UNIDAD EJECUTORA TUMBES

UNIDAD EJECUTORA 002: SERVICIOS DE SANEAMIENTO TUMBES

DIRECTIVA QUE REGULA LA GESTIÓN DE ACCESO A LOS SISTEMAS DE INFORMACIÓN Y USO ADECUADO DE LOS EQUIPOS Y SERVICIOS INFORMATICOS DE LA UE002SST

DOCUMENTO INSTITUCIONAL

TUMBES – PERÚ

2026

PERÚ | Ministerio de Vivienda, Construcción y Saneamiento | Organismo Técnico de la Administración de los Servicios de Saneamiento | Unidad Ejecutora 002 "Servicios de Saneamiento Tumbes" | UNIDAD EJECUTORA TUMBES

Tipo de documento normativo	Código de documento normativo	Versión	Total, de páginas
DIRECTIVA	DIR-011-2026-UE002SST-GG	01	23

DIRECTIVA QUE REGULA LA GESTIÓN DE ACCESOS A LOS SISTEMAS DE INFORMACION Y USO ADECUADO DE LOS EQUIPOS Y SERVICIOS INFORMATICOS DE LA UE002SST

Etapa / Responsable	Firma
Elaborado por: Jino Luis Alva Cueva **Cargo:** Jefe de la Oficina de Tecnología de la información Oficial de Seguridad y Confianza Digital	UNIDAD EJECUTORA TUMBES Firmado digitalmente por: ALVA CUEVA Jino Luis FAU 20603799373 soft Motivo: Soy el autor del documento Fecha: 15/07/2026 12:23:40-0500
Revisado por: Nícida Gissela Paredes Hassen **Cargo:** Gerente General	UNIDAD EJECUTORA TUMBES Firmado digitalmente por: PAREDES HASEN Nicida Gissela FAU 20603799373 soft Motivo: Soy el autor del documento Fecha: 16/07/2026 17:18:03-0500
Revisado por: Karla Melissa Effio Albujar **Cargo:** Gerente de Operaciones	UNIDAD EJECUTORA TUMBES Firmado digitalmente por: EFFIO ALBUJAR Karla Melissa FAU 20603799373 soft Motivo: Soy el autor del documento Fecha: 15/07/2026 16:52:26-0500
Revisado por: Abad Cornejo Escobar **Cargo:**Gerente de Administración	UNIDAD EJECUTORA TUMBES Firmado digitalmente por: CORNEJO ESCOBAR Abad FAU 20603799373 soft Motivo: Soy el autor del documento Fecha: 15/07/2026 14:54:53-0500
Revisado por: Juan Manuel Vidau Vereau **Cargo**: Gerente Comercial	UNIDAD EJECUTORA TUMBES Firmado digitalmente por: VIDAL VEREAU Juan Manuel FAU 20603799373 soft Motivo: En señal de conformidad Fecha: 16/07/2026 11:27:26-0500
Revisado por: Julio Cesar Arévalo López **Cargo**: Gerente de Desarrollo y Presupuesto	UNIDAD EJECUTORA TUMBES Firmado digitalmente por: AREVALO LOPEZ Julio Cesar FAU 20603799373 soft Motivo: En señal de conformidad Fecha: 16/07/2026 09:21:26-0500
Revisado por: Heynar Adolfo Narro Tisnado **Cargo:** Gerente de Ingeniería, inversiones y Medio Ambiente	UNIDAD EJECUTORA TUMBES Firmado digitalmente por: NARRO TISNADO Heynar Adolfo FAU 20603799373 soft Motivo: Soy el autor del documento Fecha: 16/07/2026 15:49:17-0500
Revisado por: Esaú Alejos Liñán **Cargo:** Gerente de Asesoría Jurídica	UNIDAD EJECUTORA TUMBES Firmado digitalmente por: ALEJOS LIÑAN Esau FAU 20603799373 soft Motivo: Soy el autor del documento Fecha: 15/07/2026 15:00:18-0500

INDICE

1. OBJETIVO

Establecer la directiva que regula la gestión de accesos a los sistemas de información y el uso adecuado de los equipos y servicios informáticos en la Unidad Ejecutora 002 Servicio de Saneamiento Tumbes (UE002SST.

2. FINALIDAD

Mantener un registro de las solicitudes y proceso de atención de los requerimientos de acceso a los sistemas de información, equipos informáticos, redes y comunicaciones para incrementar la seguridad de los servicios e información de la entidad; así como, incrementar la vida útil y vigencia tecnológica de los equipos informáticos y reducir el número horas de soporte en reconfiguraciones y reinstalaciones como consecuencia de malas prácticas o uso inadecuado de sistemas, servicios o equipos de cómputo de la UE002SST.

3. ALCANCE

Las disposiciones son de aplicación obligatoria para las unidades de organización de la UE002SST.

4. BASE LEGAL

4.1. Ley N° 29733, Ley de Protección de Datos Personales.

4.2. Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital.

4.3. Decreto de Urgencia N° 006-2020, Decreto de Urgencia que crea el Sistema Nacional de Transformación Digital

4.4. Decreto de Urgencia N° 007-2020, que aprueba el marco de confianza digital. Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento

4.5. Decreto Supremo Nº 013-2003-PCM, que Dictan medidas para garantizar la legalidad de la adquisición de programas de software en entidades y dependencias del Sector Público.

4.6. Decreto Supremo N° 003-2013-JUS, que aprueba el Reglamento de la Ley Nº 29733,

Ley de Protección de Datos Personales.

4.7. Decreto Supremo N° 033-2018-PCM, que crea la Plataforma Digital Única del Estado Peruano y se establecen disposiciones adicionales para el desarrollo del Gobierno Digital.

4.8. Decreto Supremo N° 004-2019-JUS, Decreto Supremo que aprueba el Texto Único Ordenado de la Ley N° 27444 - Ley del Procedimiento Administrativo General.

4.9. Decreto Supremo N° 006- 2019-VIVIENDA que aprueba la primera sección del Reglamento de Organización y Funciones del Organismo Técnico de la Administración de los Servicios de Saneamiento - OTASS.

4.10. Decreto Supremo Nº 029-2021-PCM Decreto Supremo que aprueba el Reglamento del Decreto Legislativo Nº 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital, y establece disposiciones sobre las condiciones, requisitos y uso de las tecnologías y medios electrónicos en el procedimiento administrativo.

4.11. Decreto Supremo N° 157-2021-PCM, Decreto Supremo que aprueba el Reglamento del Decreto de Urgencia N° 006-2020, Decreto de Urgencia que crea el Sistema Nacional de Transformación Digital.

4.12. Decreto Supremo N° 007-2024-JUS, que aprueba el Reglamento de la Ley de Transparencia y Acceso a la Información Pública.

4.13. Resolución Ministerial N° 073-2004-PCM, que aprueba la Guía para la Administración Eficiente del Software Legal en la Administración Pública

4.14. Resolución de Secretaría de Gobierno y Transformación Digital N° 003-2023-PCM/SGTD, que establece la implementación y mantenimiento del Sistema de Gestión de Seguridad de la Información en las entidades públicas.

4.15. Resolución de Gerencia General N° 004-2025-UE002SST-GG, que aprueba el Plan de Aseguramiento de bienes muebles patrimoniales en el Organismo Técnico de la Administración de los Servicios de Saneamiento – OTASS",

4.16. Resolución Directoral N° 095-2018-OTASS-DE, formaliza la creación de la Unidad Ejecutora 002: denominada Servicios de Saneamiento Tumbes, en el Pliego 207:

Organismos Técnico de la Administración de los Servicios de Saneamiento.

4.17. Resolución de Presidencia Ejecutiva N° 063-2025-OTASS-PE, se aprueba el Manual de Gestión Operativa de la Unidad Ejecutora 002 Servicios de Saneamiento Tumbes.

4.18. Resolución de Gerencia General N° 036-2026-UE002SST-GG, que aprueba el Reglamento Interno de los Servidores Civiles de la Unidad Ejecutora 002 Servicios de Saneamiento Tumbes.

5. DEFINICIONES

5.1 Usuario: Persona autorizada para acceder a uno o más sistemas institucionales de la UE002SST de acuerdo con las funciones asignadas.

5.2 Rol: Conjunto de funciones asignadas a un usuario dentro de un sistema institucional, de acuerdo con el cargo o responsabilidades que desempeña.

5.3 Perfil de acceso: Conjunto de permisos y restricciones asignados a un usuario dentro de un sistema institucional, que determinan las opciones, módulos y acciones a las que puede acceder.

5.4 Usuario con privilegios administrativos: Usuario autorizado para realizar actividades de administración sobre los sistemas institucionales. Los privilegios administrativos podrán clasificarse en:

5.4.1 Administrador funcional: Usuario autorizado para gestionar parámetros operativos o funcionalidades específicas de un módulo o proceso institucional.

5.4.2 Administrador técnico: Usuario autorizado para realizar tareas técnicas de configuración, mantenimiento, soporte, gestión de usuarios o administración de infraestructura tecnológica.

5.5 Alta de usuario: Proceso mediante el cual se crea y habilita una cuenta de acceso a un sistema institucional.

5.6 Modificación de usuario: Proceso mediante el cual se actualizan roles, perfiles o permisos asignados a un usuario.

5.7 Baja de usuario: Proceso mediante el cual se deshabilita, bloquea o elimina el acceso de un usuario a los sistemas institucionales.

5.8 Cuenta de usuario: Identificador único asignado a una persona autorizada para acceder a un sistema institucional.

5.9 Privilegio: Permiso o nivel de acceso otorgado a un usuario para ejecutar determinadas acciones dentro de un sistema.

6. USO ADECUADO A LOS EQUIPOS Y SERVICIOS INFORMÁTICOS

6.1 Acceso a red inalámbrica – WIFI

a. La OTI es la responsable de gestionar las redes inalámbricas de la entidad.
b. La OTI es responsable de la administración de las conexiones a la red inalámbrica.
c. La UE002SST cuenta con una red inalámbrica **"Unifi"**.
d. La red inalámbrica **Unifi** forma parte de la red informática de la entidad y para conectarse se requiere contraseña y contar con permiso de acceso de OTI.
e. Para acceder a la red inalámbrica **Unifi**, el jefe/encargado de la oficina debe requerirlo mediante correo institucional.
f. El requerimiento debe incluir apellidos y nombres del propietario y número del equipo asignado a conectar.
g. En caso de contar con laptop personal el requerimiento en el correo debe indicar apellidos y nombres completos, nombre de la laptop y puesto para el que fue contratado.

6.2 Sobre el uso adecuado de los equipos y servicios informáticos

6.2.1 Instalación de equipos informáticos

a. El jefe o responsable del área debe de requerirlo mediante correo institucional, indicando los apellidos y nombres completos del trabajador que se hará responsable del bien y el cargo que este ocupa.

b. El jefe o encargado de la OTI procede al llenado del acta de entrega y movimiento de bienes activo fijo con las respectivas firmas de entrega y recepción por las oficinas involucradas.

c. Todo equipo informático será entregado únicamente con la firma de recepción en el acta correspondiente.

d. La OTI realiza el desplazamiento del equipo informático al sitio físico asignado al nuevo usuario, para proceder con su instalación.

e. Luego de la instalación, el usuario es responsable de la permanencia y conservación de cada uno de los equipos informáticos asignados.

6.2.2 Desplazamiento de equipos informáticos

a. Para el desplazamiento interno y la instalación de los equipos informáticos, se debe notificar a la OTI a través del correo institucional, adjuntando el acta de asignación en uso y el acta de devolución de bienes debidamente firmados.

b. Para el desplazamiento externo de los equipos informáticos, el área usuaria debe de encargarse de tramitar y obtener las firmas correspondientes de la Orden de salida, reingreso y desplazamiento interno del bien informático, luego se debe notificar a la OTI mediante el correo institucional adjuntando dicha orden firmada.

6.2.3 Uso de equipos informáticos

a. El usuario no tiene permitido modificar la configuración del software establecido en los equipos informáticos del UE002SST, y tampoco debe abrir y/o manipular los equipos informáticos de propiedad de la Entidad.

b. La instalación y configuración de programas utilitarios y servicios del sistema está restringido según los privilegios otorgados al usuario.

c. El usuario puede usar dispositivos de almacenamiento externo previa autorización del jefe o encargado de la oficina, debiendo tomar las precauciones de seguridad correspondientes.

d. Se encuentra habilitado el bloqueo automático de la sesión después de diez (10) minutos de inactividad del equipo informático, pero a pesar de ello, es responsabilidad del usuario bloquear su equipo informático, cuando tengan que ausentarse.

e. El usuario debe realizar el adecuado apagado de su equipo informático, al finalizar la jornada laboral.

f. El usuario no debe manipular las conexiones del equipo informático, esta tarea es reservada para el personal de la OTI.
g. Se encuentra prohibida la manipulación de bebidas y alimentos cerca a los equipos informáticos.
h. El usuario no debe eliminar los accesos directos de los aplicativos instalados por la OTI y ubicados en los escritorios de los equipos informáticos.
i. El usuario debe asegurar que las baterías de las computadoras portátiles, se encuentren con carga óptima.

6.2.4 Mantenimiento de equipos informáticos

a. El mantenimiento de los equipos informáticos debe ser realizado por personal de la OTI.
b. Los usuarios deben comunicar a la OTI mediante el correo institucional, si hubiese un incidente o falla con algún equipo informático, ante lo cual, el personal de OTI debe evaluar la falla para repararla o gestionar la garantía, según corresponda.

6.2.5 Gestión de contraseñas

a. La contraseña es confidencial e intransferible, el usuario es responsable de la seguridad de su contraseña y del uso adecuado de la misma.
b. La contraseña tiene un mínimo de ocho (08) hasta un máximo de treinta y dos (32) caracteres, debe ser alfanumérica (Mayúsculas, Minúsculas, Dígitos del 0 al 9, un carácter especial), y no puede contener el nombre o apellido del usuario.
c. Los usuarios son responsables del cambio de su contraseña, la cual debe realizarse al ser recibida
d. En caso algún usuario requiera recuperar su contraseña de los aplicativos o servicios informáticos de la UE002SST, debe solicitarla a la OTI a través del correo institucional. Asimismo, el usuario al recibir su nueva contraseña debe proceder a modificarla inmediatamente.

6.2.6 Información almacenada en el equipo informático

a. La información que se almacena en las unidades locales del equipo informático asignado, es responsabilidad del usuario, debiendo guardar dicha información en la unidad personal o carpetas compartidas asignadas.
b. La OTI solo es responsable de asegurar la disponibilidad de la información almacenada en las carpetas compartidas.
c. El usuario no debe almacenar información de carácter personal en las carpetas compartidas del área.
d. El usuario debe depurar de forma mensual, los espacios de las unidades locales de su equipo informático. Se recomienda realizar la depuración, considerando primero, la eliminación de los archivos más antiguos y de menor impacto.
e. Respecto a la información de los usuarios con licencia con/sin goce de haber, el jefe o responsable de la oficina debe tomar medidas para garantizar la disponibilidad de la información que deja temporalmente el usuario.
f. En caso de reinstalación del equipo informático debido a fallas o asignación de un equipo nuevo, es responsabilidad del usuario salvaguardar su información previamente.
g. El personal CAS que se retire de la UE002SST, debe presentar la “Declaración Jurada del usuario sobre la disposición del uso de la información almacenada en el equipo informático y en el correo electrónico institucional al término del vínculo laboral con la UE002SST”, como parte del proceso de entrega de cargo.
h. La carpeta compartida (Unidad P), es una carpeta solamente de uso temporal, la cual es depurada/eliminada toda información que esta contenga cada último día laborable del mes. Siendo responsabilidad de cada usuario salvaguardar su información en los equipos asignados.

6.2.7 Uso de impresoras y equipos multifuncionales

a. Los usuarios solo deben utilizar las impresoras o equipos multifuncionales para propósitos relacionados con sus funciones.
b. Cualquier problema de funcionamiento de los equipos de impresión y/o multifuncionales debe ser reportado a la OTI a través del correo institucional.
c. Los usuarios no deben manipular la configuración, o instalar tóner, cintas o cartuchos en cualquier equipo de impresión del UE002SST, pues es responsabilidad del personal de la OTI.
d. El usuario es responsable del uso adecuado de las impresoras y equipos multifuncionales.

6.2.8 Asignación de computadoras portátiles

a. La OTI en caso de disponer de computadoras portátiles, puede asignarlas en calidad de préstamo de acuerdo con el requerimiento solicitado por el usuario mediante notificación al correo institucional, para realizar reuniones, eventos, comisiones de servicios y/o presentaciones.
b. No se asignarán computadoras portátiles a los usuarios para su uso en sus domicilios, salvo autorización del Gerente de línea.
c. El usuario es responsable de mantener la computadora portátil y sus componentes en las mismas o similares condiciones durante el período de asignación, y de seguir las siguientes recomendaciones:
    - Custodiarla de forma adecuada, no dejarla desatendida en lugares públicos y transportarla de forma segura.
    - Notificar a la OTI los inconvenientes presentados con la computadora portátil, a través del correo institucional.
    - Asumir la responsabilidad por el deterioro, maltrato o extravío de la computadora portátil asignada.

6.2.9 Equipos de comunicación móvil

a. La OTI, recepciona y custodia los equipos de comunicación móvil que son entregados a la Entidad como parte de compra por el servicio contratado.
b. Todo usuario autorizado para utilizar un equipo de comunicación móvil debe de contar con el Acta de entrega y movimiento de bienes activo fijo debidamente firmado.
c. El usuario debe utilizar el equipo móvil de comunicación, asignado por la UE002SST, de manera exclusiva para el desempeño de sus funciones y/o servicios contratados.
d. El usuario debe mantener el equipo de comunicación móvil y sus componentes en las mismas o similares condiciones durante el período de asignación, sin más deterioro que el que se produzca por su uso ordinario.
e. La OTI mantiene un inventario actualizado de los equipos de comunicación móvil de la entidad cuenta.
f. En caso de pérdida, sustracción o siniestro de los equipos de comunicación móvil provistos por la UE002SST, el usuario debe informar a la OTI mediante el correo institucional en un plazo máximo de 24 horas con la denuncia policial de corresponder para proceder de acuerdo a lo siguiente:
    - **Pérdida:** El personal al que se le haya asignado el bien será responsable de su custodia. En caso de pérdida, deberá reponer un bien de iguales o similares características, o asumir el valor correspondiente, de acuerdo con la evaluación y disposiciones de la entidad.
    - **Sustracción:** En caso de robo o hurto del bien, el personal deberá comunicar el hecho y presentar la denuncia policial correspondiente. Cumplido este requisito y previa evaluación de las circunstancias del caso, podrá quedar exonerado de responsabilidad.
    - **Siniestro:** Cuando el bien resulte afectado o destruido por un siniestro debidamente acreditado, el personal quedará exonerado de

responsabilidad, salvo que se determine la existencia de negligencia o incumplimiento de sus deberes de custodia.

g. Al finalizar el vínculo laboral con la UE002SST o cuando la OTI o jefe/responsable de la oficina lo requiera, el usuario debe devolver el equipo en las mismas o similares condiciones en las que le fue asignado, sin más deterioro que el que se produzca por su uso ordinario, y debe gestionar la devolución a través del Acta de entrega y movimiento de bienes activo fijo debidamente firmado.

6.2.10 Seguridad de la información en los equipos y servicios informáticos de la UE002SST

a. El usuario no puede instalar o hacer uso de software no autorizado por la OTI y no puede utilizar herramientas que puedan comprometer la seguridad de la información de la Entidad.
b. El usuario no puede desactivar o desinstalar el software antivirus instalado en su equipo informático, solo el personal de la OTI está autorizado para administrar dicho software.
c. Para el uso de dispositivos de almacenamiento externo, el antivirus se activa de forma automática para escanear y desinfectar los archivos, por cual los usuarios deben esperar a que el antivirus finalice su verificación.
d. Los documentos físicos de uso interno no se deben dejar en las impresoras y equipos multifuncionales, a fin de evitar el acceso no autorizado a la información de la UE002SST.
e. Los documentos físicos o digitales que contengan información confidencial que no serán usados, deben ser destruidos o depurados.
f. El usuario es responsable de la información contenida en el equipo de comunicación móvil, por lo cual debe tomar las medidas de seguridad correspondientes.

g. Al finalizar la jornada laboral, el usuario debe guardar en un lugar seguro, los documentos físicos o digitales que contengan información confidencial.

7. GESTIÓN DE ACCESOS A LOS SISTEMAS DE INFORMACION

7.1 Clasificación de los sistemas institucionales

Los sistemas institucionales de la UE002SST se clasifican de la siguiente manera:

7.1.1 Sistemas Comerciales:

Comprende los sistemas y módulos relacionados con la gestión comercial y operativa de los servicios brindados por la entidad, tales como:

a. Reglas de negocio
b. Solicitudes y presupuestos
c. Catastro
d. Medición
e. Facturación
f. Cobranza
g. Cartera morosa
h. Reclamos
i. Reclamos ONLINE
j. Cierres y aperturas
k. Consulta y reportes
l. Indicadores de gestión comercial
m. Dispositivos móviles
n. SUNAT
o. Bancos

7.1.2 Sistemas Administrativos:

Comprende los sistemas y módulos relacionados con la gestión administrativa y operativa institucional, tales como:

a. SIAF
b. Logística

c. Finanzas
d. Nómina
e. Patrimonio
f. Contabilidad
g. Planificación

7.2 Principios para la gestión de accesos

La gestión de accesos a los sistemas institucionales deberá regirse por los siguientes principios:

7.2.1 Principio de mínimo privilegio

Los usuarios deberán contar únicamente con los accesos y permisos estrictamente necesarios para el cumplimiento de sus funciones.

7.2.2 Responsabilidad individual de cada usuario del uso de su cuenta de acceso y de las acciones realizadas con sus credenciales.

7.2.3 Segregación de funciones

Los accesos deberán asignarse evitando conflictos de funciones o concentraciones indebidas de privilegios.

7.2.4 Control de accesos

Todo acceso a los sistemas institucionales deberá encontrarse debidamente autorizado y registrado.

7.2.5 Confidencialidad de credenciales

Las credenciales de acceso son de uso personal e intransferible, quedando prohibido compartir usuarios o contraseñas entre servidores o terceros autorizados.

7.2.6 Trazabilidad

Toda asignación, modificación, bloqueo o eliminación de accesos deberá quedar registrada, permitiendo identificar al usuario, fecha, responsable y acción realizada.

7.3 Roles y responsabilidades

7.3.1 Del jefe inmediato o responsable del área usuaria

El jefe inmediato o responsable del área usuaria es responsable de solicitar formalmente la creación, modificación o baja de accesos para el personal a su cargo, de acuerdo con las funciones que este desempeñe dentro de la entidad. Asimismo, deberá verificar que los accesos solicitados sean estrictamente necesarios para el cumplimiento de las labores asignadas, evitando requerimientos de privilegios innecesarios o incompatibles con el puesto.

Las solicitudes deberán realizarse mediante correo electrónico institucional de la UE002SST o a través de los mecanismos formalmente establecidos por la entidad, consignando como mínimo la siguiente información:

a. Nombres y apellidos del usuario.
b. Cargo o función.
c. Área de pertenencia.
d. Sistema al que requiere acceso.
e. Módulos requeridos.
f. Perfil o nivel de acceso solicitado.
g. Motivo de la solicitud.

En el caso de modificaciones o ampliaciones de permisos, deberá sustentar la necesidad del cambio solicitado.

Para las bajas de usuario, el jefe inmediato deberá comunicar de manera inmediata el cese, rotación, suspensión, término de contrato o cualquier otra condición que implique la restricción o retiro del acceso a los sistemas institucionales.

7.3.2 Del área responsable de tecnologías de la información

El área responsable de tecnologías de la información es la encargada de administrar y controlar los accesos a los sistemas institucionales de la UE002SST.

Son responsabilidades del área de tecnologías de la información:

a. Verificar que toda solicitud cuente con la autorización correspondiente.
b. Validar que el perfil solicitado corresponda a las funciones del usuario.
c. Crear, modificar, bloquear o eliminar cuentas de acceso.
d. Asignar privilegios conforme a los perfiles aprobados.
e. Mantener registro de las altas, modificaciones y bajas realizadas.
f. Supervisar los accesos con privilegios administrativos.
g. Implementar controles de seguridad relacionados con autenticación y gestión de credenciales.
h. Realizar revisiones periódicas de usuarios y permisos asignados.

El área de tecnologías de la información podrá observar o rechazar solicitudes que representen riesgos de seguridad o incumplan la presente directiva.

Asimismo, podrá deshabilitar cuentas que permanezcan inactivas por periodos prolongados o que representen riesgos para la seguridad de la información institucional.

7.3.3 De los usuarios de los sistemas institucionales

Los usuarios autorizados son responsables del uso adecuado de las cuentas y accesos asignados.

Todo usuario deberá:

a. Utilizar únicamente la cuenta asignada a su nombre.
b. Mantener la confidencialidad de sus credenciales.
c. Evitar compartir usuarios o contraseñas.
d. Informar inmediatamente incidentes relacionados con accesos no autorizados.
e. Utilizar los sistemas únicamente para fines institucionales.
f. Cumplir las disposiciones establecidas en la presente directiva.

El usuario será responsable de toda acción realizada con su cuenta de acceso mientras esta se encuentre habilitada.

7.4 Gestión de altas, modificaciones y bajas de usuarios

7.4.1 Alta de usuarios

La creación de cuentas de usuario deberá realizarse únicamente a solicitud formal del jefe inmediato o responsable del área usuaria.

No se crearán accesos sin autorización previa. La solicitud deberá indicar expresamente:

a. Sistema al que accederá el usuario.
b. Módulos requeridos.
c. Perfil solicitado.
d. Funciones que realizará.

Recibida la solicitud, el área de tecnologías de la información verificará que el perfil solicitado sea coherente con las funciones asignadas al usuario.

Una vez validada la solicitud, se procederá a:

a. Crear la cuenta de usuario.
b. Asignar el perfil correspondiente.
c. Generar credenciales temporales.
d. Registrar la creación del acceso.

Las credenciales deberán ser entregadas únicamente al usuario autorizado, mediante mecanismos que garanticen la confidencialidad de la información de acceso.

Las credenciales iniciales deberán ser cambiadas por el usuario en el primer inicio de sesión.

En caso de usuarios temporales, terceros o personal de soporte externo, el acceso deberá contar con una fecha de vencimiento definida.

7.4.2 Modificación de accesos

La modificación de perfiles o permisos deberá ser solicitada formalmente por el jefe inmediato o responsable del área usuaria.

Las modificaciones podrán realizarse por motivos tales como:

a. Cambio de funciones.
b. Reasignación de responsabilidades.
c. Rotación de personal.
d. Necesidad operativa debidamente sustentada.
e. Ampliación o reducción de permisos.

Toda modificación deberá quedar registrada, indicando:

a. Usuario afectado.
b. Permisos anteriores.
c. Nuevos permisos asignados.
d. Fecha de modificación.
e. Responsable que autorizó el cambio.

La asignación de perfiles con privilegios administrativos o accesos de nivel elevado deberá contar con autorización expresa del jefe responsable del área usuaria y validación del área de tecnologías de la información.

7.4.3 Baja de usuarios

La baja de accesos deberá realizarse de manera inmediata cuando el usuario:

a. Cese sus funciones.
b. Concluya su vínculo contractual.
c. Cambie de funciones y ya no requiera acceso.
d. Sea suspendido.
e. Incumpla disposiciones de seguridad.
f. Cuando exista disposición expresa de la entidad.

El jefe inmediato o responsable del área usuaria deberá comunicar oportunamente la baja del usuario al área de tecnologías de la información.

Recibida la comunicación, el área de tecnologías de la información procederá a:

a. Bloquear o deshabilitar la cuenta.
b. Retirar privilegios asignados.
c. Revocar accesos administrativos.

d. Registrar la baja realizada.

En ningún caso deberán mantenerse cuentas activas de personal que ya no mantenga vínculo funcional o contractual con la entidad.

7.4.4 Gestión de usuarios con privilegios administrativos

Los usuarios con privilegios administrativos deberán ser restringidos únicamente al personal autorizado por la entidad y estrictamente necesario para la administración de los sistemas institucionales.

La asignación de privilegios administrativos deberá contar con autorización expresa del responsable correspondiente y encontrarse debidamente sustentada.

Las cuentas con privilegios administrativos deberán cumplir como mínimo con las siguientes medidas:

a. Uso individual e intransferible.
b. Contraseñas seguras.
c. Restricción de acceso según funciones.
d. Registro de actividades realizadas.
e. Revisión periódica de privilegios asignados.

Queda prohibido el uso de cuentas genéricas compartidas para actividades administrativas, salvo casos excepcionales debidamente justificados y autorizados.

7.5 Tipos de acceso y roles

7.5.1 Usuario de consulta

Acceso únicamente para visualización de información y generación de reportes, sin permisos para registrar, modificar o eliminar información.

7.5.2 Usuario operativo

Acceso destinado al personal encargado del registro y actualización de información relacionada con los procesos institucionales asignados.

UNIDAD EJECUTORA TUMBES
Firmado digitalmente por: PAREDES HASEN Nicida Gissela FAU 20603799373 soft
Motivo: Soy el autor del documento
Fecha: 16/07/2026 17:18:32-0500

7.5.3 Usuario supervisor

Acceso destinado al personal responsable de supervisar operaciones, validar información, aprobar procesos y acceder a reportes de control.

7.5.4 Administrador funcional

Acceso destinado al personal autorizado para administrar parámetros operativos o configuraciones específicas de determinados módulos institucionales.

No incluye privilegios técnicos sobre infraestructura, bases de datos o administración general del sistema.

UNIDAD EJECUTORA TUMBES
Firmado digitalmente por: NARRO TISNADO Heynar Adolfo FAU 20603799373 soft
Motivo: Soy el autor del documento
Fecha: 16/07/2026 15:50:14-0500

7.5.5 Administrador técnico

Acceso restringido al personal de tecnologías de la información encargado de:

UNIDAD EJECUTORA TUMBES
Firmado digitalmente por: ALEJOS LIÑAN Esau FAU 20603799373 soft
Motivo: Soy el autor del documento
Fecha: 15/07/2026 15:00:33-0500

a. Administración de usuarios.
b. Soporte técnico.
c. Configuración del sistema.
d. Mantenimiento.
e. Administración de bases de datos.
f. Control de seguridad.
g. Gestión de infraestructura tecnológica.

UNIDAD EJECUTORA TUMBES
Firmado digitalmente por: EFFIO ALBUJAR Karla Melissa FAU 20603799373 soft
Motivo: Soy el autor del documento
Fecha: 15/07/2026 16:52:57-0500

UNIDAD EJECUTORA TUMBES
Firmado digitalmente por: AREVALO LOPEZ Julio Cesar FAU 20603799373 soft
Motivo: En señal de conformidad
Fecha: 16/07/2026 09:22:04-0500

8. DISPOSICIONES FINALES

La Oficina de Tecnologías de la Información podrá emitir disposiciones complementarias necesarias para la adecuada aplicación de la presente directiva.

Los casos no previstos en el presente documento serán evaluados por el área competente de la UE002SST, considerando los principios de seguridad de la información y control institucional.

El incumplimiento de las disposiciones establecidas en la presente directiva podrá dar lugar a las acciones administrativas correspondientes, de acuerdo con la normativa vigente y disposiciones internas de la UE002SST.

UNIDAD EJECUTORA TUMBES
Firmado digitalmente por: ALVA CUEVA Jino Luis FAU 20603799373 soft
Motivo: Soy el autor del documento
Fecha: 15/07/2026 12:24:39-0500

UNIDAD EJECUTORA TUMBES
Firmado digitalmente por: CORNEJO ESCOBAR Abad [illegible] FAU 20603799373 soft
Motivo: Soy el autor del documento
Fecha: 15/07/2026 14:55:14-0500

UNIDAD EJECUTORA TUMBES
Firmado digitalmente por: VIDAL VEREAU Juan Manuel FAU 20603799373 soft
Motivo: En señal de conformidad
Fecha: 16/07/2026 11:28:31-0500