospital podrá autorizar modalidades extraordinarias de trabajo a distancia.

En todos los casos será obligatoria la evaluación técnica previa de la Unidad de Operaciones TI antes de habilitar cualquier acceso remoto, el cual mantendrá los mismos principios declarados en esta política.

7.3.5 CRITERIOS DE EVALUACIÓN TÉCNICA

La Unidad de Operaciones TI evaluará todas las solicitudes considerando, al menos, los siguientes criterios:

- Factibilidad técnica del acceso remoto.
- Disponibilidad de equipamiento institucional.
- Cumplimiento de los requisitos mínimos de ciberseguridad.
- Compatibilidad con los sistemas institucionales.
- Riesgos asociados al tratamiento de información institucional.
- Necesidad operacional del servicio solicitante.
- Cumplimiento de las políticas institucionales de Seguridad de la Información.

Cuando el Hospital disponga de equipamiento institucional para asignación, éste será el medio preferente para el desarrollo del trabajo a distancia.

Cuando excepcionalmente se autorice la utilización de equipos de propiedad del funcionario, éstos deberán cumplir la totalidad de los requisitos técnicos y de seguridad definidos por la Unidad de Operaciones TI y la Unidad de Seguridad de la Información.

7.3.6 VIGENCIA DE LAS AUTORIZACIONES

Las autorizaciones otorgadas en virtud de la presente política mantendrán su vigencia mientras subsistan las condiciones administrativas, operacionales y técnicas que justificaron su aprobación, esto se declara en la solicitud las cuales a priori serán de 3, 6 o 12 Meses.

La Unidad de Operaciones TI realizará una revisión técnica periódica de las autorizaciones vigentes **al menos una vez por año**, pudiendo efectuar verificaciones extraordinarias cuando existan cambios tecnológicos relevantes, incidentes de seguridad, modificaciones en el equipamiento utilizado, cambios de funciones del funcionario o cuando así lo determine la Unidad de Seguridad de la Información.

Respecto de equipos personales autorizados, la Unidad de Operaciones TI podrá solicitar en cualquier momento antecedentes que acrediten el cumplimiento de los requisitos técnicos establecidos. El funcionario dispondrá de **tres (3) días hábiles** para remitir la información solicitada.

La falta de entrega de dichos antecedentes facultará a la Unidad de Operaciones TI para suspender preventivamente el acceso remoto hasta que se regularice la situación, debiendo informar esta medida a la jefatura correspondiente, a la Unidad de Calidad de Vida Laboral cuando aplique y a la Unidad de Seguridad de la Información.

7.3.7 RENOVACIÓN

Las autorizaciones serán objeto de revisión cuando:

- Cambien las funciones del funcionario.
- Se modifique la modalidad de trabajo.
- Se reemplace el equipo utilizado.
- Existan cambios significativos en los riesgos identificados.
- Lo solicite la jefatura correspondiente.
- Lo determine la Unidad de Operaciones TI o la Unidad de Seguridad de la Información.
- Se agote el tiempo declarado en la solicitud (3, 6 o 12 Meses)

7.3.8 REVOCACIÓN

La Unidad de Operaciones TI podrá suspender inmediatamente los accesos remotos cuando existan antecedentes que hagan presumir un riesgo para la seguridad de la información.

La autorización de trabajo a distancia podrá ser revocada cuando concurra cualquiera de las siguientes circunstancias:

a) Incumplimiento de la presente política.
b) Incumplimiento de otras políticas institucionales de Seguridad de la Información.
c) Incumplimiento de la legislación vigente aplicable.
d) Pérdida de las condiciones técnicas mínimas exigidas.
e) Detección de vulnerabilidades críticas no corregidas.
f) Uso indebido de los recursos tecnológicos institucionales.
g) Incumplimiento de las instrucciones impartidas por la Unidad de Operaciones TI o la Unidad de Seguridad de la Información.
h) Término de la modalidad de trabajo a distancia, cambio de funciones, cese de la relación laboral o cuando desaparezcan las condiciones que justificaron la autorización.

La revocación del acceso remoto no exime al funcionario de las responsabilidades administrativas, civiles o penales que pudieran derivarse de los hechos que motivaron dicha medida.

7.4 REQUISITOS DE SEGURIDAD PARA EL ACCESO REMOTO

El Hospital de Tomé adopta un modelo de protección basado en la validación integral del acceso remoto, considerando la seguridad del **Origen** (identidad del usuario y dispositivo), del **Tránsito** (canal de comunicación seguro mediante VPN institucional y mecanismos criptográficos) y del **Destino** (plataformas institucionales protegidas mediante controles de acceso, autenticación y monitoreo continuo), aplicando los principios del modelo **Zero Trust**, donde ningún usuario, dispositivo o conexión es considerado confiable por defecto

Todo acceso remoto a plataformas, sistemas, aplicaciones o recursos tecnológicos del Hospital de Tomé deberá cumplir las medidas de seguridad establecidas en la presente política y en los estándares técnicos institucionales vigentes.

Los mecanismos de acceso remoto serán administrados exclusivamente por la Unidad de Operaciones TI, la cual implementará los controles técnicos necesarios para reducir los riesgos asociados al acceso desde redes externas, de conformidad con el Sistema de Gestión de Seguridad de la Información (SGSI), la Política Institucional de Acceso Remoto del Servicio de Salud Talcahuano y el modelo de seguridad Zero Trust adoptado por la institución.

7.4.1 ACCESO MEDIANTE VPN INSTITUCIONAL

Todo acceso remoto a los recursos tecnológicos institucionales deberá realizarse obligatoriamente mediante la Red Privada Virtual (VPN) institucional o mediante otro mecanismo de acceso remoto autorizado formalmente por el Área de Tecnologías de la Información.
Se prohíbe el acceso directo desde Internet a plataformas institucionales que no hayan sido expresamente publicadas para dicho propósito.

7.4.2 MODELO DE SEGURIDAD ZERO TRUST

Todo acceso remoto deberá considerar la validación permanente de los siguientes componentes de seguridad:

- Identidad del usuario.
- Estado de seguridad del dispositivo.
- Canal seguro de comunicación.
- Recurso solicitado.
- Nivel de riesgo asociado a la sesión.

La autorización del acceso no constituirá un estado permanente de confianza, pudiendo ser reevaluada durante toda la sesión de trabajo.

7.4.3 AUTENTICACIÓN

Todo acceso remoto deberá realizarse utilizando credenciales institucionales únicas e intransferibles.

Cuando la tecnología lo permita o así lo determine el Área de Tecnologías de la Información, será obligatoria la utilización de mecanismos de Autenticación Multifactor (MFA).

Se prohíbe compartir credenciales, almacenar contraseñas en texto plano o utilizar mecanismos de autenticación distintos de los autorizados institucionalmente.

7.4.4 EQUIPOS AUTORIZADOS

El acceso remoto únicamente podrá efectuarse desde equipos previamente autorizados por la Unidad de Operaciones TI.

Los equipos institucionales constituirán el mecanismo preferente para el trabajo a distancia.

Excepcionalmente podrá autorizarse el uso de equipos personales, siempre que éstos cumplan los requisitos establecidos en el **ANEXO TÉCNICO A - REQUISITOS PARA EQUIPOS PERSONALES**

7.4.5 CONFIGURACIÓN SEGURA DEL DISPOSITIVO

Todo equipo autorizado para trabajo a distancia deberá mantener una configuración segura durante toda la vigencia de la autorización.
Los requisitos técnicos mínimos serán definidos por la Unidad de Operaciones TI y se mantendrán documentados en los anexos técnicos vigentes de la presente política.

7.4.6 PROTECCIÓN DEL DISPOSITIVO

Todo dispositivo autorizado deberá mantener, como mínimo:

- mecanismos de protección contra software malicioso;
- sistema operativo soportado y actualizado;
- firewall habilitado;
- cifrado del almacenamiento cuando corresponda;
- bloqueo automático por inactividad;
- demás controles técnicos definidos por el Área de Tecnologías de la Información.

7.4.7 REGISTRO Y MONITOREO

Toda conexión remota podrá ser registrada, monitoreada y auditada por el Hospital de Tomé con fines de ciberseguridad, continuidad operacional, investigación de incidentes y cumplimiento normativo.

Los registros de auditoría serán administrados conforme a las políticas institucionales de gestión de registros y monitoreo de seguridad.

7.4.8 SUSPENSIÓN PREVENTIVA

La Unidad de Operaciones TI podrá suspender preventivamente cualquier acceso remoto cuando detecte condiciones que representen un riesgo para la seguridad de la información, sin perjuicio de las investigaciones administrativas que pudieren corresponder.

Cuando la suspensión obedezca a un posible incumplimiento de la presente política, deberá informarse a la Unidad de Seguridad de la Información para efectos de seguimiento y auditoría.

7.5 USO SEGURO DE ACTIVO TI DURANTE EL TRABAJO A DISTANCIA

Los activos tecnológicos proporcionados por el Hospital de Tomé constituyen recursos institucionales destinados exclusivamente al cumplimiento de funciones oficiales. Todo funcionario autorizado para desarrollar actividades mediante trabajo a distancia será responsable de su correcto uso, protección, custodia y conservación, debiendo adoptar las medidas necesarias para prevenir pérdidas, daños, accesos no autorizados o cualquier situación que comprometa la seguridad de la información institucional.

Las obligaciones establecidas en el presente apartado serán aplicables tanto a los activos institucionales como, cuando corresponda, a los equipos personales autorizados para el desarrollo de trabajo a distancia.

7.5.1 USO EXCLUSIVO INSTITUCIONAL

Los activos tecnológicos institucionales deberán utilizarse exclusivamente para el desarrollo de funciones propias del Hospital de Tomé.

Queda prohibido:

a) Facilitar o prestar equipos, credenciales o dispositivos institucionales a terceros.
b) Utilizar los activos tecnológicos para fines personales, comerciales, recreativos o cualquier actividad ajena a las funciones institucionales.
c) Instalar software, aplicaciones, extensiones o herramientas no autorizadas por la Unidad de Operaciones TI.
d) Alterar, deshabilitar o intentar evadir los controles de seguridad implementados por la institución.

7.5.2 CUSTODIA DE LOS ACTIVOS TECNOLÓGICOS

El funcionario será responsable de mantener los activos tecnológicos bajo su custodia directa durante todo el período de utilización.

Deberá adoptar las medidas necesarias para:

- Evitar el acceso de personas no autorizadas.
- Proteger los equipos frente a robos, pérdidas o daños.
- Mantener los dispositivos en condiciones adecuadas de conservación.
- Evitar su exposición a humedad, líquidos, temperaturas extremas, golpes u otros riesgos físicos.

Los activos institucionales no deberán permanecer desatendidos en lugares públicos, vehículos o espacios que representen un riesgo para su seguridad.

7.5.3 PROTECCIÓN DE LAS CREDENCIALES

Las credenciales institucionales constituyen información confidencial y de uso estrictamente personal.

El funcionario deberá:

- Mantener reserva sobre sus credenciales de acceso.
- No compartir contraseñas ni mecanismos de autenticación.
- No almacenar credenciales en medios inseguros.
- Informar inmediatamente cualquier sospecha de compromiso de las mismas.

7.5.4 INSTALACIÓN Y MODIFICACIONES DE SOFTWARE

Toda instalación, actualización o modificación de software en equipos institucionales deberá ser realizada o autorizada por la Unidad de Operaciones TI.

Se prohíbe expresamente:

- Instalar software sin autorización.
- Deshabilitar antivirus, herramientas EDR, agentes de monitoreo o mecanismos de protección.
- Modificar configuraciones de seguridad implementadas por la institución.
- Alterar políticas de seguridad, cifrado o mecanismos de autenticación.

7.5.5 DISPOSITIVOS DE ALMACENAMIENTO EXTERNO

El uso de dispositivos de almacenamiento extraíble deberá limitarse exclusivamente a situaciones debidamente justificadas y autorizadas por la Unidad de Operaciones TI.

No se permitirá almacenar información institucional en dispositivos personales o medios de almacenamiento que no cuenten con las medidas de seguridad establecidas por el Hospital de Tomé.

7.5.6 IMPRESIONES Y DOCUMENTACIÓN FÍSICA

La impresión de documentos institucionales durante el trabajo a distancia deberá restringirse a aquellos casos estrictamente necesarios para el cumplimiento de las funciones autorizadas.

Los documentos impresos deberán mantenerse bajo resguardo permanente, evitando su exposición a personas no autorizadas, y deberán eliminarse mediante mecanismos seguros una vez que dejen de ser necesarios.

7.5.7 USO DE EQUIPOS PERSONALES

Cuando excepcionalmente se autorice el uso de equipos personales, el funcionario será responsable de mantener permanentemente el cumplimiento de los requisitos establecidos en el **ANEXO TÉCNICO A – REQUISITOS PARA EQUIPOS PERSONALES**.

La utilización de un equipo personal no exime al funcionario del cumplimiento de las obligaciones establecidas en la presente política ni limita las facultades de supervisión técnica y auditoría del Hospital de Tomé.

7.5.8 PERDIDA, ROBO O DAÑO

Toda pérdida, robo, hurto, extravío o daño que afecte a un activo tecnológico institucional deberá ser informado inmediatamente a:

- La Mesa de Servicio TI.
- La jefatura directa.
- La Unidad de Seguridad de la Información, cuando corresponda.

En caso de robo o hurto, el funcionario deberá efectuar la denuncia ante la autoridad competente cuando la naturaleza del hecho así lo requiera, remitiendo los antecedentes al Hospital para la activación de las medidas de respuesta y resguardo de la información.

7.5.9 MANTENIMIENTO Y DEVOLUCIÓN

Los activos tecnológicos institucionales deberán mantenerse disponibles para las actividades de mantenimiento, actualización, soporte técnico o auditoría que determine la Unidad de Operaciones TI.

Asimismo, deberán ser restituidos inmediatamente cuando:

- Finalice la modalidad de trabajo a distancia.
- Se revoque la autorización correspondiente.
- Cambien las funciones del funcionario y los activos ya no sean necesarios.
- Cese la relación contractual o funcionaria con el Hospital de Tomé.

La devolución deberá efectuarse considerando todos los accesorios entregados originalmente y en las condiciones que permitan verificar su integridad y funcionamiento, sin perjuicio del desgaste derivado del uso normal.

7.6 PROTECCIÓN DE LA INFORMACIÓN INSTITUCIONAL

Toda información institucional tratada durante el trabajo a distancia deberá mantenerse protegida durante todo su ciclo de vida, aplicando medidas que resguarden su confidencialidad, integridad, disponibilidad y trazabilidad, de conformidad con la legislación vigente, las políticas institucionales y el Sistema de Gestión de Seguridad de la Información (SGSI).

Las obligaciones establecidas en el presente apartado serán aplicables a toda información institucional, independientemente de su formato, soporte o medio de transmisión.

7.6.1 TRATAMIENTO DE LA INFORMACIÓN INSTITUCIONAL

Toda información utilizada durante el trabajo a distancia deberá ser tratada exclusivamente para el cumplimiento de funciones institucionales y conforme a las autorizaciones otorgadas.

El funcionario deberá acceder únicamente a la información necesaria para el desarrollo de sus funciones, respetando los principios de mínimo privilegio y necesidad de conocer.

7.6.2 PROTECCIÓN DE DATOS PERSONALES Y DATOS SENSIBLES

El tratamiento de datos personales, datos sensibles y antecedentes clínicos deberá efectuarse en estricto cumplimiento de la legislación vigente, especialmente de las Leyes N° 19.628, N° 21.719 y N° 20.584.

El funcionario deberá adoptar todas las medidas necesarias para impedir el acceso, visualización o divulgación de dicha información por personas no autorizadas.

7.6.3 REGISTRO CLÍNICO ELECTRÓNICO Y SISTEMAS ASISTENCIALES

El acceso al Registro Clínico Electrónico (RCE), plataformas clínicas, sistemas administrativos y demás aplicaciones institucionales sólo podrá efectuarse mediante los mecanismos autorizados por el Hospital de Tomé.

Queda estrictamente prohibido copiar, descargar, fotografiar, grabar, reproducir o almacenar información clínica fuera de las plataformas institucionales, salvo autorización expresa emitida conforme a la normativa vigente.

7.6.4 ALMACENAMIENTO DE INFORMACIÓN

La información institucional deberá almacenarse únicamente en los repositorios, servidores, plataformas o servicios autorizados por el Hospital de Tomé.

Se prohíbe expresamente:

a) Almacenar información institucional en dispositivos personales no autorizados.
b) Utilizar servicios de almacenamiento en la nube distintos de los autorizados institucionalmente.
c) Mantener copias locales permanentes de información institucional cuando existan repositorios oficiales para dicho propósito.

7.6.5 INTERCAMBIO DE INFORMACIÓN

El intercambio de información institucional deberá efectuarse únicamente mediante canales oficiales autorizados por el Área de Tecnologías de la Información. (Correo Electrónico Institucional u otro declarado por el Área TIC.)

No podrán utilizarse cuentas de correo personales, aplicaciones de mensajería no autorizadas ni plataformas externas para compartir información institucional, salvo autorización expresa de la autoridad competente.

7.6.6 IMPRESIONES Y MANEJO DE DOCUMENTOS FÍSICOS

La impresión de documentación institucional deberá limitarse estrictamente a situaciones justificadas por necesidades del servicio.

Los documentos impresos deberán mantenerse bajo resguardo permanente y evitar su exposición a personas no autorizadas.

Cuando dejen de ser necesarios, deberán eliminarse utilizando mecanismos que impidan la recuperación de la información contenida en ellos.

7.6.7 PROTECCIÓN DE LA INFORMACIÓN EN PANTALLA

Durante el trabajo a distancia, el funcionario deberá adoptar medidas para evitar que terceros puedan visualizar información institucional.

Deberá privilegiarse el uso de espacios de trabajo que garanticen privacidad, evitando la exposición de información en lugares públicos o de libre acceso.

Cuando corresponda, se recomienda el uso de filtros de privacidad para pantallas u otras medidas que reduzcan el riesgo de observación no autorizada.

7.6.8 CONVERSACIONES Y REUNIONES REMOTAS

Las reuniones, videoconferencias y conversaciones que involucren información institucional deberán realizarse utilizando plataformas autorizadas por el Hospital de Tomé. (Catálogo de Servicio – Salas de VideoConferencia)

El funcionario deberá verificar que personas ajenas a la institución no puedan escuchar conversaciones, visualizar documentación o acceder a información institucional durante el desarrollo de reuniones remotas.

7.6.9 ELIMINACIÓN SEGURA DE LA INFORMACIÓN

Toda información institucional que deba ser eliminada durante o como consecuencia del trabajo a distancia deberá destruirse de forma segura, asegurando que no pueda ser recuperada, reconstruida o accedida por personas no autorizadas. La eliminación deberá realizarse considerando la naturaleza del soporte utilizado, distinguiéndose, al menos, las siguientes modalidades:

a) **Información digital:** La información almacenada temporalmente en equipos autorizados, dispositivos de almacenamiento o medios electrónicos deberá eliminarse utilizando los mecanismos definidos por el Área de Tecnologías de la Información, procurando su eliminación permanente cuando corresponda. No se permitirá conservar copias locales de información institucional una vez finalizada la actividad que justificó su almacenamiento temporal, debiendo mantenerse únicamente la información contenida en los repositorios oficiales del Hospital de Tomé. Cuando la naturaleza de la información o el nivel de riesgo lo requiera, el Área de Tecnologías de la Información podrá instruir la utilización de métodos de borrado seguro, sobrescritura criptográfica, destrucción lógica u otros mecanismos técnicamente equivalentes, para borrado digital tradicional se debe eliminar el archivo y enviar a la papelera, asegurando que posterior a ello se "vacíe la papelera".
b) **Información en soporte físico:** Todo documento impreso que contenga información institucional y cuya conservación no sea necesaria deberá destruirse utilizando mecanismos que impidan la reconstrucción o recuperación de su contenido, tales como trituradoras de corte cruzado u otros métodos de destrucción segura autorizados por la institución. En ningún caso los documentos institucionales podrán eliminarse mediante su disposición en basureros comunes, contenedores de reciclaje sin tratamiento previo o cualquier otro mecanismo que permita el acceso de terceros a la información contenida en ellos.

La eliminación de documentos deberá efectuarse respetando las normas sobre conservación documental, gestión documental, archivo institucional y demás disposiciones legales aplicables.

En ningún caso la eliminación de información podrá afectar registros oficiales, expedientes administrativos, fichas clínicas, respaldos institucionales o cualquier otro antecedente sujeto a obligaciones legales de conservación.

7.6.10 DEBER DE CONFIDENCIALIDAD

La obligación de resguardar la confidencialidad de la información institucional subsistirá durante toda la relación funcionaria o contractual y continuará vigente aun cuando finalice la autorización de trabajo a distancia o el vínculo con el Hospital de Tomé.

El incumplimiento de este deber podrá dar lugar a la aplicación de las medidas administrativas, civiles o penales que correspondan conforme a la legislación vigente.

7.7 USO DE REDES Y CONECTIVIDAD

Todo acceso remoto a plataformas institucionales deberá realizarse utilizando redes de comunicaciones que proporcionen condiciones adecuadas de seguridad, estabilidad y disponibilidad, minimizando los riesgos de interceptación, alteración o acceso no autorizado a la información institucional.

El funcionario será responsable de utilizar conexiones que cumplan los requisitos establecidos en la presente política y de adoptar las medidas necesarias para proteger la confidencialidad e integridad de las comunicaciones.

7.7.1 REDES DOMESTICAS

Se deberá privilegiar el uso de redes domésticas de confianza correctamente configuradas y protegidas mediante mecanismos de autenticación robustos.

Las redes inalámbricas deberán utilizar, como mínimo, cifrado **WPA2-Personal** o **WPA3**, manteniendo contraseñas robustas y evitando configuraciones predeterminadas del fabricante.

Asimismo, se recomienda mantener actualizado el firmware del router o punto de acceso utilizado para el trabajo a distancia. En caso de que el funcionario desconozca esto, puede consultarle a su proveedor de Internet (ISP).

7.7.2 REDES PÚBLICAS

Se prohíbe el acceso a plataformas institucionales desde redes Wi-Fi públicas, abiertas o que no proporcionen mecanismos adecuados de autenticación y cifrado.

Cuando, por razones excepcionales, no exista otra alternativa de conectividad, el acceso sólo podrá efectuarse mediante la VPN institucional y siempre que el funcionario verifique razonablemente la legitimidad de la red utilizada.

En ningún caso se deberá acceder directamente a recursos institucionales desde una red pública sin la utilización de los mecanismos de protección definidos por el Área de Tecnologías de la Información.

Un ejemplo de lo anterior es usar una red de un aeropuerto tipo WIFI para acceder al Registro Clínico Electrónico. Estas redes al ser públicas tienen sistemas de seguridad escasos que podrían vulnerar gravemente el dispositivo y la integridad completa de la conexión hacia el sistema.

7.7.3 COMPARTICIÓN DE INTERNET (HOTSPOT)

Podrá utilizarse la funcionalidad de compartición de Internet (Hotspot) mediante dispositivos móviles únicamente cuando constituya una alternativa segura frente a redes públicas.

El dispositivo utilizado deberá mantenerse protegido mediante contraseña, cifrado y las medidas de seguridad definidas por el fabricante y por la institución. Sin perjuicio de lo anterior, esto no cambia el hecho de que se debe establecer la conexión a través de una VPN Institucional.

7.7.4 CONFIGURACIÓN DE RED

Las configuraciones de red requeridas en el caso de los equipos institucionales para el acceso remoto serán administradas por la Unidad de Operaciones TI.
Los funcionarios no deberán modificar configuraciones relacionadas con VPN, DNS, certificados digitales, rutas de comunicación u otros parámetros de seguridad que afecten el acceso remoto, salvo autorización expresa de dicha Unidad.

En el caso de los equipos personales, la configuración será la estándar DHCP, IPv4, generalmente esto es configurado por el Proveedor de Internet o la configuración por defecto de los dispositivos.

Se recomienda que los equipos de conectividad utilizados para el trabajo a distancia (routers) mantengan actualizado su firmware, utilicen credenciales de administración distintas a las predeterminadas por el fabricante, deshabiliten funciones de administración remota cuando no sean necesarias y empleen mecanismos de cifrado inalámbrico vigentes. (Solicitar a su proveedor de Internet)

7.7.5 CONEXIONES DESDE EL EXTRANJERO

Como medida de protección de la infraestructura crítica del Hospital de Tomé y considerando su condición de Operador de Importancia Vital (OIV), todo acceso remoto originado desde el extranjero requerirá autorización previa de la jefatura correspondiente y de la Unidad de Operaciones TI.

El Área de Tecnologías de la Información podrá establecer restricciones geográficas, listas de países autorizados, mecanismos adicionales de autenticación o bloquear conexiones provenientes de ubicaciones que representen un riesgo para la ciberseguridad institucional. Toda aquella vez que se detecte conexiones entrantes desde ubicaciones no documentadas, se solicitará el bloqueo vía Firewall, esto incluye a terceros y proveedores de servicios.

7.7.6 MONITOREO DE CONECTIVIDAD

El Área de Tecnologías de la Información podrá monitorear las conexiones remotas con el objeto de detectar comportamientos anómalos, accesos desde ubicaciones inusuales, cambios significativos en el origen de las conexiones o cualquier otro evento que pueda representar un riesgo para la seguridad de la información.

Cuando se detecten condiciones que comprometan la seguridad del acceso remoto, la Unidad de Operaciones TI podrá suspender preventivamente la conexión hasta verificar su legitimidad y restablecer las condiciones de seguridad correspondientes.

7.8 VERIFICACIÓN DEL CUMPLIMIENTO Y AUDITORÍA

Con el objeto de verificar el cumplimiento permanente de los requisitos establecidos en la presente Política y sus Estándares Técnicos asociados, el Hospital de Tomé podrá realizar actividades de verificación, revisión y auditoría respecto de las modalidades de trabajo a distancia autorizadas.

Estas actividades tendrán por finalidad comprobar el cumplimiento de las medidas de seguridad implementadas, evaluar la eficacia de los controles establecidos y detectar oportunamente desviaciones que puedan representar riesgos para la seguridad de la información institucional.

7.8.1 VERIFICACIÓN TÉCNICA

La Unidad de Operaciones TI será la responsable de efectuar las verificaciones técnicas necesarias para comprobar el cumplimiento de los requisitos establecidos en los Anexos Técnicos de la presente Política.

Para estos efectos podrá solicitar al funcionario antecedentes que acrediten el cumplimiento de los controles técnicos exigidos, incluyendo, entre otros:

- Capturas de pantalla de configuraciones de seguridad.
- Evidencias del estado del sistema operativo.
- Evidencias del antivirus.
- Evidencias del firewall.
- Evidencias del cifrado del dispositivo.
- Evidencias de actualización del sistema.
- Otras verificaciones técnicas definidas por la Dirección de Tecnologías de la Información.

Los medios de verificación específicos y los requisitos mínimos se encontrarán definidos en los respectivos Estándares Técnicos.

7.8.2 PLAZO PARA LA ENTREGA DE EVIDENCIA

Cuando la Unidad de Operaciones TI solicite antecedentes para verificar el cumplimiento de los requisitos establecidos en la presente Política o en sus Estándares Técnicos, el funcionario deberá remitir la información requerida dentro del plazo máximo de **tres (3) días hábiles**, salvo que la solicitud establezca un plazo distinto por razones fundadas.

La falta de entrega de los antecedentes dentro del plazo establecido podrá dar lugar a la suspensión preventiva del acceso remoto hasta que la situación sea regularizada.

La información será solicitada al correo institucional del funcionario, será exclusiva responsabilidad de este revisar su casilla, según lo establece el estatuto administrativo.

7.8.3 VERACIDAD DE LAS EVIDENCIAS

Toda evidencia presentada por el funcionario deberá corresponder fielmente al estado real del equipo y de las configuraciones de seguridad existentes al momento de su remisión.

La alteración, manipulación, falsificación o presentación de antecedentes destinados a inducir a error respecto del cumplimiento de los requisitos establecidos en la presente Política constituirá un incumplimiento grave de las obligaciones institucionales, sin perjuicio de las responsabilidades administrativas, civiles y penales que pudieren derivarse conforme a la legislación vigente.

La Unidad de Operaciones TI podrá aplicar mecanismos de validación técnica para verificar la autenticidad de las evidencias recibidas, incluyendo la revisión de metadatos, consistencia de la información, validaciones remotas u otros procedimientos técnicamente apropiados.

Dado lo anterior solo se aceptarán dos formatos de evidencias JPG y PNG, las capturas deben ser sin procesar desde el capturador de pantalla al correo, sin pasar por ningún otro software. En caso de que esto no sea así o se trate de enviar un DOCX o PDF esa evidencia será inmediatamente anulada y se entenderá por incumplimiento.

Las evidencias podrán consistir en capturas de pantalla, reportes del sistema operativo, información obtenida mediante herramientas institucionales de gestión, sesiones remotas autorizadas u otros mecanismos técnicamente equivalentes

7.8.4 AUDITORÍA

La Unidad de Seguridad de la Información podrá realizar auditorías periódicas o extraordinarias para verificar el cumplimiento de la presente Política, sus Estándares Técnicos y demás controles asociados al trabajo a distancia.

Las auditorías podrán comprender, entre otras materias:

- Cumplimiento de los requisitos de seguridad.
- Correcta aplicación de los controles técnicos.
- Cumplimiento de las autorizaciones otorgadas.
- Gestión de accesos remotos.
- Protección de la información institucional.
- Cumplimiento de las obligaciones establecidas para el uso de equipos personales.

Las observaciones derivadas de dichas auditorías podrán dar origen a planes de acción, medidas correctivas, recomendaciones de mejora o la revocación de autorizaciones cuando se detecten incumplimientos que representen un riesgo para la seguridad de la información.

7.8.5 CONSERVACIÓN DE EVIDENCIAS

Las evidencias obtenidas durante los procesos de verificación y auditoría serán resguardadas por la Unidad de Operaciones TI conforme a las políticas institucionales de gestión documental y seguridad de la información.

El acceso a dichas evidencias quedará restringido exclusivamente al personal autorizado que requiera utilizarlas para fines de administración, auditoría, investigación de incidentes o cumplimiento normativo.

7.9 INCUMPLIMIENTO DE LA POLÍTICA

El cumplimiento de la presente Política constituye una obligación para todo funcionario, prestador de servicios, estudiante, interno, becario o tercero que haya sido autorizado para desarrollar actividades mediante cualquiera de las modalidades de trabajo a distancia definidas por el Hospital de Tomé.

Todo incumplimiento a las disposiciones contenidas en la presente Política, sus Estándares Técnicos, procedimientos asociados o a la normativa legal vigente será evaluado de acuerdo con su naturaleza, impacto y nivel de riesgo para la seguridad de la información institucional.

7.9.1 MEDIDAS ADMINISTRATIVAS

Sin perjuicio de las acciones administrativas o legales que pudieren corresponder, el Hospital de Tomé podrá adoptar una o más de las siguientes medidas cuando se verifique un incumplimiento:

a) Requerir la implementación de medidas correctivas dentro de un plazo determinado.
b) Suspender temporalmente el acceso remoto a plataformas institucionales hasta la regularización de las observaciones detectadas.
c) Revocar la autorización para desarrollar trabajo a distancia cuando el incumplimiento represente un riesgo para la seguridad de la información, la continuidad operacional o el cumplimiento de las obligaciones institucionales.
d) Solicitar la restitución inmediata de los activos tecnológicos institucionales asignados al funcionario.

7.9.2 RESPONSABILIDADES

El incumplimiento de la presente Política podrá dar lugar, según corresponda, a responsabilidades administrativas, civiles o penales, de conformidad con la legislación vigente, incluyendo las disposiciones contenidas en el Estatuto Administrativo, la Ley Marco de Ciberseguridad, la Ley sobre Delitos Informáticos, la normativa sobre protección de datos personales y demás cuerpos legales aplicables.

7.9.3 REPORTE DE INCUMPLIMIENTOS

Todo funcionario que tome conocimiento de un incumplimiento o de una situación que pueda comprometer la seguridad de la información deberá comunicarlo oportunamente a la Mesa de Servicio TI, a su jefatura directa o a la Unidad de Seguridad de la Información, conforme al procedimiento institucional de gestión de incidentes.
El reporte oportuno de un incidente o de un posible incumplimiento será considerado una medida de colaboración para la protección de la información institucional y no

eximirá de la aplicación de las medidas que correspondan cuando se determine la existencia de responsabilidades.

7.9.4 MEJORA CONTINUA

Las observaciones, incidentes, resultados de auditorías, revisiones técnicas y lecciones aprendidas derivadas de la aplicación de la presente Política podrán utilizarse para fortalecer los controles institucionales, actualizar los Estándares Técnicos y mejorar continuamente el Sistema de Gestión de Seguridad de la Información del Hospital de Tomé, conforme a los principios de mejora continua establecidos en la Norma ISO/IEC 27001:2022.

8 VIGENCIA, REVISIÓN Y CONTROL DE LA POLÍTICA

La presente Política de Trabajo a Distancia entrará en vigencia a contar de la fecha de total tramitación del acto administrativo que la apruebe y será de cumplimiento obligatorio para todas las personas comprendidas dentro de su ámbito de aplicación.

8.1 ADMINISTRACIÓN DE LA POLÍTICA

La administración, mantención y control documental de la presente Política corresponderá a la Unidad de Seguridad de la Información, la que actuará como responsable de su custodia, difusión, actualización y alineamiento con el Sistema de Gestión de Seguridad de la Información (SGSI).

La Unidad de Operaciones TI será responsable de mantener actualizados los Estándares Técnicos, procedimientos e instructivos asociados a la presente Política, proponiendo las modificaciones que resulten necesarias producto de cambios tecnológicos, operacionales o regulatorios.

8.2 REVISIÓN PERIODICA

La presente Política deberá ser revisada, a lo menos, cada **dos (2) años**, o anticipadamente cuando ocurra alguna de las siguientes circunstancias:

a) Modificaciones a la legislación o normativa aplicable.
b) Cambios relevantes en los procesos institucionales o en las modalidades de trabajo a distancia.
c) Incorporación de nuevas tecnologías o mecanismos de acceso remoto.
d) Cambios en el contexto de ciberseguridad institucional o en la condición del Hospital de Tomé como Operador de Importancia Vital (OIV).
e) Resultados de auditorías internas o externas que hagan recomendable su actualización.
f) Incidentes de seguridad de la información que evidencien la necesidad de fortalecer o modificar los controles establecidos.

8.3 ACTUALIZACIÓN DE ESTANDARES TÉCNICOS

Los Estándares Técnicos, procedimientos e instructivos derivados de la presente Política podrán actualizarse cuando las necesidades operacionales o los avances tecnológicos así lo requieran, siempre que dichas modificaciones no alteren los principios, objetivos o lineamientos establecidos en esta Política.

Las actualizaciones deberán mantener la coherencia con el Sistema de Gestión de Seguridad de la Información, la normativa institucional vigente y los requisitos de la Norma ISO/IEC 27001:2022.

8.4 CONTROL DOCUMENTAL

Toda modificación a la presente Política deberá efectuarse mediante el acto administrativo que corresponda, asegurando el adecuado control de versiones, la trazabilidad de los cambios y la conservación del historial documental conforme a las normas institucionales de gestión documental.

Las versiones derogadas deberán mantenerse resguardadas como antecedente histórico, evitando su utilización como documento vigente.

8.5 DIFUSIÓN

Una vez aprobada o actualizada, la presente Política deberá ser difundida por los medios institucionales que determine la Dirección del Hospital o la Unidad de Seguridad de la Información, asegurando que las personas sujetas a su cumplimiento conozcan oportunamente sus disposiciones y las responsabilidades que de ella emanan.

9 ANEXO TÉCNICO A - REQUISITOS PARA EQUIPOS PERSONALES

9.1 OBJETIVO

El presente Anexo Técnico establece los requisitos mínimos de seguridad que deberán cumplir los equipos computacionales de propiedad del funcionario (Bring Your Own Device – BYOD) cuando, excepcionalmente, sean autorizados para acceder a plataformas institucionales del Hospital de Tomé mediante alguna de las modalidades de Trabajo a Distancia definidas en la presente política.

El cumplimiento de estos requisitos constituye una condición obligatoria para la habilitación y mantención del acceso remoto a los recursos institucionales.

9.2 APLICABILIDAD

El presente Anexo será aplicable únicamente cuando:

- No exista disponibilidad de equipamiento institucional.
- La Unidad de Operaciones TI autorice expresamente el uso de un equipo particular.
- El funcionario requiera acceder a recursos institucionales desde un equipo de su propiedad.

La autorización para utilizar un equipo personal tendrá carácter excepcional y podrá ser revocada en cualquier momento cuando el equipo deje de cumplir los requisitos establecidos.

9.3 REQUISITOS TÉCNICOS OBLIGATORIOS

9.3.1 CONECTIVIDAD

Requisito	Exigencia
Velocidad mínima	20 Mbps de descarga y 20 Mbps de subida
Medio recomendado	Cable Ethernet o Wi-Fi 5 GHz con señal estable
Como Configurarlo	Conectar el computador preferiblemente mediante cable de red (Ethernet) al router o asegurar una señal fuerte de Wi-Fi en la banda de 5 GHz.
Evidencia	Adjuntar una captura de pantalla de una prueba de velocidad oficial (por ejemplo, speedtest.net) donde se aprecie claramente que los resultados superan los 20 Mbps tanto en descarga como en subida.

9.3.2 SISTEMA OPERATIVO

Requisito	Exigencia
Sistema soportado	Windows soportado oficialmente por Microsoft
Actualizaciones	Últimos parches instalados

Como Configurarlo	En Windows, ir a **Configuración > Actualización y seguridad > Windows Update** (o **Configuración > Windows Update** en Windows 11) y buscar actualizaciones pendientes hasta que el equipo indique que está al día.
Evidencia	Captura de pantalla de la ventana de configuración de Windows Update donde se muestre el mensaje **"Estás al día"** o el historial de actualizaciones recientes instaladas con éxito.

9.3.3 LICENCIAMIENTO

Requisito	**Exigencia**
Licencia	Sistema Operativo original y activado
Como Configurarlo	Ingresar la clave de producto legítima provista por el fabricante o la institución en la sección de activación del sistema operativo.
Evidencia	Captura de pantalla de **Configuración > Sistema > Información**, específicamente en la sección de **Especificaciones de Windows**, donde se confirme que el sistema operativo se encuentra **Activado**.

9.3.4 SEGURIDAD DE ACCESO

Requisito	**Exigencia**
Contraseña local	Mínimo 12 caracteres
Complejidad	Mayúsculas, minúsculas, números y símbolos
Como Configurarlo	Ir a **Configuración > Cuentas > Opciones de inicio de sesión > Contraseña**, y modificarla usando una combinación de al menos 12 caracteres que incluyan mayúsculas, minúsculas, números y símbolos.
Evidencia	Captura de pantalla de la sección de opciones de inicio de sesión donde se evidencie que el método de contraseña está activo (por seguridad, **nunca** se debe mostrar la clave escrita en la imagen, sino la configuración del requisito o la pantalla de bloqueo de cambio de contraseña).

9.3.5 BLOQUEO AUTOMÁTICO

Requisito	**Exigencia**
Bloqueo por inactividad	Máximo 5 minutos
Como Configurarlo	Ir a **Configuración > Personalización > Pantalla de bloqueo** (o Energía y suspensión) y configurar el tiempo de apagado de pantalla y suspensión a **5 minutos o menos**.
Evidencia	Captura de pantalla de la sección de configuración de energía y suspensión donde se muestren seleccionados los valores de tiempo en **5 minutos** (o menos) para el bloqueo de pantalla.

9.3.6 PERFIL EXCLUSIVO

Requisito	Exigencia
Usuario dedicado	Perfil exclusivo para funciones institucionales
Privilegios	Preferentemente usuario estándar
Como Configurarlo	Crear un usuario estándar adicional en el equipo exclusivo para las tareas del hospital (**Configuración > Cuentas > Familia y otros usuarios > Agregar a otra persona a este equipo**).
Evidencia	Captura de pantalla de la sección de **Cuentas** -> **Otros Usuarios** donde se muestre claramente el nombre del perfil de usuario dedicado exclusivamente a la labor institucional.

9.3.7 HARDWARE MÍNIMO

El equipo deberá cumplir, como mínimo:

- Procesador de 64 bits compatible con Windows soportado.
- GB de memoria RAM.
- 256 GB de almacenamiento disponible.
- TPM cuando el sistema operativo lo requiera.
- Espacio suficiente para VPN, antivirus y aplicaciones institucionales.

Evidencia:
Captura de pantalla de la sección de **Cuentas** -> **Otros Usuarios** donde se muestre claramente el nombre del perfil de usuario dedicado exclusivamente a la labor institucional.

9.3.8 ANTIVIRUS

Requisito	Exigencia
Protección	Antivirus licenciado y actualizado
Estado	Protección activa
Como Configurarlo	Instalar y verificar el estado del software de seguridad corporativo o el antivirus oficial asignado por la institución, asegurando que las definiciones estén actualizadas.
Evidencia	Captura de pantalla de la interfaz principal del antivirus (por ejemplo, *Seguridad de Windows* o el panel del antivirus corporativo) donde se muestre explícitamente el estado **"Protegido"** o **"Al día"** con la última fecha de actualización de firmas.

9.3.9 FIREWALL

Requisito	Exigencia
Firewall	Activado
Perfiles	Público y Privado
Como Configurarlo	Ir a **Panel de control > Firewall de Windows Defender** (o Privacidad y seguridad > Seguridad de Windows > Firewall y protección de red) y

	comprobar que esté activado para redes de dominio, privadas y públicas.
Evidencia	Captura de pantalla de la interfaz principal del antivirus (por ejemplo, *Seguridad de Windows* o el panel del antivirus corporativo) donde se muestre explícitamente el estado **"Protegido"** o **"Al día"** con la última fecha de actualización de firmas.

9.3.10 CIFRADO

Requisito	**Exigencia**
Disco del sistema	Obligatoriamente cifrado
Tecnología	BitLocker o equivalente
Como Configurarlo	Ir a **Panel de control > Cifrado de unidad BitLocker** y activar la protección en la unidad principal del sistema (o verificar su estado de activación).
Evidencia	Captura de pantalla de la ventana de administración de **BitLocker** (o la sección de seguridad del dispositivo) donde se indique que la unidad del sistema operativo se encuentra **Cifrada**.

Nota Aclaratoria: Las ayudas en las etiquetas "Como Configurarlo" no pretende ser un manual acabado de como realizar una configuración, dado que esto es responsabilidad exclusiva del dueño del dispositivo.

9.4 EVALUACIÓN TÉCNICA

La Unidad de Operaciones TI verificará el cumplimiento de los requisitos establecidos en el presente Anexo antes de habilitar el acceso remoto.
Podrá solicitar antecedentes adicionales cuando existan dudas respecto del cumplimiento de alguno de los controles.

Algunos de los elementos adicionales podrían ser:

Requisito	**Exigencia**
Protección	Arranque Seguro
Estado	Activado
Como Configurarlo	Se debe iniciar en modo BIOS y configurar Secure Boot en el firmware UEFI (siempre que el Hardware lo soporte)
Evidencia	Captura desde "Información del sistema" (msinfo32) donde el estado de **Arranque Seguro** figure como **Activado**.

Requisito	**Exigencia**
Protección	Uso de Recursos
Estado	Optimo
Como Configurarlo	No se configura.
Evidencia	Presionar Ctrl+alt+supr lo que abrirá el administrador de tareas, se debe sacar una captura de la ventana.

9.5 MANTENCIÓN DE LAS CONDICIONES

Los funcionarios deberán mantener permanentemente el cumplimiento de los requisitos técnicos definidos en este Anexo.

La Unidad de Operaciones TI podrá solicitar, en cualquier momento, antecedentes actualizados que acrediten el cumplimiento de los controles.

El funcionario dispondrá de tres (3) días hábiles para remitir la información solicitada. La falta de respuesta facultará a la Unidad de Operaciones TI para suspender preventivamente el acceso remoto hasta la regularización de la situación.

9.6 RESPONSABILIDAD DEL FUNCIONARIO

Cuando se utilicen equipos personales, será de exclusiva responsabilidad del funcionario:

- Mantener el equipo actualizado.
- Mantener el antivirus operativo.
- Mantener habilitado el firewall.
- Mantener el cifrado del dispositivo.
- No deshabilitar las configuraciones de seguridad.
- Mantener la confidencialidad de las credenciales institucionales.
- Permitir las verificaciones técnicas requeridas por la Unidad de Operaciones TI.

El Hospital de Tomé no será responsable por fallas, pérdidas de información personal, incompatibilidades de software o daños derivados del uso de equipos particulares.

9.7 VERACIDAD DE LA INFORMACIÓN

Toda evidencia proporcionada por el funcionario tendrá el carácter de declaración para efectos administrativos.

La alteración, falsificación o manipulación de imágenes, capturas de pantalla o cualquier otra evidencia destinada a acreditar el cumplimiento de este Anexo constituirá un incumplimiento grave de la presente Política, sin perjuicio de las responsabilidades administrativas, civiles y penales que pudieren derivarse conforme a la legislación vigente, incluyendo la Ley N° 21.459 sobre Delitos Informáticos.

La Unidad de Operaciones TI y la Unidad de Seguridad de la Información podrán verificar la autenticidad de las evidencias mediante procedimientos técnicos, revisión de metadatos, validaciones remotas u otros mecanismos que estimen pertinentes.

9.8 AUDITORÍA

La Unidad de Seguridad de la Información podrá auditar el cumplimiento del presente Anexo como parte de las actividades de monitoreo y mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI), pudiendo recomendar medidas correctivas o la suspensión de accesos cuando se detecten incumplimientos que representen un riesgo para la seguridad de la información institucional.

10 ANEXO TÉCNICO B ESTÁNDAR DE SEGURIDAD PARA ACCESO REMOTO

10.1 OBJETIVO

El presente Anexo Técnico establece los requisitos mínimos de seguridad que deberán cumplir todas las conexiones remotas autorizadas hacia los recursos tecnológicos del Hospital de Tomé.

Su finalidad es garantizar que el acceso remoto se efectúe bajo un modelo de confianza cero (Zero Trust), reduciendo los riesgos asociados al acceso desde redes externas y asegurando la protección de la información institucional durante todo el ciclo de la comunicación.

10.2 ALCANCE

El presente Anexo será aplicable a:

- Teletrabajo.
- Hospital Digital.
- Gestión Administrativa Remota.
- Accesos extraordinarios autorizados.

Será obligatorio para funcionarios, prestadores de servicios y terceros que accedan remotamente a recursos institucionales.

10.3 MODELO DE SEGURIDAD

El Hospital de Tomé adopta un modelo de protección basado en los principios de **Zero Trust**, considerando que ningún usuario, dispositivo o conexión será considerado confiable por defecto.

Todo acceso remoto deberá protegerse mediante tres niveles complementarios de seguridad:

- **Origen** (Identidad + Dispositivo)
- **Tránsito** (Comunicación)
- **Destino** (Servicios Institucionales)

Cada uno de estos componentes deberá cumplir los requisitos establecidos en el presente Anexo.

10.4 SEGURIDAD DEL ORIGEN

Antes de autorizar cualquier conexión deberán verificarse, como mínimo, los siguientes elementos:

10.4.1 IDENTIDAD

El usuario deberá autenticarse utilizando exclusivamente:

- Cuenta institucional.
- Credenciales individuales.
- Usuario no compartido.
- Cuenta vigente.

- Cuenta autorizada.

Queda prohibido:
- compartir cuentas;
- utilizar cuentas genéricas;
- utilizar credenciales de terceros.

10.4.2 AUTENTICACIÓN MULTIFACTOR (MFA)

Cuando la plataforma lo permita, el acceso remoto deberá utilizar autenticación multifactor. El Área de Tecnologías de la Información podrá definir qué plataformas tendrán MFA obligatorio.

10.4.3 ESTADO DEL DISPOSITIVO

Previo a la habilitación del acceso remoto el equipo deberá cumplir los requisitos establecidos en el:

- **Anexo Técnico A – Equipos Personales**

o bien tratarse de un equipo institucional administrado por el Área de Tecnologías de la Información.

10.5 SEGURIDAD DEL TRÁNSITO

Toda comunicación entre el usuario y el Hospital deberá encontrarse protegida mediante mecanismos criptográficos.

10.5.1 VPN INSTITUCIONAL

Será obligatorio utilizar exclusivamente la VPN institucional autorizada.

No se permitirá:
- exposición directa de servicios;
- acceso por escritorio remoto publicado en Internet;
- túneles no autorizados;
- software VPN de terceros.

10.5.2 CIFRADO

Toda la información transmitida deberá viajar cifrada utilizando protocolos criptográficos seguros autorizados por el Área de Tecnologías de la Información.

No podrán utilizarse protocolos considerados inseguros u obsoletos.

10.5.3 INTEGRIDAD

Los mecanismos de acceso remoto deberán garantizar que la información transmitida no sea modificada durante el tránsito.

10.5.4 REDES

Se recomienda utilizar:

- conexiones cableadas;
- redes Wi-Fi WPA2/WPA3.

Queda prohibido utilizar redes públicas abiertas cuando exista riesgo para la información institucional.

Cuando no exista otra alternativa, el usuario deberá conectarse exclusivamente mediante la VPN institucional antes de acceder a cualquier recurso institucional.

10.6 SEGURIDAD DEL DESTINO

Todo acceso remoto deberá dirigirse únicamente hacia recursos institucionales autorizados. No podrán habilitarse accesos directos a servidores o aplicaciones sin autorización expresa del Área de Tecnologías de la Información.

10.6.1 CONTROL DE ACCESOS

Los permisos otorgados deberán respetar los principios de:

- mínimo privilegio;
- necesidad de conocer;
- segregación de funciones.

10.6.2 REGISTRO DE ACTIVIDAD

Toda sesión remota podrá generar registros de:

- usuario;
- dirección IP;
- fecha y hora;
- duración;
- recurso accedido;
- eventos de autenticación;
- eventos de seguridad.

Estos registros podrán utilizarse para auditorías, investigaciones de incidentes y cumplimiento normativo.

10.6.3 MONITOREO

El Área de Tecnologías de la Información podrá implementar mecanismos automáticos de monitoreo orientados a detectar:

- accesos anómalos;
- intentos reiterados de autenticación;
- conexiones desde ubicaciones inusuales;
- dispositivos no autorizados;
- eventos de ciberseguridad.

10.7 ADMINISTRACIÓN DEL ACCESO REMOTO

Corresponderá a la Unidad de Operaciones TI:

- habilitar accesos;
- modificar accesos;
- suspender accesos;
- revocar accesos;
- mantener registros;
- administrar la infraestructura VPN;
- administrar certificados;
- administrar mecanismos de autenticación.

10.8 SUSPENSIÓN AUTOMÁTICA

La Unidad de Operaciones TI podrá suspender inmediatamente un acceso remoto cuando:

- exista riesgo para la seguridad;
- se detecte malware;
- exista compromiso de credenciales;
- el equipo deje de cumplir los requisitos técnicos;
- existan vulnerabilidades críticas;
- exista incumplimiento de la presente política.

10.9 AUDITORÍA

La Unidad de Seguridad de la Información podrá revisar periódicamente:

- configuraciones;
- registros;
- autenticaciones;
- controles implementados;
- cumplimiento del presente Anexo.

Podrá solicitar acciones correctivas cuando detecte desviaciones respecto de los estándares institucionales.

10.10 REVISIÓN DEL ESTÁNDAR

El presente Anexo será revisado por la Unidad de Operaciones TI al menos una vez al año o cuando ocurra alguna de las siguientes circunstancias:

- cambios tecnológicos significativos;
- incorporación de nuevas plataformas;
- cambios regulatorios;
- incidentes relevantes de ciberseguridad;
- recomendaciones de auditoría;
- actualización del Sistema de Gestión de Seguridad de la Información.

Toda modificación deberá ser informada a la Unidad de Seguridad de la Información para efectos de control documental y seguimiento del SGSI.