PROTOCOLO DE GESTIÓN DE ACCESOS A SISTEMAS DE INFORMACIÓN

HOSPITAL METROPOLITANO DE SANTIAGO (HOSMET)

Versión: 2.0
Fecha de Actualización: Febrero 2026
Responsable:

ÍNDICE

---

1. INTRODUCCIÓN Y PROPÓSITO

El Hospital Metropolitano de Santiago (HOSMET), en el marco de su estrategia de transformación digital y en estricto cumplimiento de la Ley N° 21.663 (Ley Marco de Ciberseguridad), Ley N° 20.584 y normativas MINSAL, establece este protocolo para regular

el ciclo de vida completo de las identidades digitales en los sistemas de información clínica y administrativa.

El propósito es establecer un marco normativo, técnico y administrativo claro, seguro y eficiente que garantice la integridad, confidencialidad y disponibilidad de la información clínica, mitigando riesgos de accesos no autorizados y fugas de información sensible. Este protocolo es aplicable a toda persona que, por la naturaleza de sus funciones, requiera acceso a los sistemas, independientemente de su vínculo contractual con la institución.

---

2. OBJETIVO GENERAL

Establecer y garantizar que los procedimientos para la creación, activación, modificación, inactivación y gestión general de cuentas de acceso a los sistemas institucionales se realicen de manera eficiente, segura, trazable y conforme a las políticas de seguridad de la información del HOSMET, asegurando que cada usuario posea únicamente los privilegios necesarios para el desempeño de su labor.

---

3. ALCANCE Y APLICABILIDAD UNIVERSAL

Este protocolo es de cumplimiento obligatorio para todo individuo que requiera el uso de los sistemas institucionales para el desempeño de sus funciones asignadas dentro del HOSMET, independientemente de su calidad jurídica:

- Personal de Planta, Contrata y Honorarios.
- Personal en calidad de Reemplazo o Suplencia.
- Becados, Internos y Residentes de profesiones de la salud (gestionados vía Unidad RAD).
- Estudiantes en práctica o pasantías curriculares (debidamente autorizados y supervisados).
- Personal de empresas externas (terceros) que presten servicios al Hospital y requieran acceso justificado.
- Personal en comisión de servicio.
- Voluntariado autorizado con funciones que impliquen uso del sistema.

Sistemas cubiertos: Registro Clínico Electrónico (HIS), RIS-PACS, LIS, Anatomía Patológica, ERP, Correo Institucional, entre otros sistemas de información clínica y administrativa.

Condición de aplicación: La aplicación de este protocolo está condicionada a la previa y exitosa finalización del proceso de Habilitación Institucional Unificada correspondiente al tipo de colaborador (ver Sección 5).

---

4. DEFINICIONES CLAVE

Basadas en estándares de ciberseguridad (ISO 27001) y adaptadas al contexto institucional:

- Tríada CIA: Pilares de la seguridad de la información: Confidencialidad (acceso solo para autorizados), Integridad (exactitud y completitud de la información) y Disponibilidad (acceso para autorizados cuando lo requieran).
- Principio de Mínimo Privilegio: Restringir los derechos de acceso al nivel mínimo necesario para realizar las funciones laborales.
- Necesidad de Saber (Need-to-know): Acceso limitado solo a la información necesaria para cumplir una tarea específica.
- Segregación de Funciones (SoD): Control para asegurar que las responsabilidades de solicitar, autorizar y ejecutar un acceso recaigan en distintas personas o unidades.
- Habilitación Institucional Unificada: Proceso obligatorio y sin excepciones gestionado por RRHH y/o la Unidad RAD, según corresponda, que certifica el vínculo legal o contractual vigente del usuario con el hospital.
- Constancia de Habilitación Institucional: Documento oficial emitido por RRHH o RAD que acredita la identidad, el rol y la condición contractual del colaborador. Es el único documento válido para iniciar solicitudes de acceso.
- Grupo de Seguridad: Conjunto de permisos predefinidos en los sistemas que determinan las funcionalidades a las que un usuario puede acceder.
- Perfil de Acceso: Configuración específica dentro de un Grupo de Seguridad que puede refinar los accesos.
- Cuenta Activa: Cuenta de usuario habilitada para acceder a los sistemas.
- Cuenta Inactiva: Cuenta de usuario deshabilitada temporal o permanentemente.
- IAM (Identity and Access Management): Gestión de identidades y accesos.
- Trazabilidad: Capacidad de reconstruir la historia de uso de un sistema (quién, qué, cuándo) mediante logs.
- Colaborador: Término genérico que engloba a toda persona que requiera acceso a los sistemas por funciones clínicas o administrativas asignadas por el HOSMET.
- Calidad jurídica: Posición o estatus legal que adquiere el personal al integrarse contractualmente al hospital (planta, contrata, honorarios, externos, becados, etc.).

- Jefe de Unidad de Gestión de la Información: Responsable de la gestión operativa de las cuentas, reemplazando funciones de Mesa de Servicio mientras esta función no se encuentre operando en el hospital.
- Departamento de Tecnologías de la Información (TI): Responsable de la supervisión del cumplimiento del protocolo, definición de grupos de seguridad, auditorías y resolución de incidentes.

---

5. HABILITACIÓN INSTITUCIONAL UNIFICADA (PRERREQUISITO OBLIGATORIO)

El acceso a los sistemas de información clínica y administrativa es un privilegio otorgado únicamente a colaboradores que han sido formalmente validados a través del proceso de Habilitación Institucional Unificada.

- Obligatoriedad y Universalidad: Este proceso es obligatorio y sin excepciones para todo individuo que requiera acceso a sistemas, independientemente de su profesión, rol o tipo de vínculo con la institución.
- Gestión del Proceso:
    - RRHH es responsable para funcionarios (planta, contrata), personal a honorarios, comisiones de servicio y personal de empresas externas.
    - La Unidad RAD es responsable para becados, internos, estudiantes y otros colaboradores bajo convenios docentes asistenciales.
- Resultado del Proceso: La emisión de la "Constancia de Habilitación Institucional", que debe especificar de manera explícita la condición contractual del colaborador, el servicio de destino y la vigencia (fechas de inicio y término). Este documento es la única fuente de verdad para la gestión de accesos.
- Responsabilidad de la Jefatura: La Jefatura solicitante es responsable de asegurar que el colaborador haya completado este proceso y cuente con su Constancia de Habilitación antes de iniciar cualquier solicitud de acceso.

---

6. PRINCIPIOS GENERALES DE GESTIÓN DE ACCESO

1. Principio de menor privilegio: Cada usuario debe tener acceso únicamente a los datos y funcionalidades necesarias para el desempeño de sus funciones.

2. Individualidad e intransferibilidad: Las credenciales son personales e intransferibles. Está estrictamente prohibido compartir usuarios y contraseñas.
3. Acceso condicionado a habilitación previa: Ningún colaborador podrá acceder a los sistemas sin contar con la Constancia de Habilitación vigente emitida por RRHH o RAD.
4. Justificación funcional: Todo perfil o permiso asignado debe estar respaldado por una necesidad operativa explícita, validada por la jefatura directa.
5. Control y trazabilidad: Todas las acciones vinculadas a la gestión de accesos deben quedar registradas formalmente en el sistema de gestión interna, garantizando trazabilidad ante auditorías.
6. Temporalidad y revisión periódica: Los accesos se mantendrán vigentes sólo mientras exista una función formal o vínculo activo con el hospital. Las jefaturas deben revisar semestralmente la vigencia de los accesos.
7. Seguridad de la información: Todo acceso debe cumplir con los lineamientos de confidencialidad, integridad y disponibilidad establecidos en la normativa legal vigente y en las políticas internas del HOSMET.
8. Autorización Jerárquica: Toda solicitud debe ser visada y firmada por el Jefe de Servicio o Unidad respectivo (Dueño del Activo).
9. Formalidad Técnica: Todas las acciones (solicitud, validación, ejecución) deben quedar registradas en el sistema de gestión interna de la Unidad de Gestión de la Información.

---

7. ROLES Y RESPONSABILIDADES

COLABORADOR SOLICITANTE:

- Completar satisfactoriamente su proceso de Habilitación Institucional.
- Cumplir con las políticas de seguridad y uso de contraseñas.
- Informar a su jefatura sobre cambios de rol que requieran modificación de accesos.
- Responsable del uso ético y legal de su cuenta.
- Reportar cualquier incidente o actividad sospechosa relacionada con su acceso.

JEFATURA / SUPERVISOR / REFERENTE DESIGNADO DE UNIDAD/SERVICIO:

- Asegurar que el colaborador haya completado su Habilitación Institucional antes de iniciar la solicitud de acceso.

- Validar la necesidad de acceso y el perfil solicitado, en coherencia con las funciones definidas.
- Firmar el formulario de solicitud correspondiente, autorizando la creación, modificación o inactivación.
- Notificar formalmente a RRHH o RAD sobre desvinculaciones, traslados o cambios de función del personal a su cargo, con la debida antelación.
- Notificar al Jefe de Unidad de Gestión de la Información para la inactivación INMEDIATA de cuentas en caso de desvinculaciones.
- Participar en las revisiones semestrales de acceso de su personal.

RRHH / UNIDAD RAD:

- Ejecutar el Protocolo de Habilitación Institucional Unificada para todos los colaboradores bajo su esfera de competencia.
- Emitir la "Constancia de Habilitación Institucional" oficial, asegurando que contenga toda la información requerida (identidad, rol, condición contractual, servicio, vigencia).
- Notificar formalmente al Jefe de Unidad de Gestión de la Información sobre las vinculaciones (una vez habilitadas) y, de manera prioritaria e inmediata, las desvinculaciones de todo colaborador.

JEFE DE UNIDAD DE GESTIÓN DE LA INFORMACIÓN (Funciones de Mesa de Servicio y Gestión Técnica):

- Recepcionar y validar las solicitudes de gestión de cuentas (creación, activación, modificación, inactivación).
- Validar que la "Constancia de Habilitación Institucional" adjunta sea legítima, completa y contenga la información contractual del solicitante. Rechazar solicitudes sin este documento o con información ambigua.
- Crear, activar, inactivar y modificar perfiles en los sistemas según los procedimientos.
- Registrar cada acción en el sistema de gestión interna y en las planillas designadas.
- Notificar al usuario la creación/activación de su cuenta y los pasos para el primer acceso.
- Gestionar el reseteo de contraseñas, verificando la identidad del usuario.
- Ejecutar los procesos de inactivación programada o por inactividad.
- Escalar problemas o solicitudes complejas al Departamento de TI.

DEPARTAMENTO DE TECNOLOGÍAS DE LA INFORMACIÓN (TI) (Funciones de Supervisión y Auditoría):

- Supervisar el cumplimiento de este protocolo.
- Definir y mantener los Grupos de Seguridad y Perfiles de Acceso estándar, en conjunto con las unidades clínicas y administrativas.
- Realizar auditorías de seguridad y cumplimiento.
- Resolver y/o escalar incidentes y problemas técnicos reportados.
- Velar por la correcta gestión de licencias de software.

DIRECCIÓN HOSMET:

- Aprobar el protocolo y definir la política de seguridad institucional.

---

8. PROCEDIMIENTO DE SOLICITUD Y CREACIÓN DE CUENTAS NUEVAS

Descripción: Creación de usuario nuevo en los sistemas para un colaborador debidamente habilitado.

Requisitos previos:

1. El colaborador debe contar con su "Constancia de Habilitación Institucional" vigente, emitida por la unidad correspondiente (RRHH o RAD).
2. El colaborador ha completado la capacitación específica obligatoria (ver Sección 13) y cuenta con su certificado de aprobación.

Proceso de Solicitud (Jefatura):

1. Completar el Formulario Único de Solicitud de Acceso (Anexo A) con todos los datos requeridos (Nombre Completo, RUN, Profesión, Funciones, Servicio, Fechas de vigencia).
2. Asegurar que el colaborador haya firmado el Acuerdo de Confidencialidad (Anexo C).
3. Enviar la solicitud al correo designado (ej: gestionaccesos@hosmet.cl), adjuntando:
    - Copia de la Constancia de Habilitación Institucional.
    - Formulario de Solicitud completo y firmado por la jefatura.
    - Acuerdo de Confidencialidad firmado.

- Certificado de Capacitación (o constancia de agendamiento).

Pasos a seguir (Jefe de Unidad de Gestión de la Información):

1. Verificar la presentación, validez y completitud de la Constancia de Habilitación.
2. Verificar la completitud y firma del formulario de solicitud y del Acuerdo de Confidencialidad.
3. Verificar que el usuario cuente con certificación de capacitación vigente. De lo contrario, agendar la formación antes de proceder.
4. Crear el usuario en los sistemas asignando el Grupo de Seguridad y Perfil de Acceso validados.
5. Registrar la solicitud y la acción en el sistema de gestión interna (un registro por usuario).
6. Completar los datos en la planilla maestra "Cuentas Creadas" (RUN, nombre, grupo de seguridad, perfil, fecha de creación, servicio, jefatura autorizante).
7. Notificar al usuario y a su jefatura la creación de su cuenta.
8. Coordinar la entrega segura de las credenciales (de forma presencial validando identidad con cédula, o mediante método cifrado previamente establecido).

---

9. PROCEDIMIENTO DE ACTIVACIÓN DE CUENTAS EXISTENTES

Descripción: Reactivación de cuenta para un colaborador que, teniendo una cuenta previamente creada pero inactiva, retoma funciones en el establecimiento.

Requisitos:

1. Solicitud formal enviada por la jefatura directa al correo designado, indicando el motivo de la activación y confirmando la vigencia del vínculo laboral/funcional.
2. Si el perfil de acceso o los datos no han cambiado, no es necesario reenviar el formulario original completo, salvo que la jefatura lo considere necesario.
3. Caso especial: Si la cuenta ha permanecido inactiva por un período superior a 90 días, el Jefe de Unidad de Gestión de la Información podrá requerir una revalidación de la habilitación institucional ante RRHH o RAD antes de proceder.

Pasos a seguir (Jefe de Unidad de Gestión de la Información):

1. Verificar que la cuenta exista en los sistemas y se encuentre en estado inactivo.
2. Activar la cuenta en los sistemas.
3. Registrar la acción de activación en el sistema de gestión interna.

4. Completar los datos en la planilla "Activación de Cuentas" (fecha, RUN, nombre, servicio, perfil).
5. Notificar al usuario y a su jefatura sobre la reactivación de la cuenta.
6. Entregar una contraseña temporal o instrucciones para el reseteo, si es necesario, mediante un método seguro.

---

10. PROCEDIMIENTO DE INACTIVACIÓN DE CUENTAS

Descripción: Medida fundamental para garantizar la seguridad del sistema, optimizar licencias y evitar accesos indebidos. Se ejecuta bajo tres modalidades:

- Revocación Definitiva (Leavers): Por término del vínculo contractual o funcional. RRHH/RAD debe informar en un plazo máximo de 24 horas. El bloqueo debe ser efectivo inmediatamente al término del vínculo.
- Inhabilitación Temporal: Por licencias médicas prolongadas, vacaciones superiores a 15 días o procesos sumarios internos. La Jefatura debe informar para proceder al bloqueo preventivo.
- Inhabilitación por Inactividad Técnica: Cuentas sin log-in en 60 días son bloqueadas automáticamente por el sistema o mediante revisión manual mensual.

Pasos a seguir (Jefe de Unidad de Gestión de la Información):

1. Recepción de la notificación formal (de RRHH, RAD o la Jefatura).
2. Inactivación inmediata de la cuenta en todos los sistemas.
3. Registrar la acción de inactivación en el sistema de gestión interna, especificando el motivo (término de contrato, licencia, inactividad).
4. Completar los datos en la planilla "Registro de Revocación de Accesos" (Anexo E).
5. Notificar a la jefatura del colaborador (cuando aplique) sobre la acción ejecutada.

---

11. PROCEDIMIENTO DE MODIFICACIÓN DE PERMISOS

Descripción: Ajuste de los permisos de un usuario debido a un cambio de funciones, rol o traslado interno (Movers).

Requisitos:

1. Nueva solicitud mediante el Formulario Único (Anexo A), indicando el nuevo perfil requerido y la justificación funcional del cambio.
2. Validación y firma de la jefatura directa del colaborador.
3. Para cambios sustanciales de rol o estamento (ej: de Interno a Médico), puede requerirse una actualización del proceso de habilitación con RRHH o RAD.

Pasos a seguir (Jefe de Unidad de Gestión de la Información):

1. Validar la solicitud de modificación y su justificación.
2. Aplicar el principio de "Reset de Privilegios" en caso de traslado de servicio: se eliminan todos los permisos del servicio de origen y se configuran desde cero los del nuevo servicio.
3. Para modificaciones puntuales (aumento/reducción de permisos dentro del mismo servicio), ajustar el Perfil de Acceso según lo solicitado y validado.
4. Registrar la modificación en el sistema de gestión interna y en la planilla correspondiente.
5. Notificar al usuario y a su jefatura sobre los cambios realizados.

---

12. GESTIÓN DE CONTRASEÑAS

- Creación y Entrega Inicial:
    - Las contraseñas iniciales serán temporales y generadas por el sistema o por el Jefe de Unidad.
    - Se entregarán de forma segura (ej: correo personal institucional verificado, entrega presencial con validación de cédula, portal de auto-servicio con autenticación previa).
    - El usuario DEBERÁ cambiar su contraseña en el primer inicio de sesión.
- Complejidad y Seguridad (Política):
    - Mínimo 10 caracteres.
    - Combinación obligatoria de mayúsculas, minúsculas, números y símbolos.
    - No debe contener información personal fácilmente deducible (nombres, fechas, RUN).
    - No debe ser igual al nombre de usuario.
    - No debe reutilizar las últimas 5 contraseñas.
- Caducidad: Cambio de contraseña obligatorio cada 90 días. El sistema notificará con antelación.
- Bloqueo por Intentos Fallidos: Tras 5 intentos fallidos consecutivos, la cuenta se inhabilitará por 30 minutos o hasta una intervención manual del Jefe de Unidad.

- Reseteo de Contraseña: El usuario debe contactar directamente al Jefe de Unidad de Gestión de la Información. Se verificará su identidad mediante preguntas de seguridad predefinidas o validación presencial antes de proceder al reseteo.

---

13. CAPACITACIÓN ESPECÍFICA EN SISTEMAS INSTITUCIONALES

- Distinción: Esta capacitación es específica para el uso funcional y seguro de los sistemas institucionales (HIS, LIS, etc.). Es posterior y complementaria al proceso de Habilitación Institucional.
- Obligatoriedad: Todo colaborador, una vez habilitado institucionalmente, y antes de recibir acceso efectivo a los sistemas, deberá completar satisfactoriamente esta capacitación.
- Gestión y Contenidos (Responsable: Unidad de Gestión de la Información):
    - Módulo 1: Navegación funcional del sistema principal (HIS) y sistemas asociados.
    - Módulo 2: Marco legal de la ficha clínica electrónica, derechos del paciente (Ley 20.584) y responsabilidades del usuario.
    - Módulo 3: Taller de ciberseguridad básica: manejo seguro de contraseñas, identificación de phishing, reporte de incidentes.
- Evaluación: El usuario debe aprobar un test de conocimientos teórico-práctico con un mínimo de 85%.
- Certificación: El Jefe de la Unidad de Gestión de la Información emitirá un certificado digital de aprobación (Anexo D). La cuenta del usuario solo será activada o creada una vez que el folio de este certificado sea ingresado en su registro.

---

14. AUDITORÍA Y CONTROL

- Revisión Periódica de Jefaturas (Semestral): Cada 6 meses, los Jefes de Servicio/Unidad deben recibir, revisar y validar por escrito el listado de todos los usuarios con acceso activo en su área, confirmando la vigencia del vínculo y la pertinencia de los perfiles.
- Auditoría Interna Operativa (Mensual): El Jefe de Unidad de Gestión de la Información realizará controles mensuales enfocados en:
    - Detección de cuentas inactivas (>60 días sin login).
    - Cruce de listas de usuarios activos con las bases de datos de habilitaciones vigentes de RRHH/RAD.

    - Verificación del cierre oportuno de accesos.
- Auditoría de Logs de Seguridad (Mensual/Aleatoria): La Unidad de Gestión de la Información, en coordinación con el Departamento de TI, realizará revisiones mensuales aleatorias de los logs de acceso, enfocándose en:
    - Accesos a fichas clínicas de alto perfil (pacientes públicos, personal del hospital).
    - Patrones de búsqueda o consulta inusuales (volumen, horarios, datos).
    - Intentos de acceso fallidos masivos.
- Auditoría de Cuentas Privilegiadas (Trimestral): Se auditarán trimestralmente las cuentas con permisos de administrador o altos privilegios en cualquier sistema, para asegurar que no existan privilegios excesivos, no justificados o cuentas compartidas.

---

15. FLUJOGRAMA GENERAL DE GESTIÓN DE ACCESOS

FLUJO PRINCIPAL (ALTA/MODIFICACIÓN):

1. HABILITACIÓN: Ingreso y registro formal en RRHH o Unidad RAD. Emisión de Constancia de Habilitación Institucional.
2. SOLICITUD: Jefatura completa y firma Formulario Único (Anexo A) y asegura firma del Acuerdo de Confidencialidad (Anexo C). Envía solicitud con documentación.
3. VALIDACIÓN TÉCNICA: Jefe de Unidad de Gestión de la Información valida habilitación, documentación y requisitos.
4. CAPACITACIÓN (HITO CRÍTICO): Usuario realiza capacitación obligatoria y aprueba evaluación. Se emite Certificado (Anexo D).
5. EJECUCIÓN: Con certificado en regla, se crea/modifica la cuenta en los sistemas, asignando perfil validado.
6. ENTREGA SEGURA: Se notifica y se entregan credenciales de forma segura (presencial/cifrada).
7. MANTENIMIENTO: Auditoría semestral por jefatura, controles mensuales de inactividad y revisiones periódicas de seguridad.

FLUJO DE BAJA:

1. Notificación de Término → RRHH/RAD (formal) y Jefatura (inmediata) → Jefe de Unidad de Gestión de la Información → Inactivación INMEDIATA → Registro en Anexo E.

---

16. ANEXOS (FORMULARIOS TIPO)

- Anexo A: Formulario Único de Solicitud de Acceso / Modificación de Permisos.
- Anexo B: Formulario de Solicitud de Inactivación de Acceso.
- Anexo C: Acuerdo de Confidencialidad y Uso Responsable de Activos de Información.
- Anexo D: Constancia de Capacitación y Aprobación Técnica (Certificado).
- Anexo E: Registro de Revocación/Inactivación de Accesos.
- Anexo F: Modelo Referencial de Constancia de Habilitación Institucional (RRHH/RAD).
