N°277 -2025/HAPCSR-II-2-DE-OPE

RESOLUCIÓN DIRECTORIAL

Veintiséis de Octubre, 03 JUN 2025

VISTO: El Informe Nº 114-2025 /HAPCSRII-2.430020177 de fecha 15 de mayo del 2025, emitido por la Unidad de Estadística e Informática del Hospital de la Amistad Peru Corea Santa Rosa II-2, mediante el cual se solicita revisar y aprobar la Directiva "Gestión de Cuentas de Usuarios para el Acceso a los Sistemas y Servicios Informáticos del Hospital de la Amistad Perú Corea Santa Rosa II-2", y;

CONSIDERANDO:

Que, mediante la Ley General de Salud N° 26842, se establece que la salud es condición indispensable del desarrollo humano y medio fundamental para alcanzar el bienestar individual y colectivo, siendo la protección de la salud de interés público y responsabilidad del estado regularla, vigilarla y promoverla.

Que, mediante Resolución Ministerial N° 004-2016-PCM, se aprueba el uso obligatorio de la Norma Técnica Peruana "NTP-ISO-IEC 27001:2014, Tecnología de la Información. Técnicas de seguridad. Sistema de Gestión de Seguridad de la Información. Requisito 2da edición, en todas las entidades integrantes del Sistema Nacional de Informática; la cual señala como aplicar los "Objetivos de Control y Controles", los controles que la organización debe definir y aplicar a los procesos de tratamiento de riesgos de seguridad de la información. Así, en el acápite A.9 "Control de Acceso", el punto A.9.2 "Gestión de acceso al usuario" el cual tiene como objetivo asegurar el acceso de usuarios autorizados y prevenir el acceso no autorizado a los sistemas y servicios, así mismo contienen 6 controles respecto a la gestión de accesos, entre los cuales se puede destacar al punto A.9.2.1 "Registro y baja de usuarios" y A.9.2.2 "Aprovisionamiento de acceso a usuario";

Que, mediante Decreto Legislativo N° 1412, se aprueba la Ley de Gobierno Digital, la cual en su artículo 32: Gestión del Marco de Seguridad Digital del Estado Peruano, establece que, dentro del ámbito Institucional, "Las entidades de la Administración Pública deben establecer, mantener y documentar un Sistema de Gestión de Seguridad de la Información (SGSI)".

Que, el numeral 4 del artículo 5 del Decreto de Urgencia N° 006-2020, norma que creó el Sistema Nacional de Transformación Digital, señala como una de sus finalidades la de fortalecer el acceso y la inclusión a las tecnologías digitales en el país y la confianza digital fomentando la seguridad, transparencia, protección de datos personales y gestión ética de las tecnologías en el entorno digital para la sostenibilidad, prosperidad y bienestar social y económico del país;

Que, el numeral 9.3 del artículo 9 del Decreto de Urgencia N° 007-2020, norma que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento, establece que las entidades de la administración pública deben implementar, entre otros, un Sistema de Gestión de Seguridad de la Información (SGSI);

Que, con Informe Nº 114-2025 /HAPCSRII-2.430020177 de fecha 15 de mayo del 2025, el Jefe de la Unidad de Estadística e Informática del Hospital de la Amistad Perú Corea Santa Rosa II-2, solicita revisar y aprobar la Directiva "Gestión de Cuentas de Usuarios para el Acceso a los Sistemas y Servicios Informáticos del Hospital de la Amistad Perú Corea Santa Rosa II-2.

Veintiséis de Octubre,

INFORME N° 114 -2025/HAPCSRP II-2-430020177

A : **CPC. JULISSA DEL PILAR MARCHENA CRUZ**
Jefe De Oficina De Planeamiento Estratégico del HAPCSRII.2

De : **ING. TEMÍSTOCLES EDUARDO FARFÁN PALACIOS**
JEFE DE LA UNIDAD DE ESTADÍSTICA E INFORMATICA

Asunto : **REVISIÓN DE POPUESTA DE DIRECTIVA**
Gestión De Cuentas De Usuarios Para El Acceso A Los Sistemas y Servicios Informáticos del HAPCSRII.2

Tengo a bien dirigirme a Usted para saludarlo y al mismo remitir a su despacho la Propuesta de la Directiva de Gestión de Cuentas de Usuario para el Acceso a los Sistemas y Servicios Informáticos del HAPCSRII.2, con el objetivo de mejorar el proceso de identificar, rastrear, controlar y gestionar el acceso de usuarios específicos a un sistema o aplicación.

Contar con la visacion de las Oficinas de Recursos Humanos, Logística y Asesoría Legal.

Sin otro en particular

Atentamente.

GOBIERNO REGIONAL PIURA
DIRECCION REGIONAL DE SALUD - PIURA
HOSPITAL DE LA AMISTAD PERU COREA SANTA ROSA II-2
Ing. Temistocles Eduardo Farfan Palacios
CIP N 122301
Jefe de la unidad de estadistica e informática

PROVEIDO OPE - HAPCSR II
A: Unidad de Organización y métodos
ASUNTO:
FOLIOS:
FECHA: 17 NOV 2025

GOBIERNO REGIONAL PIURA
DIRECCION REGIONAL DE SALUD PIURA
HOSPITAL DE LA AMISTAD PERU COREA SANTA ROSA II-2
OFICINA DE PLANEAMIENTO ESTRATEGICO
FOLIOS:
FECHA: 15 NOV 2025
HORA: 8:26
FIRMA:

---

c.c.
Archivo
TEFP/lml

“GESTIÓN DE CUENTAS DE USUARIO PARA EL ACCESO A LOS SISTEMAS Y SERVICIOS INFORMÁTICOS DEL HAPCSRII.2”

AÑO 2025

OBJETIVO

Establecer disposiciones para la creación, actualización y eliminación de cuentas de usuario requeridas para el acceso a los sistemas y servicios informáticos administrados por la Unidad de Estadística e Informática (en adelante UEI)

2. ÁMBITO DE APLICACIÓN

Esta directiva es aplicable a todas las unidades funcionales de la entidad que solicitan la asignación de cuentas de usuario para el acceso a los sistemas y servicios informáticos del HAPCSRII.2 administrados por la UEI.

3. BASE NORMATIVA

- Ley N° 28612, Ley que norma el uso, adquisición y adecuación del software en la Administración Pública, y su Reglamento aprobado mediante Decreto Supremo N° 024-2006-PCM.
- Ley N° 27815, Ley del Código de Ética de la Función Pública, y su Reglamento aprobado mediante Decreto Supremo N° 033–2005–PCM.
- Ley N° 27658, Ley Marco de Modernización de la Gestión del Estado, y su Reglamento aprobado mediante Decreto Supremo N° 030-2002-PCM.
- Ley N° 27444, Ley de Procedimiento Administrativo General, y su Texto Único Ordenado aprobado mediante Decreto Supremo N° 004-2019-JUS.
- Decreto Legislativo N° 1412, que aprueba la Ley de Gobierno Digital.
- Decreto Supremo Nº 029-2021-PCM que aprueba el Reglamento de la Ley de Gobierno Digital.
- Resolución Ministerial N° 004–2016–PCM, que aprueba el uso obligatorio de la Norma Técnica Peruana "NTP-ISO/IEC 27001:2014 - Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la información. Requisitos. 2ª. Edición", en todas las entidades integrantes del Sistema Nacional de Informática, así como su modificatoria.
- Resolución de Secretaría de Gestión Pública N° 006-2018-PCM/SGP, que aprueba la Norma Técnica N° 001-2018-PCM/SGP, "Implementación de la Gestión por Procesos en las Entidades de la Administración Pública". 3.11 Resolución Directoral N° 056 – 2017 – INACAL/DN, que aprueba la Norma Técnica Peruana "NTP-ISO/IEC 27002:2017 - Tecnología de la información. Técnicas de seguridad. Código de prácticas para controles de seguridad de la información. 1ª Edición".

4. DEFINICIONES

4.1 Glosario de Términos

Activo: Cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas), que tenga valor para la organización.

Alta: Dar acceso a un usuario a los sistemas y/o servicios del HAPCSRII.2

Autenticación: Métodos para garantizar que un sujeto sea quien dice ser (por ejemplo, contraseña, token, huella digital, etc.).

Autorización: Métodos para controlar qué acciones puede realizar un sujeto en un objeto (entidad a la que se accede).

Baja: Retirar el acceso a un usuario a los sistemas y/o servicios del HAPCSRII.2.

Cuentas de usuario: Colección de información que indica a un sistema las tareas que puede realizar un determinado usuario en el mismo, además de la información a la que puede tener acceso, los cambios que puede realizar en él y sus preferencias personales.

Identificación: Métodos para proporcionar a un sujeto (entidad que solicita acceso) con una identidad reconocible (por ejemplo, ID usuario o cuenta de usuario, IVA, número de seguro social, pasaporte, etc.).

Proceso: Conjunto de actividades mutuamente relacionadas o que interactúan, las cuales transforman entradas en salidas.

Phishing: Estafa que tiene como objetivo obtener datos privados de los usuarios, especialmente para acceder a sus cuentas o datos bancarios.

Seguridad de la información: Preservación de la confidencialidad, la integridad y la disponibilidad de la información.

Servicio: Ejecución de actividades, trabajo o deberes asociados a un producto

Sistema: Combinación de elementos organizados que interactúan para lograr uno o más propósitos establecidos.

Usuario: Individuo que se beneficia de un sistema o servicio durante su utilización.

4.2 Siglas

UEI: Unidad de Estadística e Informatica

HAPCSRII.2: Hospital de la Amistad Perú Corea Santa Rosa II.2

1. DISPOSICIONES GENERALES

1.1 La UEI es la unidad funcional encargada de la gestión de cuentas de usuarios para el acceso a los sistemas y servicios informáticos del HAPCSRII.2.

1.2 La UEI debe garantizar que solamente los usuarios autorizados accedan a los sistemas y servicios informáticos de la entidad, por ello administra las cuentas de usuario de todo el personal y/o terceros del HAPCSRII.2, otorgando los accesos y privilegios que hayan sido autorizados por los(as) Directores(as) de las unidades funcionales solicitantes.

1.3 La UEI podrá tomar las acciones de seguridad correspondientes a fin de salvaguardar la información institucional en el caso de usuarios que hayan transgredido las normas de acceso y uso de los activos de información del HAPCSRII.2.

1.4 Los usuarios deben mantener a salvo su información de autenticación, no compartiendo sus credenciales, asegurando que sus contraseñas no se divulguen o evitando el uso de registros de contraseñas (anotaciones en papel, archivos, etc.).

2. DISPOSICIONES ESPECÍFICAS

2.1 Del Formato de Altas y Bajas de Usuario

El Formato de Altas y Bajas de Usuario será utilizado para solicitar la creación, actualización o eliminación de cuentas de usuario de cualquier sistema o servicio que administre la UEI. El formato se adjunta en el Anexo N° 1 de la presente Directiva y contiene las siguientes secciones:

2.1.1 Identificación de Usuario

a. En la sección "Responsable de la cuenta", colocar los apellidos y nombres completos del usuario, así como su correo personal en caso se trate de una solicitud de creación de cuenta. Se debe especificar el correo institucional para los casos de actualización o eliminación de cuenta. Asimismo, se especificará el DNI, teléfono, cargo y si se trata de personal CAS, se marcará la casilla correspondiente con una "X".

b. Se debe especificar, además, el tipo de solicitud realizada: C: Crear, A: Actualizar y E: Eliminar.

Anexo Nº 01

N°	RESPONSABLE DE LA CUENTA						Crear(C) Actualizar(A) Eliminar(E)
	APELLIDOS Y NOMBRES (Deberá de consignar los 02 Apellidos)	CORREO PERSONAL / INSTITUCIONAL	DNI	TELÉFONO	CARGO O SERVICIO	Nombrado (N) CAS (C)	

2.1.2 Especificación de los accesos a otorgar

a. En la sección "Acceso a" se debe especificar los servicios o sistemas a los cuales se solicita dar accesos. En la casilla "Otros" se podrá especificar privilegios, accesos, o sistemas de información no especificados en el formato.

Anexo Nº 02

ACCESO A										
RED	INTERNET	CORREO ELECTRÓNICO	Servicio de telefonía				Sistemas de Información (colocar número de lista)			Otros
			Fijos	Celulares	Nacionales	Internacionales	Operador	Administrador	Consulta	

1.- SIGA (Sistema Integrado de Gestion Administrativa)
2.- SIAF (Sistema Integrado de Gestion Financiera)
3.- GalenHos (Sistema de Gestion Hospitalaria)
4.- SIGH (Aplicativo WEB-Gestion Hospitalaria)
5.- ASISPER (Asistencia y Permanencia)
6.- PACS (Archivo de Imágenes)

a. Cuando se solicite el acceso a sistemas de información, se debe especificar el número de sistema conforme a la lista ubicada en la parte inferior del formato, considerando el tipo de acceso a otorgar entre los cuales se detallan:

a.1 <u>Operador</u>

Usuarios que tendrán un manejo constante de los sistemas y requieren tener acceso a la operación básica de los mismos, lo cual es necesario dentro de la actividad que realizan.

a.2 Administrador

Usuario con mayores privilegios. Puede encargarse de manejar el sistema o tener la posibilidad de crear, actualizar o eliminar aspectos de la plataforma sobre la que trabaje.

a.3 Consulta

Usuario que solo puede realizar consultas y visualizar reportes.

1.2 De la solicitud de creación, actualización o eliminación de cuentas de usuario

1.2.1 Las solicitudes de creación, actualización o eliminación de cuentas de usuario podrán ser remitidas a la UEI mediante:

a. Correo electrónico Soporte Informático de UEI: soporteinfotmatico@hsantarosa.gob.pe ; El correo debe ser enviado desde una cuenta de correo institucional.
b. Memorándum a través del sistema de trámite documentario.

1.2.2 Las solicitudes deben adjuntar el Formato de Altas y Bajas de Usuario debidamente firmado por el/la Director/Administrador, responsable de la unidad funcional donde labora el usuario; de lo contrario, no podrán ser atendidas por la UEI.

1.2.3 Las solicitudes recibidas por la UEI para creación, actualización o eliminación de cuentas de usuario serán derivadas al equipo de Informatica para su atención. El diagrama del proceso de Gestión de Cuentas de Usuario que realiza la UEI se especifica en el Anexo N° 2.

1.2.4 Un usuario sólo puede contar con una cuenta por cada sistema o servicio al que se le autoriza acceder, la cual estará bajo su responsabilidad.

1.2.5 Las acciones realizadas por accesos no autorizados a sistemas o servicios informáticos, por parte de usuarios que se desvincularon de la entidad o que cambiaron de funciones y de los cuales no se haya solicitado la eliminación o actualización de sus cuentas, serán responsabilidad de jefe a de la unidad funcional a la que pertenecía o pertenece el usuario, según corresponda.

1.3 De la Creación de Cuentas de Usuario

1.3.1 Mediante la creación de una cuenta de usuario se asignan derechos y restricciones de acceso a la información a un usuario identificado.

1.3.2 Al solicitar a la UEI la creación de una cuenta de usuario, se debe considerar las competencias del usuario, los fines laborales y el uso racional de los activos informáticos a fin de especificar correctamente los activos informáticos a los que accederá y el nivel de acceso a otorgar.

1.3.3 Cuando se solicite asignación de perfiles con privilegios de administrador o uso de programas utilitarios privilegiados, se debe incluir una justificación en el formato de Altas y Bajas de Usuario en la sección "Observaciones", y debe contar con la firma del/de la Jefe/a de la unidad funcional que administra el proceso o sistema de información, en caso esta sea diferente a la de la unidad funcional solicitante.

1.3.4 La UEI, a través del Responsable del Área Informatica o quien haga sus veces, procederá a crear la cuenta de usuario y otorgar los accesos indicados en el Formato de Altas y Bajas de Usuario.

1.3.5 La UEI, a través del Responsable del Área Informatica o quien haga sus veces, comunicará mediante correo electrónico, la creación de la nueva cuenta de usuario. El Analista o quien haga sus veces asignará la atención al Soporte Tecnico reenviando el correo donde se especifican el nombre de usuario y la contraseña temporal establecida.

1.3.6 La UEI, a través del Soporte Técnico o quien haga sus veces, realizará, según corresponda, la configuración del perfil y/o de las aplicaciones y servicios para la cuenta de usuario creada.

1.3.7 La UEI a través del Soporte Tecnico o quien haga sus veces, coordina con el usuario para que ingrese con el usuario y contraseñas asignados, y lo asiste en el cambio de su contraseña. Asimismo, verifica que pueda acceder satisfactoriamente y que la configuración y accesos sean correctos.

1.3.8 La UEI informa mediante correo electrónico a la unidad funcional solicitante respecto a la atención realizada y

procede al cierre de la solicitud.

1.4 De la Actualización de Cuentas de Usuario

1.4.1 En los casos en que un usuario haya cambiado de unidad funcional y se reciba una solicitud de actualización de su cuenta (no habiéndose recibido previamente la solicitud de eliminación de la cuenta por parte de la unidad funcional a la que pertenecía el usuario), la UEI, a través del Responsable del Area Informatica o quien haga sus veces, procederá a revocar todos los accesos de la cuenta de usuario, para posteriormente actualizar la cuenta y otorgar los accesos indicados en el Formato de Altas y Bajas de Usuario.

1.4.2 En los casos en que un usuario haya cambiado de unidad funcional y se reciba una solicitud de actualización de su cuenta (habiéndose atendido previamente la solicitud de eliminación de la cuenta por parte de la unidad funcional a la que pertenecía el usuario), la UEI a través del del Responsable de Informatica o quien haga sus veces, procederá a crear la cuenta de usuario y configurar posteriormente la cuenta, otorgando los accesos indicados en el Formato de Altas y Bajas de Usuario.

1.4.3 La UEI, a través del Responsable del Área de Informatica o quien haga sus veces, comunicará mediante correo electrónico, la actualización de la cuenta de usuario. Se asignará la atención al Soporte Técnico reenviando el correo donde se especifican el nombre de usuario y la contraseña temporal establecida.

1.4.4 La UEI, a través del Soporte Técnico o quien haga sus veces realizará, según corresponda, la configuración del perfil y/o de los sistemas y servicios para la cuenta de usuario actualizada. Asimismo, coordina con el usuario para que ingrese con el usuario y contraseñas asignados, y lo asiste en el cambio de su contraseña. Además, verificará que pueda acceder satisfactoriamente y que la configuración y accesos sean correctos.

1.4.5 La UEI a través del Analista de Mesa de Ayuda informa

mediante correo electrónico a la unidad funcional solicitante respecto a la atención realizada y procede al cierre de la solicitud.

1.5 De la Eliminación de Cuentas de Usuario

1.5.1 Cuando se reciba una solicitud de eliminación de cuenta de usuario, la UEI, a través del responsable del Área Informatica o quien haga sus veces, realizará una copia de respaldo de la información contenida en el equipo que hubiera sido asignado al usuario. La información podrá ser entregada al usuario y/o custodiada por la UEI durante la vigencia del HAPCSRII.2.

1.5.2 La UEI, a través del Responsable del Área Informatica o quien haga sus veces, procederá a revocar todos los accesos y privilegios de la cuenta de usuario y a eliminar posteriormente la cuenta o cuentas asociadas al usuario (cuenta de red, de sistemas y servicios, etc.).

1.5.3 La UEI, a través del Responsable del Área Informatica o quien haga sus veces, comunicará mediante correo electrónico, la eliminación de la cuenta de usuario.

1.5.4 La UEI informa mediante correo electrónico a la unidad funcional solicitante respecto a la atención realizada y procede al cierre de la solicitud.

1.5.5 En los casos en que un usuario haya cambiado de unidad funcional y se reciba una solicitud de eliminación de su cuenta (habiéndose recibido previamente la solicitud de actualización de la cuenta por parte de la nueva unidad funcional a la que pertenece el usuario), no corresponderá la eliminación de la cuenta. La UEI, a través del Responsable del Área Informatica o quien haga sus veces, comunicará mediante correo electrónico a la Mesa de Ayuda que la cuenta fue actualizada previamente. El Analista de Mesa de Ayuda o quien haga sus veces informará a la unidad funcional solicitante respecto a la actualización previa de la cuenta.

1.5.6 La UEI eliminará de oficio las cuentas de usuario que identifique que pertenecen a personal que ya no labora en la entidad, o que hayan cambiado de funciones y dicho cambio no haya sido notificado mediante el procedimiento descrito en la presente Directiva. Lo mismo aplica para cuentas de usuario asignadas temporalmente a terceros los cuales ya no tengan vínculo con la entidad.

2. RESPONSABILIDADES

2.1 La UEI es responsable de:

2.1.1 Crear, actualizar o eliminar las cuentas de usuario para el acceso a los sistemas y servicios informáticos de la entidad.

2.1.2 Dar cumplimiento total, parcial, o denegar las solicitudes de creación o actualización de cuentas de usuario, de acuerdo con la disponibilidad de activos y licencias, restricciones técnicas de los sistemas de información y/o políticas de seguridad de la información.

2.1.3 En caso de detectarlo, poner en conocimiento del mal uso de los activos informáticos a la Unidad de Recursos Humanos, con copia al Director/a del Sistema Administrativo III, o el/la Director/a del Sistema Administrativo II responsable de la unidad funcional donde labora el usuario que realizó tal acción, a fin de que se adopten las medidas que correspondan, según las normas institucionales vigentes.

2.1.4 Registrar de manera sistematizada y automática los accesos a los activos informáticos por parte de los usuarios, contando con un control de los registros de cuentas de usuario y accesos (logs), ante cualquier auditoria que se requiera.

2.1.5 Mantener actualizado el registro de cuentas de usuario.

2.1.6 Mantener la versión actualizada del Formato de Altas y Bajas de Usuario.

2.2 Las Unidades Funcionales del HAPCSRII.2 son responsables de:

2.2.1 Solicitar a la UEI la creación, actualización o eliminación de cuentas de usuario, mediante Formato de Altas y Bajas de Usuario debidamente firmado por el/la Jefe responsable de la unidad funcional solicitante, según corresponda.

2.2.2 Informar oportunamente a la UEI mediante Formato de Altas y Bajas de Usuario, respecto a los usuarios que se desvincularon de la entidad (personal bajo cualquier modalidad de contratación o terceros), requerimientos de cambios de privilegios para una cuenta, bloqueo de accesos a usuarios que cambiaron de funciones, o de aquellos que ya no cuentan con autorizaciones para determinadas tareas, o de quienes han sufrido robo de credenciales de acceso o prácticas de phishing.

2.2.3 Informar a la UEI con copia la Unidad de Recursos Humanos respecto al uso indebido de las cuentas de usuario asignados al personal de la unidad funcional.

2.3 La Oficina de Recursos Humanos es responsable de:

2.3.1 Informar mensualmente a la UEI, de forma complementaria, la lista de los servidores cuyo vínculo laboral con el HAPCSRII.2 ha quedado extinguido, a fin de proceder a la eliminación de las cuentas de acceso a los activos informáticos.

2.4 La Oficina de Logística es responsable de:

2.4.1 Informar mensualmente a la UEI de forma complementaria, la lista de terceros (locadores de servicios) cuyo vínculo con la entidad ha quedado extinguido, a fin de que la UEI pueda proceder a la eliminación de las cuentas de acceso a los activos informáticos.

2.5 El Usuario es responsable de:

2.5.1 Utilizar de buenas prácticas de seguridad de la

información en el uso de información confidencial para la autenticación.

2.5.2 Preservar el uso de carácter personal e intransferible de sus cuentas de usuario y contraseñas, estando bajo su responsabilidad las acciones que se realicen con ellas, excepto los casos en que se haya reportado a la UEI y se haya comprobado fehacientemente la vulneración de sus cuentas.

2.5.3 Reportar a la UEI ante un indicio de pérdida de confidencialidad de la cuenta de usuario, o un evento que ponga en riesgo la seguridad de los activos de información a los cuales se le brindó acceso.

3. DISPOSICIONES COMPLEMENTARIAS

Las disposiciones no previstas en la presente Directiva serán resueltas por la UEI, conforme lo establecido en el Manual de Operaciones del HAPCSRII.2, y normatividad vigente aplicable al caso.