DIRECCION
STG/CGS/CMM

RESOLUCION EXENTA Nº 4273

SANTIAGO 30 OCT 2025

VISTOS:

Las facultades concedidas por los artículos 35 y 36 del DFL N° 1, de 2005, del Ministerio de Salud, que fijó el texto refundido, coordinado y sistematizado del Decreto Ley N° 2.763, de 1979 y de las leyes N°18.933 y N° 18.469; el Decreto de Salud N°38, de 2005, Reglamento Orgánico de los Establecimientos de Salud de Menor complejidad y de los Establecimientos de Autogestión en Red; la ley 19.799 sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma; en el Decreto Supremo Nº 83, del Ministerio Secretaría General de la Presidencia, de 2004, que aprueba norma técnica para los órganos de la Administración del Estado sobre seguridad y confidencialidad de los documentos electrónicos; en el Decreto Nº 14 de 2014 que modifica Decreto Nº 181, de 2002, que aprueba reglamento de la ley 19.799 sobre documentos electrónicos, firma electrónica y la certificación de dicha firma, y deroga los decretos que indica; ley 21459 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; en el Decreto Nº 83 de 28 de agosto de 2017, del Ministerio de Relaciones Exteriores que promulga Convenio sobre la Ciberdelincuencia; en la norma chilena NCh-ISO 27001: 2022; en el Instructivo Presidencial N°8 que imparte instrucciones urgentes en materia de ciberseguridad; Resolución Exenta Numero RA 446/9/2024 de 09 de febrero de 2024 del Servicio de Salud Metropolitano Sur sobre nombramiento en el cargo de director del Hospital Barros Luco Trudeau; La Resolución N°36 de 19 de diciembre de 2024, de Contraloría General de la República, sobre exención del trámite de toma de razón;

CONSIDERANDO

Que, conforme dispone el artículo 20°, letra b) del decreto 83, aprueba norma técnica para los órganos de la administración del estado sobre seguridad y confidencialidad de los documentos electrónicos, 2004, del Ministerio Secretaría General de la Presidencia, sobre el uso de la red interna, uso de Internet, uso del correo electrónico, acceso a servicios públicos, recursos compartidos, servicios de mensajería y comunicación remota, y otros; Que, en mérito de lo antes mencionado, y en cumplimiento a los principios de escrituración, transparencia, eficiencia y eficacia en la administración pública, dicto la siguiente:

RESOLUCION

1.- DÉJESE SIN EFECTO la resolución N°855 del 5 de abril 2021, de la dirección del Hospital que aprueba el documento "Política de seguridad control de acceso, acceso a redes y servicios";

2.- APRUÉBESE el documento denominado "Política de seguridad control de acceso, acceso a redes y servicios", Código DGTI 03, Versión 03, que rige desde la fecha de la presente resolución exenta, cuyo texto es del siguiente tenor:

POLÍTICA DE SEGURIDAD CONTROL DE ACCESO, ACCESO A REDES Y SERVICIOS

	Nombre	Cargo	Firma
Realizado por:	Mijail Muñoz Valenzuela	Encargado de Seguridad de la Información y Ciberseguridad	
Revisado por:	Carolina Muñoz Valenzuela	Jefa de unidad de calidad y seguridad del paciente	
	Fabiola Fuentes Carreño	Jefa del Depto. de Gestión de las Personas	
	Claudio Gómez Silva	Asesor Jurídico	
	Osvaldo Augusto De La Barra Ugalde	Jefe Departamento Control de Gestión	
	Francisco Epul Huilipan	Jefe Departamento Gestión Financiera y Contable	
	Hilbert González Cárcamo	Jefe Unidad de Seguridad	
Aprobado por:	Walter Keupuchur Meza	Director HBLT	

SERVICIO DE SALUD M. SUR * DIRECTOR * HOSPITAL BARROS LUCO TRUDEAU

INDICE

OBJETIVO 3
ALCANCE 3
RESPONSABLES 3
DEFINICIONES 4
DESARROLLO 5
I. CONTROL DE ACCESO 5
1. Derechos de Acceso 5
2. Control de Acceso a la Información 6
3. Revocación de Acceso (Baja de Usuarios) 7
4. Gestión de Cuentas Privilegiadas 7
5. Revisión de los Derechos de Acceso 8
II. ACCESO A REDES Y SERVICIOS 8
1. Acceso a redes 8
2. Acceso a Servicios 8
3. Acceso por VPN (Virtual Private network) 9
4. Acceso a Internet 9
III. PROCEDIMIENTOS RELACIONADOS A LAS POLITICAS DE SEGURIDAD DE CONTROL DE ACCESO, ACCESO A REDES Y SERVICIOS. 10
1. Procedimiento Administración de Acceso de Usuarios 10
2. Procedimiento Responsabilidades de los Usuarios 12
SANCIONES 13

OBJETIVO

Establecer lineamientos formales para la asignación, modificación, uso y revocación de derechos de acceso a la información, sistemas y activos de información del Hospital Barros Luco Trudeau, asegurando que dichos accesos estén justificados, sean proporcionales a las funciones de la usuaria y usuario.

ALCANCE

Esta política aplica a toda persona con vínculo laboral con el Hospital Barros Luco Trudeau (HBLT), así como al personal externo debidamente autorizado por la jefatura para acceder a sistemas institucionales. También, incluye a colaboradores internos y externos que, por razones de proyectos o funciones específicas, necesiten acceso a recursos del hospital, tanto de forma presencial como remota.

RESPONSABLES

- **Departamento de Gestión de Tecnologías de la Información:** Diseñar, implementar y mantener los controles técnicos necesarios para la gestión segura de accesos, monitoreo de uso y revocación oportuna de privilegios.
- **Jefe de Departamento de gestión de Tecnologías de la Información:** Es el responsable de Gestionar los procedimientos necesarios para que el departamento de gestión de Tecnologías de la información pueda solucionar los incidentes de seguridad, aprobar manuales y procedimientos de atención de mesa de ayuda.
- **Encargado de seguridad de la Información y Ciberseguridad:** Velar por el cumplimiento de esta política, asesorar a las áreas responsables en materia de acceso seguro.
- **Departamento de gestión y desarrollo de las personas:** Responsables de la gestión del ciclo de vida de los usuarios (alta, baja, cambios de rol) y la comunicación con el DGTI sobre las bajas o cambios de rol.
- **Funcionarios del Hospital Barros Luco Trudeau:** Es el personal de la institución al cual está sujeto al cumplimiento de las políticas descritas en este documento.
- **Personal Externo al Hospital Barros Luco Trudeau:** Es el personal, que presta funciones al Hospital Barros Luco Trudeau, perteneciente a empresas externas, el cual está sujeto al cumplimiento de las políticas descritas en este documento.
- **Dueños del sistema:** Responsables de definir los niveles de acceso requeridos para sus respectivos datos, aplicaciones y sistemas.

DEFINICIONES

- **Acceso:** Permiso para entrar y usar un sistema, red o información.
- **Acceso autorizado:** Permiso legítimo y aprobado para usar un recurso.
- **Acceso no autorizado:** Intento de ingresar a un sistema sin permiso.
- **Alejamiento:** Renuncia, desvinculación, jubilación o fallecimiento de una funcionaria o funcionario (planta, contrata, reemplazos y suplencia), personal externo que prestaba servicios en el HBLT y tenía acceso a sistemas y/o servicios.
- **Baja de usuario / Revocación de acceso:** Acción de eliminar permisos cuando alguien deja de necesitar acceso.
- **Bóveda de contraseñas / bóveda digital:** Lugar seguro (físico o digital) donde se guardan contraseñas administrativas.
- **Confidencialidad:** Garantía de que la información solo es vista por personas autorizadas.
- **Contraseña:** Clave secreta que permite acceder a un sistema o equipo. La cual es personal e intransferible.
- **Cuenta de usuario / credenciales:** Identificación única (usuario + contraseña) que da acceso a un sistema.
- **Cuenta genérica:** Cuenta compartida por múltiples personas; su uso es excepcional y controlado.
- **Cuenta privilegiada:** Cuenta especial con permisos avanzados para administrar sistemas.
- **Derechos de acceso:** Conjunto de permisos que tiene una cuenta para ver o usar cosas.
- **Disponibilidad:** Que la información y sistemas estén accesibles cuando se necesitan.
- **Dueño de la información:** Persona responsable de autorizar quién puede ver o usar ciertos datos.
- **Dueño del sistema:** También se define como "dueño del proceso", proceso en el cual el sistema presta apoyo.
- **Incidente de seguridad:** Cualquier situación que ponga en riesgo la información (ej.: acceso no autorizado, pérdida de datos).
- **Integridad:** Seguridad de que la información no se altera o modifica sin autorización.

- **Navegador (Browser):** Programa para acceder a páginas y servicios en Internet (ej.: Chrome, Edge).
- **Segregación de funciones:** Distribuir tareas para que una sola persona no controle todo un proceso crítico.

DESARROLLO

I. CONTROL DE ACCESO

1. Derechos de Acceso

Los derechos de acceso tienen por objeto establecer los lineamientos para la creación, control y gestión de las cuentas de usuario con acceso a los sistemas de información del Hospital Barros Luco Trudeau, resguardando la integridad, confidencialidad y disponibilidad de los sistemas y los recursos de información. En este contexto, deberán cumplirse los siguientes requisitos y disposiciones.

- Toda persona que desee ingresar a algún recurso de red o sistema del HBLT, deberá tener un usuario y contraseña, válido y autorizado por el DGTI, bajo los procedimientos establecidos por éste.
- El usuario y contraseña es personal e intransferible, incluso a personas con mayor autoridad o grado.
- Los derechos de acceso se otorgarán únicamente cuando exista una necesidad legítima y justificada para el desempeño de las funciones del usuario.
- El acceso a la información y sistemas, deberá ser solicitada, siempre indicando el perfile que se le asignará al usuario y, aprobado por la jefatura directa.
- El acceso a la información y sistemas, será administrado por el DGTI, y la gestión para su acceso, será mediante la metodología que el DGTI defina.
- Toda solicitud de acceso a información o sistemas, deberá ser formalizado por el solicitante, y aprobado por la jefatura directa, al DGTI por el método que éste último defina.
- La eliminación de los derechos a accesos a sistemas e información, deberá ser solicitada por la jefatura directa del usuario con estos accesos. Según la metodología definida por el DGTI, para estos efectos.
- El DGTI puede realizar o solicitar la baja o bloqueo de accesos a sistemas, redes e información, previa revisión y análisis de la información de acceso de los usuarios; si considera que puede estar en riesgo la privacidad, integridad de los sistemas, redes e información.

- Debe quedar un registro formal y documentado de la solicitud y autorización de acceso a los sistemas y aplicaciones.
- Todos los equipos computacionales deben tener un usuario y contraseña de ingreso. Además, un protector de pantalla, el cual debe activarse en un tiempo de inactividad del equipo, que bloquee el uso de sesión hasta ingresar nuevamente la contraseña.
- Existirán equipos computacionales que no tendrán tiempo de activación de protector de pantalla, los cuales serán solicitados por la jefatura, y esta solicitud será analizada por DGTI, el cual podrá aceptar o rechazar lo solicitado.
- Las contraseñas de cuentas de administración de servidores, servicios, administración de equipos de red, serán guardadas en sobre cerrado o bóveda digital, y entregados a la jefatura del DGTI. Debiendo ser actualizada con cada cambio de contraseña, nuevo servicio o nuevo equipo de red.
- No deben existir cuentas genéricas dentro de los sistemas de información, siempre se debe identificar el usuario que utiliza el sistema y accede a la información, salvo excepciones que serán analizadas, rechazado o aprobadas por el DGTI.
- El modelo de roles, perfiles y los derechos de acceso asignados se revisarán y actualizarán para reflejar los cambios en las funciones, responsabilidades y necesidades del HBLT.
- Un usuario tendrá un único Rol el cual tendrá un único perfil (grupo de permisos) por sistema o servicio. Varios usuarios podrán tener el mismo ROL, si esto aplica.
- Se implementará la segregación de funciones para prevenir que una sola persona tenga control sobre procesos críticos que pudieran permitir actividades fraudulentas o no autorizadas.
- La gestión de derechos de acceso se realizará en cumplimiento con la normativa legal vigente.

2. Control de Acceso a la Información

- Para todo medio de procesamiento de información al que se necesite conceder accesos (por ejemplo: aplicaciones, carpetas compartidas, NUBE HBLT u otro similar), el dueño de la Información es quién será encargado de autorizar los permisos de acceso y solicitar los espacios necesarios.
- Sólo se deben conceder accesos a terceros previa solicitud del dueño del sistema información, y nunca antes de haberse firmado un acuerdo de confidencialidad. Los accesos serán definidos y otorgados por el DGTI a solicitud del dueño del sistema.

- El encargado de seguridad de la información y Ciberseguridad tiene las facultades de suspender o eliminar los accesos a cualquier persona que represente riesgo en la confidencialidad, integridad o disponibilidad de la información.
- Cualquier intento de acceso no autorizado a los equipos, carpetas compartidas, sistemas e información será considerado un incidente, por lo que debe reportarse de inmediato al DGTI.

3. Revocación de Acceso (Baja de Usuarios)

Ante situación de un cambio de cargo de funcionario, se deben revisar sus permisos de acceso lógico asignados y verificar que éstos sigan siendo válidos de acuerdo con su nueva función.

- Las jefaturas directas.
- Los(as) encargados(as) de contratos de personal externo.
- Los(as) encargados(as) de docencia.
- Los(as) encargados(as) de auditorías (en caso de auditores externos).
- Y de toda persona responsable de personal con acceso a sistemas o servicios del HBLT, debe informar formalmente al DGTI sobre el término de funciones, ya sea por alejamiento, finalización de becas, término de contratos o cambios de personal, entre otros.

Esta notificación debe realizarse utilizando los formularios establecidos (los mismos usados para la creación de cuentas, marcando la opción de eliminación), con el fin de revocar oportunamente los accesos a los sistemas y servicios del HBLT.

A su vez, deberán informar al Departamento de Gestión de las Personas, sobre estos alejamientos, por las vías que éste defina.

4. Gestión de Cuentas Privilegiadas

- Los sistemas no deben tener cuantas privilegiadas o de administrador, que puedan ser solicitadas por usuarias y usuarios del HBLT.
- Estas cuentas solamente serán otorgadas a usuarios claves, con capacitación del uso de ésta y autorización del dueño del sistema.
- Las contraseñas de cuentas privilegiadas deben ser robustas, únicas y gestionadas de forma segura (ej. mediante bóvedas de contraseñas).
- El uso de cuentas privilegiadas debe ser auditado y monitoreado de forma regular.
- Se deben identificar claramente las cuentas con privilegios administrativos o de alto nivel en los sistemas y aplicaciones.

Pese al alto privilegio las cuentas no pueden ser capaces de realizar un flujo completo dentro del proceso que apoya.

5. Revisión de los Derechos de Acceso

Los derechos de accesos deben ser revisados a intervalos regulares no mayores a 6 meses.

El Departamento de Gestión de las Personas, deberá enviar cada 6 meses, los alejamientos correspondientes a ese periodo, y que le fueron comunicados desde otras unidades organizacionales.

El DGTI revisará si los usuarios en el listado se les revocó el acceso.

II. ACCESO A REDES Y SERVICIOS

Los siguientes lineamientos tienen por objeto controlar el acceso a las redes y servicios del HBLT, desde el punto de vista de la integridad y seguridad de los recursos de información, a través de un adecuado manejo de los accesos del usuario, los derechos y privilegios asociadas al acceso de las redes y servicios.
A continuación, se describen los distintos accesos normados al HBLT:

1. Acceso a redes

- Todo funcionario o personal externo que realice labores en y para el HBLT, si la jefatura directa lo solicitase y sus funciones lo requiriesen, tendrán acceso a la red del HBLT.
- La solicitud de acceso a la red del HBLT, deberá ser formalizado por el solicitante, y autorizado por la jefatura directa, al DGTI por el método que éste último defina.
- Están prohibidos los equipos personales en la red del HBLT.
- Todo equipo para conectarse a la red del HBLT, deberá estar autorizado por el DGTI.
- Es el DGTI el único autorizado a dar credenciales de acceso a la red del HBLT.
- El usuario y contraseña es personal e intransferible, incluso a personas con mayor autoridad o grado.
- Los equipos que sean usados por más de un usuario, podrán tener cuenta genérica, pero ésta debe estar asignada a la jefatura del área, siendo esta persona responsable del acceso a la red.

2. Acceso a Servicios

- Todo funcionario o personal externo que realice labores en y para el HBLT, si la jefatura directa lo solicitase y sus funciones lo requiriesen, tendrán acceso a los servicios del HBLT.

- Todos los servicios del HBLT, deberán solicitar un usuario y una contraseña para poder acceder a éstos. Por lo cual, los usuarios deben haber sido previamente autorizados y cargados sus datos en los servicios.
- La solicitud de acceso a los servicios del HBLT deberá ser formalizado por el solicitante, y autorizado por la jefatura directa, al DGTI por el método que éste último defina.
- El usuario y contraseña es personal e intransferible, incluso a personas con mayor autoridad o grado.

3. **Acceso por VPN** (Virtual Private network)

Una VPN (Red Privada Virtual) es una tecnología que permite conectarse de forma segura a la red interna de una organización (como el HBLT), usando Internet.

- Esta es la única herramienta y método válido para ingresar a la red del HBLT y los servicios no publicados hacia internet.
- Para acceso a la red y servicios a través de una VPN, esta debe ser solicitada al DGTI, según la metodología que éste y MINSAL indiquen.
- El usuario y contraseña es personal e intransferible, incluso a personas con mayor autoridad o grado.

4. **Acceso a Internet**

- El servicio de Internet será restringido y con perfiles de navegación.
- Los accesos estarán definidos, según Perfil definido por MINSAL, el cual está determinado dependiendo del Rol que tenga dentro de la institución.
- Solamente podrán conectarse a internet usando los medios dispuestos por el HBLT y no podrá acceder a través de otros canales de proveedores de servicio de internet Externo.
- El uso equipos personales (banda ancha móvil, celulares u otros) para conectar equipos del HBLT hacia internet u otras redes, está prohibido.
- Solo se podrán utilizar los Browsers aprobados por el DGTI.
- La configuración de los Browser solo podrá ser autorizada y/o realizada por personal del DGTI.
- Los perfiles de navegación son los definidos por MINSAL.
- Está prohibido el acceso desde internet y descarga de material que infrinja las leyes vigentes de Chile, así como, la normativa interna del HBLT.

- Está prohibido publicar en internet información interna del HBLT, sin la debida autorización formal de las autoridades del HBLT.
- Está prohibido visitar sitios de entretenimiento, redes sociales y ocio. A menos que esté contemplado en lo estrictamente laboral.
- Todo archivo descargado desde internet, debe ser revisado por el Antivirus del equipo, de forma manual o automática.

III. PROCEDIMIENTOS RELACIONADOS A LAS POLITICAS DE SEGURIDAD DE CONTROL DE ACCESO, ACCESO A REDES Y SERVICIOS.

1. Procedimiento Administración de Acceso de Usuarios

El presente procedimiento tiene por objetivo establecer las directrices para la administración segura de los accesos de usuarios, garantizando que solo personal autorizadas puedan acceder a los sistemas, aplicaciones, redes y servicios, y previniendo accesos no autorizados.

a) Creación y baja de cuentas de usuarios

Las solicitudes de **CREACIÓN** de usuario en los sistemas:

- Toda solicitud la debe realizar la Jefatura del usuario interesado.
- Toda solicitud debe realizarse a través de formularios definidos por el DGTI para cada sistema.
- Todo formulario debe estar íntegramente completado y firmado por el interesado y su jefatura directa.
- La jefatura debe indicar el perfil/permisos que se le asignará al nuevo usuario.
- El formulario debe ser digitalizado (escaneados) a PDF y enviado a la "Mesa de Ayuda" de Soporte del DGTI, soportedgti.cabl@redsalud.gob.cl, detallando la solicitud, datos básicos del usuario: Nombre completo de quien requiere el acceso, Unidad o servicio, Anexo.
- Para los casos de creación masiva de registros de usuarios, se puede generar un (1) formulario indicando "Lista adjunta", una lista en Excel, y la misma lista impresa y firmada por la jefatura directa y los interesados(as). Y enviar todos los archivos como se indicó anteriormente.
- La solicitud (ticket), será revisada por el encargado de seguridad de la información y Ciberseguridad y el Supervisor de soporte (o quien defina el jefe del DGTI), si se aprueba, ambos firmarán el formulario. De no ser aprobado, se informará al usuario.

- El formulario firmado, será enviado por la misma vía (plataforma) e identificación de solicitud (número de ticket), a los administradores de los sistemas, según corresponda, para realizar la creación del registro de usuario en éste.
- Cada registro de usuario al ser creados en un sistema debe tener un identificador único, RUN o Pasaporte, en lo posible.
- Las credenciales de acceso serán entregadas únicamente al usuario que requiere el acceso. La vía por la cual se hará esta entrega, será telefónicamente, por correo electrónico o de la forma más segura posible.

Las solicitudes de **ELIMINACIÓN** de registros de usuarios en los sistemas:

- Toda solicitud la debe realizar la Jefatura del usuario al cual se le eliminará el registro.
- Toda solicitud debe realizarse a través de formularios definidos por el DGTI para cada sistema.
- Todo formulario debe estar íntegramente completado y firmado por la jefatura directa del usuario al cual se le eliminará el registro.
- El formulario debe ser digitalizado (escaneados) a PDF y enviado a la "Mesa de Ayuda" de Soporte del DGTI, soportedgti.cabl@redsalud.gob.cl.
- La solicitud (ticket), será revisada por el encargado de seguridad de la información y el Supervisor de soporte (o quien defina el jefe del DGTI), si se aprueba, ambos firmarán el formulario.
- El formulario firmado, será enviado por la misma vía (plataforma) e identificación de solicitud (número de ticket), a los administradores de los sistemas, según corresponda, para realizar la eliminación del registro de usuario en éste.
- Una vez realizada la eliminación del registro de usuario, se le informará al solicitante telefónicamente, por correo electrónico o de la forma más segura posible.

b) Modificación de registro de usuarios cambio de perfil/permiso

Las solicitudes de **NUEVO** perfil/permisos y/o **CAMBIO** registros de usuarios en los sistemas:

- Toda solicitud la debe realizar la Jefatura del usuario interesado.
- Toda solicitud debe realizarse a través de formularios definidos por el DGTI para cada sistema.
- Todo formulario debe estar íntegramente completado y firmado por el interesado y su jefatura directa.

- La jefatura debe indicar el nuevo perfil/permisos que se le asignará al usuario o modificación en su registro.
- El formulario debe ser digitalizado (escaneados) a PDF y enviado a la "Mesa de Ayuda" de Soporte del DGTI, soportedgti.cabl@redsalud.gob.cl, detallando la solicitud, datos básicos del usuario: Nombre completo de quien requiere el acceso, Unidad o servicio, Anexo.
- La solicitud (ticket), será revisada por el encargado de seguridad de la información y el Supervisor de soporte (o quien defina el jefe del DGTI), si se aprueba, ambos firmarán el formulario.
- El formulario firmado, será enviado por la misma vía (plataforma) e identificación de solicitud (número de ticket), a los administradores de los sistemas, según corresponda, para realizar el cambio de perfil/permiso o modificación en el registro de usuario.
- Una vez realizada la eliminación del registro de usuario, se le informará al solicitante telefónicamente, por correo electrónico o de la forma más segura posible.

2. Procedimiento Responsabilidades de los Usuarios

Establecer el Procedimiento de Seguridad de Responsabilidades de los Usuarios para todo usuario del HBLT que tengan acceso a la red, sistemas y aplicaciones. Con el objetivo de concientizar a los usuarios sobre su responsabilidad en la protección su información de autenticación.

- Al cambiar la contraseña el largo mínimo de ésta debe ser de 8 caracteres, el contenido de ésta debe tener como mínimo una (1) MAYUSCULA, un (1) número, minúsculas y caracteres especiales (por ejemplo, +, *, #).
- Si la contraseña es de tipo temporal, debe ser cambiada en el primer inicio de sesión.
- El usuario y/o contraseña no debe registrarse en papel o equipos móviles (salvo que utiliza una bóveda digital).
- La contraseña debe ser cambiada cuando exista alguna indicación de su posible divulgación.
- Se recomienda utilizar contraseñas:
  - Sean fáciles de recordar para evitar la necesidad de anotarlas o almacenarlas en lugares inseguros.
  - No se basen en información personal fácilmente deducible o accesible, como nombres, fechas, datos familiares o información visible en redes sociales.

- Eviten el uso de palabras comunes, incluyendo combinaciones predecibles.
- Estén libres de caracteres idénticos consecutivos, como "222" o "AAA", que reducen la imprevisibilidad de la contraseña.
- No se reutilicen contraseñas personales en entornos laborales, especialmente aquellas utilizadas en redes sociales, correos personales u otras plataformas externas.

- Se establece como excepción al acceso a equipamiento computacional asignado a terceros, únicamente en situaciones de ausencia justificada del titular (feriado legal, licencia médica u otras), y solo en caso de que dicho acceso sea estrictamente necesario para asegurar la continuidad operativa del área o servicio, y no exista una alternativa técnica viable que permita evitar la entrega de credenciales. En tales circunstancias, la entrega de usuario y contraseña quedará bajo la responsabilidad, voluntad y autorización expresa del usuario titular del equipo. Finalizado el periodo de ausencia, el titular deberá proceder obligatoriamente al cambio de contraseña. Esta excepción no será aplicable bajo ninguna circunstancia a los sistemas de información institucionales.
- No utilice la misma contraseña para distintos sistemas o aplicaciones.
- Mantener la confidencialidad de la información contenida, según lo establecido en la ley.
- Garantizar la Integridad de los datos ingresados y almacenado en los sistemas.
- El uso de los sistemas es exclusivamente para los fines previstos y no para otros propósitos.
- No compartir sus credenciales de acceso (usuario y contraseña) con tercero.
- La información contenida en los sistemas y servicios, se encuentra protegida por la Ley N°19.628, sobre protección de la vida privada, ley N°20.584, regula los derechos y deberes que tienen las personas en relación con acciones vinculadas a su atención en salud, así como otras relacionadas.

SANCIONES

El incumplimiento de las disposiciones establecidas en esta Política de Seguridad de Respaldo de la Información se considerará una infracción a las obligaciones de las funcionarias y funcionarios del Hospital Barros Luco Trudeau.

Las acciones u omisiones que contravengan esta política podrán dar lugar a responsabilidad administrativa, de acuerdo con lo dispuesto en la Ley N°18.834, sobre Estatuto Administrativo o la normativa de personal que resulte aplicable al infractor.

Dependiendo de la gravedad de la infracción, la afectación a la seguridad de la información, la reincidencia y el dolo o culpa con que se haya actuado, las medidas disciplinarias aplicables serán aquellas establecidas en el Estatuto Administrativo, que incluyen, entre otras:

- **Censura:** Reprensión por escrito que se anota en la hoja de vida del funcionario.
- **Multa:** Descuento de un porcentaje de la remuneración mensual.
- **Suspensión del empleo:** Privación temporal del ejercicio del cargo, con goce de parcial de remuneraciones.
- **Destitución:** Término de la relación laboral, por faltas graves a la probidad.

Adicionalmente, sin perjuicio de las responsabilidades administrativas, el incumplimiento grave de esta política, especialmente si involucra el acceso, divulgación o uso no autorizado de datos sensibles (como la ficha clínica), podría acarrear responsabilidad civil o penal, según lo establecido en la Ley N°19.628 sobre Protección de la Vida Privada y el Código Penal, así como otras leyes especiales que sancionen delitos informáticos o la vulneración de la confidencialidad de la información de salud.

Para el personal externo (proveedores y terceros autorizados), el incumplimiento de esta política dará lugar a las sanciones contractuales estipuladas en los contratos o convenios respectivos, sin perjuicio de las acciones legales que el Hospital pueda ejercer por los daños y perjuicios ocasionados.

3.- DÉJESE ESTABLECIDO que, el documento antes aprobado, por razones de continuidad y buen servicio, inicio su vigencia desde la fecha de la presente resolución exenta.

4.- DÉJESE ESTABLECIDO que, cualquier modificación a la presente Resolución Exenta, deberá ser ratificada por el correspondiente acto administrativo.

ANÓTESE, REGISTRESE Y PUBLIQUESE

SERVICIO DE SALUD M. SUR * DIRECTOR * HOSPITAL BARROS LUCO TRUDEAU

WALTER KEUPUCHUR MEZA
DIRECTOR
HOSPITAL BARROS LUCO TRUDEAU

JENNY CANCINO QUIROZ
MINISTRA DE FE - HBLT

Distribución:
Dirección HBLT
Subdirección Administrativa
Subdirección Gestión Clínica
Subdirección Gestión y Desarrollo de las Personas
Subdirección Médica Atención Cerrada
Subdirección Médica Área Quirúrgica
Subdirección Médica Atención Abierta
Subdirección Gestión de Usuarios
Subdirección Unidades de Apoyo
Enfermera Coordinadora de Atención Cerrada
Enfermera Coordinadora de Atención Abierta
Depto. De Atención a las Personas
DGTI
Oficina de Partes

MINISTRO DE FE