# DIRECTIVA PARA EL ACCESO Y USO DE LOS ACTIVOS INFORMÁTICOS DE LA SUPERINTENDENCIA NACIONAL DE EDUCACIÓN SUPERIOR UNIVERSITARIA – SUNEDU

| ROL | NOMBRE | CARGO | FIRMA |
|---|---|---|---|
| **Elaborado por:** | Isaac Ernesto Bringas Masgo | Jefe de la Oficina de Tecnologías de la Información | Documento firmado digitalmente<br>**ISAAC ERNESTO BRINGAS MASGO**<br>Jefe de la de la Oficina de Tecnologías de la Información<br>Superintendencia Nacional de Educación Superior Universitaria |
| **Revisado por:** | Zoraida Vargas Zapata | Jefa de la Oficina de Planeamiento y Presupuesto | Documento firmado digitalmente<br>**ZORAIDA VARGAS ZAPATA**<br>Jefa de la Oficina de Planeamiento y Presupuesto<br>Superintendencia Nacional de Educación Superior Universitaria |
| | Fressia Mercedes Munárriz Infante | Jefa de la Oficina de Asesoría Jurídica | Documento firmado digitalmente<br>**FRESSIA MERCEDES MUNÁRRIZ INFANTE**<br>Jefa de la Oficina de Asesoría Jurídica<br>Superintendencia Nacional de Educación Superior Universitaria |

**CONTROL DE CAMBIOS**

| N° | Ítems | Descripción del cambio |
|---|---|---|
| 1 | 3.2 | Se agregó Ley N° 29733, Ley de protección de Datos Personales |
| 2 | 3.3 | Se agregó Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital. |
| 3 | 3.7 | Se agregó Decreto de Urgencia N° 007-2020 se aprueba el Marco de Confianza Digital y dispone medidas para su Fortalecimiento |
| 4 | 3.4 | Decreto Supremo N° 029-2021-PCM que aprueba el Reglamento del Decreto Legislativo 1412 |
| 5 | 3.9 | Se incluyó la Resolución de Secretaría General N° 065-2019-SUNEDU, Directiva para la elaboración, aprobación y modificación de documentos de Gestión interna. |
| 6 | 2 | Modificación de Finalidad |
| 7 | 5.3 | Se agregó definición de Coordinadores de requerimientos |
| 8 | 5.4 | Se agregó definición de Directorio Activo |
| 9 | 5.5 | Cambio de definición de líder usuario |
| 10 | 5.6 | Modificación de la definición de plataforma de comunicación y conferencia |
| 11 | 5.7 | Incorporación de definición de OneDrive |
| 12 | 5.8 | Incorporación de definición de Office 365 |
| 13 | 5.10 | Modificación de definición de Usuario/a de Tecnologías de la Información (Usuario/a TI): |
| 14 | 5.12 | Incorporación de definición de Sistema de mesa de ayuda |
| 15 | 5.13 | Incorporación de definición de Servicio en la nube |
| 16 | 5.14 | Incorporación de definición de SharePoint |
| 17 | 5.15 | Incorporación de definición de Spam |
| 18 | 5.16 | Incorporación de definición de Software libre |
| 19 | 5.17 | Incorporación de definición de Software Autorizado |
| 20 | 5.18 | Incorporación de definición de Oficial de Seguridad Digital |
| 21 | 5.19 | Incorporación de definición de VPN (Virtual Private Network por sus siglas en inglés) |
| 22 | 6.2 | Adición de responsabilidades de la Oficina de Recursos Humanos |
| 23 | 6.3 | Adición de responsabilidades de la Unidad de Abastecimiento |
| 24 | 6.5 | Modificación de responsabilidades de el/la Oficial de Seguridad Digital |
| 25 | 6.6 | Adición de responsabilidades de los/las jefes/as o directores/as de los Órganos y Unidades Orgánicas |
| 26 | 7.3 | Se adicionó disposiciones generales con el acceso a un activo informático |
| 27 | 7.3 | Se adicionó disposiciones del/la Coordinador/a de Requerimientos |
| 28 | 7.8 | Se modificó sobre El Órgano o Unidad Orgánica que requiera adquirir un activo informático |
| 29 | 7.10 | Se modificó sobre El desplazamiento de los activos informáticos dentro o fuera de la institución |
| 30 | 8.1.1 | Modificación del gráfico de Información digital institucional |

| | | |
|---|---|---|
| 31 | 8.1.3 | Modificación y adición de párrafos en correo electrónico |
| 32 | 8.1.4 | Modificación y adición de párrafos en Servicio de Internet |
| 33 | 8.1.5 | Modificación de párrafos en Software |
| 34 | 8.1.6 | Modificación de párrafos en Sistemas de Información |
| 35 | 8.1.7 | Modificación de párrafos en Plataforma de comunicación y conferencias |
| 36 | 8.1.8 | Modificación de párrafos en Acceso telefónicos |
| 37 | 8.1.9 | Adición de ítem Acceso remoto por VPN. |
| 38 | 9.1 | Modificación de párrafos en De la creación, actualización y desactivación de cuentas para el acceso y uso de los activos informáticos |
| 39 | 9.2 | Modificación de párrafos en De la gestión y uso de las contraseñas |
| 40 | 9.3 | Modificación de párrafos en De la solicitud, instalación y configuración de hardware o equipamiento informático |
| 41 | 9.4 | Modificación de párrafos en De los incidentes en los activos informáticos |
| 42 | 9.5 | Modificación de párrafos en Del monitoreo de cumplimiento de la directiva |
| 43 | 10 | Modificación de párrafos en Disposiciones Complementarias |
| 44 | 11.1 | Modificación de Anexo N° 1: “Formato de creación, actualización o desactivación de cuentas de usuarios de red”. |

## 1. OBJETIVO

Establecer lineamientos para el acceso y uso adecuado de los activos informáticos de la Superintendencia Nacional de Educación Superior Universitaria - Sunedu.

## 2. FINALIDAD

Garantizar una adecuada gestión de los activos informáticos de la entidad.

## 3. BASE LEGAL

3.1 Ley N° 30220, Ley Universitaria.
3.2 Ley N° 29733, Ley de protección de Datos Personales y modificatorias.
3.3 Decreto Legislativo N° 1412, aprueba la Ley de Gobierno Digital.
3.4 Decreto Supremo 029-2021-PCM, que aprueba el Reglamento del Decreto Legislativo 1412 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.
3.5 Decreto Supremo N° 012-2014-MINEDU, que aprueba el Reglamento de Organización y Funciones de la Superintendencia Nacional de Educación Superior Universitaria -Sunedu y modificatorias.
3.6 Decreto Supremo N° 003-2013-JUS, que aprueba la Ley N° 29733, Ley de Protección de Datos Personales.
3.7 Decreto de Urgencia N° 007-2020, Marco de Confianza Digital y dispone medidas para su Fortalecimiento.
3.8 Resolución Ministerial N° 004-2016-PCM, que aprueba el uso obligatorio de la Norma Técnica Peruana "NTP - ISO/IEC 27001:2014 EDI Tecnología de la Información. Técnicas de Seguridad. Sistemas de gestión de seguridad de la Información. Requisitos" en todas las entidades integrantes del Sistema Nacional de Informática.
3.9 Resolución de Secretaría General N° 065-2019-SUNEDU, Directiva para la elaboración, aprobación y modificación de documentos de Gestión interna.
3.10 Resolución de Secretaría General N° 038-2017-SUNEDU, que aprueba la Directiva para el acceso y uso de los activos informáticos de la Superintendencia Nacional de Educación Superior Universitaria — Sunedu.
3.11 Resolución de Jefatura N° 090-95-1NEl, que aprueba la Directiva N° 008-95-1NEI/SJI denominada "Recomendaciones Técnicas para la protección Física de los Equipos y Medios de Procesamiento de la Información en la Administración Pública".

## 4 ALCANCE

La presente directiva es de aplicación obligatoria para los órganos y unidades orgánicas de la Sunedu.

## 5 DEFINICIONES

**5.1 Activo informático:** Activos de una organización que se encuentran relacionados directa o indirectamente con la actividad informática, según Resolución Jefatural N° 090- 95-INEI, entre ellos se encuentran:

- Hardware o equipamiento informático: computadora (monitor, Unidad Central de Procesamiento - CPU, teclado, mouse), laptops, tablets, impresoras, sistema de alimentación ininterrumpida - UPS, servidores, equipos de comunicación, teléfonos IP's, smartphones, switch, gabinetes, entre otros.
- La información digital almacenada en el hardware o equipamiento físico (no están incluidos los documentos fuentes que la generan).
- Medios de comunicación que se utilizan para la transmisión de datos mecanizados (redes de equipos informáticos, correo electrónico, internet, etc.).
- Medios magnéticos y ópticos de almacenamiento de la información (cinta, cartuchos, discos, etc.).
- Programas y aplicaciones de la Institución, ya sea desarrollados por ésta, adquiridos o alquilados a terceros, también conocido como software o sistemas de información.
- Manuales, procedimientos y reglamentaciones afines al área de informática (Plan de Contingencia, procedimientos de seguridad, etc.).

**5.2** **Controles de seguridad informática:** Mecanismos que se utilizan para poder controlar y monitorear los accesos y uso de los activos informáticos.

**5.3** **Coordinadores de requerimientos:** Personal de un Órgano o Unidad Orgánica que coordina ante la Oficina de Tecnologías de Información los requerimientos de su dirección u oficina para su atención.

**5.4** **Directorio Activo:** Software que administra una estructura jerárquica con información de los/las usuarios/as y sus permisos, carpetas, grupos de usuarios, computadoras e impresoras entre otros objetos existentes en una red informática.

**5.5** **Líder usuario:** Personal de un Órgano o Unidad Orgánica que define las necesidades que debe atender un sistema de información.

**5.6** **Plataforma de comunicación y conferencias:** Herramienta de comunicación instantánea exclusivo para las actividades relacionadas con la Sunedu.

**5.7** **OneDrive:** Herramienta online que permite crear, modificar y archivar documentos de Word, Excel y PowerPoint de manera colaborativa.

**5.8** **Office 365:** Versión en línea de Office y nos permite consultar y editar documentos en nuestro navegador web de las aplicaciones más comunes: Word, Excel, PowerPoint y OneNote.

**5.9** **Unidad de red:** Espacio de almacenamiento lógico de información designado para cada usuario/a TI.

**5.10** **Usuario/a de Tecnologías de la Información (Usuario/a TI):** Personal de un Órgano o Unidad Orgánica de Sunedu que utiliza y/o accede a un activo informático de la Sunedu.

**5.11** **Red de datos:** Infraestructura de tecnología que involucra componentes de hardware y software cuyo diseño posibilita la transmisión de información a través del intercambio de datos.

**5.12** **Sistema de mesa de ayuda:** Único punto de contacto para cualquier solicitud, problema o asistencia que los usuarios de Sunedu necesitan para acceder a los servicios tecnológicos e información.

**5.13** **Servicio en la nube:** Servicios que se utilizan a través de Internet. Es decir, no están físicamente instalados en un ordenador. Los servicios en la nube son programas que se alojan en un servidor accesibles desde cualquier dispositivo conectado a Internet, por ejemplo, se tiene el consultar el correo electrónico y colaborar en documentos, entre otros.

**5.14** **SharePoint:** Espacio seguro y colaborativo o portal de información empresarial donde los documentos y archivos son almacenados, organizados y compartidos, se puede acceder a la información desde cualquier dispositivo con un navegador web.

**5.15** **Spam:** Cantidades masivas de correos o envíos publicitarios, que se realizan en Internet. Los correos Spam son enviados a millones de cuentas de correo sin haber sido solicitados.

**5.16** **Software libre:** Software cuyo código fuente puede ser estudiado, modificado, y utilizado libremente con cualquier finalidad y redistribuido con cambios o mejoras sobre ellas.

**5.17** **Software Autorizado:** Aplicaciones o programas que están permitidas para ser instalado en cualquier equipo informático de la Sunedu.

**5.18** **Oficial de Seguridad Digital:** Personal designado por alta dirección, que coordina la implementación y mantenimiento del Sistema de Gestión de Seguridad de la Información en la institución; asimismo, propone las normas en materia de seguridad y confianza digital.

**5.19** **VPN (Virtual Private Network por sus siglas en inglés):** Red Privada Virtual es una tecnología de red que se utiliza para que el personal de la Sunedu se conecte desde sus casas u otro sitio a la Red Interna de la Sunedu de manera segura usando el internet.

## 6 RESPONSABILIDADES

**6.1** La Oficina de Tecnologías de la Información es responsable de:

a) Velar por la disponibilidad de los activos informáticos y utilizar herramientas o programas de bloqueo y/o filtro que aseguren tales recursos ante posibles riesgos informáticos.
b) Administrar el acceso a los activos informáticos de la institución y mantener el registro de los mismos.
c) Administrar el software legal y las licencias adquiridas.

d) Crear y entregar las cuentas de los/las usuarios/as TI para el uso de los activos informáticos.
e) Instalar, configurar y desinstalar los activos informáticos.
f) Realizar los talleres de capacitación correspondientes sobre el uso y acceso de los activos informáticos.
g) Efectuar revisiones periódicas con el objeto de desactivar cuentas de usuario/a repetidas y/o que no se encuentren en uso por más de sesenta (60) días hábiles.

**6.2** La Oficina de Recursos Humanos es responsable de remitir mensualmente a la Oficina de Tecnologías de la Información, mediante correo electrónico, la lista de personal por contrato CAS o por Ley del Servicio Civil, y practicantes que hayan iniciado o terminado sus contratos durante el mes. El Oficial de Seguridad Digital validará dicha lista y el personal de Mesa de Ayuda procederá a la actualización de las cuentas de usuarios.

**6.3** La Unidad de Abastecimiento es responsable de remitir mensualmente a la Oficina de Tecnologías de la Información, mediante correo electrónico, la lista de locadores/as de servicios que iniciaron su orden de servicio y los que hayan terminado durante el mes. El Oficial de Seguridad Digital validará dicha lista y el personal de Mesa de Ayuda procederá a la actualización de las cuentas de usuarios.

**6.4** Todo/a usuario/a TI que utiliza un activo informático es responsable de:

a) Velar por la integridad de los activos informáticos asignados.
b) Utilizar los activos informáticos solo con fines institucionales en cumplimiento de sus funciones.
c) Participar en los talleres de capacitación sobre el uso y acceso de los activos informáticos.

**6.5** El/la Oficial de Seguridad Digital es responsable de:

a) Realizar el seguimiento al cumplimiento de la presente directiva, y realizar dos (2) evaluaciones al año sobre su cumplimiento.
b) Elaborar dos (2) informes técnicos de cumplimiento de la directiva.

**6.6** Los/las jefes/as o directores/as de los Órganos y Unidades Orgánicas son responsables de:

a) Remitir a la Oficina de tecnologías de la información la solicitud mediante “Formato de creación, actualización o desactivación de cuentas de usuarios” establecido en el Anexo N° 1 de la presente directiva, de una cuenta de usuario/a TI.
b) Autorizar el acceso y uso de los activos informáticos de su personal.
c) Brindar las facilidades para que su personal asista a los talleres presenciales o virtuales de capacitación sobre el uso y acceso de los activos informáticos.
d) Remitir a la Oficina de tecnologías de la información la solicitud de desactivación de usuario/a TI mediante el “Formato de creación, actualización o desactivación de cuentas de usuarios” establecido en el Anexo N° 1 de la presente directiva, cuando su personal deja de laboral o cuando se termina el servicio de un proveedor o tercero.

## 7 DISPOSICIONES GENERALES

7.1 Todo acceso a cualquier activo informático será brindado solo bajo autorización de el/la Jefe/a o Director/a del Órgano o Unidad Orgánica.

7.2 El/la Jefe o Director/a designará a los coordinadores/as de requerimientos de su oficina o dirección mediante memorando a solitud de la Oficina de Tecnologías de información.

7.3 El/la coordinador/a de requerimientos gestionará ante la Oficina de Tecnologías de la Información los licenciamientos de Software, adquisiciones software y hardware, creación de requerimientos mediante el sistema de mesa de ayuda (Creación de usuario/a de red, correo, accesos a sistemas de información, creación de claves telefónicas, baja de accesos, permisos de carpetas compartidas, Instalación de software, SIGA y SIAF, asignación de PC y anexo telefónico, Mantenimiento de Aplicaciones y Procesamiento de Datos, entre otros) y administración del sitio SharePoint del órgano y unidad orgánica al que pertenece.

7.4 Todo acceso a los sistemas de información, correo electrónico, internet, intranet, unidades de red, impresoras y otros servicios de red, debe ser realizado a través de una cuenta de usuario/a y su respectiva contraseña generada por la Oficina de Tecnologías de la Información.

7.5 El/la usuario/a TI que crea, genera y modifica información digital relevante para la institución debe almacenarla en la unidad de red que tiene asignado como usuario/a TI.

7.6 El uso de los activos informáticos de la Sunedu queda restringido a los fines institucionales en cumplimiento de las funciones de cada usuario/a TI.

7.7 Los/las usuarios/as de los activos informáticos de la institución evitarán poner en riesgo de pérdida, robo o deterioro a los equipos, las redes, la información, los programas y los sistemas de la institución.

7.8 El Órgano o Unidad Orgánica que requiera adquirir un activo informático debe remitir los requerimientos funcionales a la Oficina de Tecnologías de la información, la cual elaborará los términos de referencia o especificaciones técnicas.

7.9 Toda solicitud de atención por avería o desperfecto de los activos informáticos, así como la habilitación de los mismos, será atendida por la Oficina de Tecnologías de la Información según el orden de llegada.

7.10 El desplazamiento de los activos informáticos dentro o fuera de la institución será autorizado por la Unidad de Abastecimiento, de acuerdo a lo regulado en la directiva de ingreso, asignación y uso de los bienes muebles de propiedad de la Sunedu.

7.11 La instalación, configuración y desinstalación de los activos informáticos será realizada por personal de soporte la Oficina de Tecnologías de la Información.

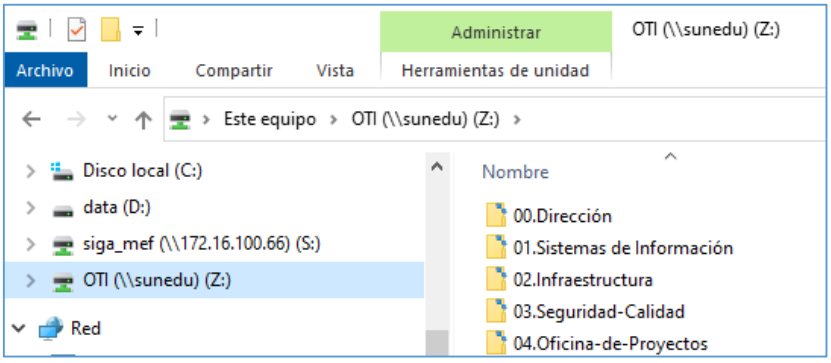
7.12 Todo/a usuario/a TI debe participar en los talleres de inducción sobre el uso de los activos informáticos.

# 8 DISPOSICIONES ESPECÍFICAS

## 8.1 Del uso de los activos informáticos

### 8.1.1 Información digital institucional

8.1.1.1 La información digital que se crea en las computadoras o equipos conectados a la red debe almacenarse en la unidad de red asignada (Z:) donde debe almacenar información que considere relevante para la institución.




8.1.1.2 La Oficina de Tecnologías de la Información debe realizar el respaldo de la información almacenada en las unidades de red, en forma diaria.

8.1.1.3 La Oficina de Tecnologías de la Información a través de un software autorizado licenciado o libre, administrará el uso de los dispositivos informáticos móviles conectados a las computadoras.

8.1.1.4 Si por fines laborales se utilizan dispositivos informáticos móviles como tablets, dispositivos de almacenamiento en USB, CDs, DVDs, entre otros, el usuario/a TI evitará almacenar en estos, en forma permanente la información institucional relevante.

### 8.1.2 Hardware o equipamiento informático

8.1.2.1 Las computadoras y equipos periféricos designados son de uso exclusivo para el desarrollo de las funciones y responsabilidades establecidas por y para la institución.

8.1.2.2 Todo requerimiento de instalación de hardware o equipamiento informático es solicitado por el/la Jefe/a o Director/a del Órgano o Unidad Orgánica correspondiente a la Oficina de tecnologías de la Información de acuerdo al numeral 9.3 de la presente directiva.

8.1.2.3 Ningún Órgano o Unidad Orgánica mantendrá guardados hardware o equipamiento informático en desuso.

**8.1.3 <u>Correo electrónico:</u>**

8.1.3.1 El correo electrónico institucional sirve como una herramienta de comunicación e intercambio de información oficial entre usuarios/as TI, de uso exclusivo para las actividades que estén relacionadas con la institución.

8.1.3.2 Todo/a usuario/a TI poseedor de una cuenta de correo electrónico institucional debe revisarla de manera diaria, por lo menos dos (2) veces al día (al inicio y al término de la jornada laboral).

8.1.3.3 De detectarse que el correo no es utilizado por más de sesenta (60) días hábiles y de verificar que no existe comunicación previa sobre dicha acción por parte del Órgano o Unidad Orgánica correspondiente, la Oficina de Tecnologías de la Información debe desactivar la cuenta de correo y comunicar de ello al respectivo Órgano para su conocimiento.

8.1.3.4 Si por necesidades laborales del Órgano o Unidad Orgánica se requiere crear cuentas genéricas de correo electrónico (por ejemplo: logistica@sunedu.gob.pe) esta deberá ser solicitada formalmente mediante "Formato de creación, actualización o desactivación de cuentas de usuarios" establecido en el Anexo N° 1 de la presente directiva, por el/la Jefe/a o Director/a del Órgano o Unidad Orgánica, quien asumirá o asignará a un personal CAS la responsabilidad del uso de la cuenta.

8.1.3.5 El usuario/a TI poseedor de una cuenta de correo electrónico institucional debe ordenar su bandeja de correo y registrar sus reuniones de trabajo.

8.1.3.6 El usuario/a TI poseedor de una cuenta de correo electrónico institucional, evitará abrir correos electrónicos sospechosos y/o con archivos adjuntos no solicitados, teniendo mayor precaución de los correos electrónicos provenientes en idiomas extranjeros.

8.1.3.7 Los mensajes de correo electrónico institucionales enviados interna o externamente no deben exceder de los 50 Megabytes, incluyendo el (los) archivo (s) adjunto (s) que lo acompañen, pero en caso se requiera más tamaño se debe solicitar justificando la necesidad.

8.1.3.8 Asimismo, la cuenta de correo le permite al usuario/a acceder a los demás servicios en la nube como es almacenamiento OneDrive, Office 365, SharePoint.

8.1.3.9 La Oficina de Tecnologías de la Información deberá contar con un sistema automático que permite filtrar los correos SPAM en salvaguarda de la seguridad de la información institucional.

8.1.3.10 Por ningún motivo se debe otorgar el acceso al correo electrónico de un usuario/a a otras personas, salvo por solicitud del mismo propietario o responsable asignado del correo o por notificación legal a solicitud de un juzgado.

**8.1.4 Servicio de internet:**

8.1.4.1 El uso del servicio de Internet es exclusivamente como herramienta de investigación y apoyo para la realización de sus labores diarias de los/las usuarios/as TI.

8.1.4.2 El uso del servicio de internet y de todas las operaciones que se realicen en ella, es de entera responsabilidad del usuario/a TI que lo usa.

8.1.4.3 La Oficina de Tecnologías de la Información deberá contar con herramientas de filtrado garantizando el uso racional del servicio de internet; asimismo, deberá contar con sistemas que permitan el bloqueo de acceso a las páginas webs que puedan ser una amenaza a la red de datos y páginas webs que no sean para la investigación y labores de los/las usuarios/as TI (por ejemplo, sitios de juegos, de descarga o escucha de música y videos, de comercio de artículos personales).

8.1.4.4 Todo/a usuario/a TI es responsable exclusivo por cualquier información obtenida de internet.

8.1.4.5 El/la Jefe/a o Director/a del Órgano o Unidad Orgánica podrá solicitar mediante correo o memorando restricciones adicionales a las páginas web o el levantamiento de las mismas al personal bajo su responsabilidad.

**8.1.5 Software**

8.1.5.1 Todo usuario/a TI cuenta con el siguiente software autorizado instalado en sus respectivas computadoras:

- Un sistema operativo
- Hoja de calculo
- Procesador de texto
- Presentación de diapositivas
- Compresor de archivos
- Lector de PDF
- Navegador Web
- Correo electrónico
- Antivirus

8.1.5.2 Si un/a usuario/a TI que requiera algún software autorizado adicional o software libre a los mencionados en la lista anterior, será gestionado por el coordinador de requerimiento asignado de su oficina o dirección, solicitándolo través de un memorándum o la plataforma de mesa de ayuda a la Oficina de Tecnologías de la Información, quien verificara si la institución cuenta con dicho software y las licencias respectivas o sea el caso se evalúe un software libre procediendo a instalarlos. En caso tampoco se cuente con un software libre, la Oficina de Tecnologías de la Información comunica al Órgano o Unidad Orgánica y remite los TDR o EETT para que continúe con la gestión ante la Unidad de Abastecimiento para la adquisición en el proceso de compra correspondiente.

8.1.5.3 La Oficina de Tecnologías de la Información es la única autorizada para instalar software en las computadoras de los/las usuarios/as TI; asimismo, es responsable de administrar el software y las licencias adquiridas. En caso se requiera privilegios de la instalación de software especializado por parte de otras oficinas o direcciones, estas le solicitaran a la Oficina de Tecnologías de la Información, los respectivos permisos justificando la necesidad y el tiempo de configuración y administración de dicho software.

8.1.5.4 Todos los/las usuarios/as TI deben informar de la existencia de algún software que no se encuentre autorizado por la Oficina de Tecnologías de la Información, contribuyendo así al cumplimiento de las normas que protegen los derechos de autor sobre softwares y aplicaciones.

8.1.5.5 La Oficina de Tecnologías de la Información debe verificar que todas las computadoras cuenten con software legal instalado, de detectar algún software instalado en las computadoras de la institución que no sea legal, se encontrará facultada de eliminar dicho software sin mediar aviso previo, ni tener responsabilidad de pérdida de información contenida en el software de ningún tipo.

### 8.1.6 Sistemas de Información

8.1.6.1 Todo sistema de información desarrollado o administrado por la Oficina de Tecnologías de la Información cuenta con un líder usuario/a del sistema quien realiza las solicitudes de posibles cambios o mejoras de los sistemas.

8.1.6.2 Todo/a usuario/a TI que requiera acceso a algún software o sistema de información debe contar con la autorización de el/la Jefe/a o Director/a del Órgano o Unidad Orgánica que lidera dicho sistema de información, la cual debe ser validado por la Oficina de Tecnologías de la Información.

8.1.6.3 El/la usuario/a TI debe ingresar o modificar información con datos válidos y verdaderos en los sistemas de información, garantizando que esta sea precisa.

### 8.1.7 Plataforma de comunicación y conferencias

8.1.7.1 Esta herramienta de comunicación y colaboración es para las reuniones de trabajo virtual entre los/las usuarios/as TI. El uso de esta herramienta y de todas las operaciones que se realicen con ella es de entera responsabilidad del usuario/a TI.

8.1.7.2 La Oficina de Tecnologías de la Información habilitará la herramienta de comunicación, configurará y la monitoreará para que permitan dar un buen servicio en la plataforma de comunicaciones y reuniones de trabajo virtual.

### 8.1.8 Accesos telefónicos

8.1.8.1 Todo/a usuario/a TI que requiera el acceso a llamadas telefónicas a nivel local, nacional e Internacional, podrá solicitar su uso mediante el "Formato de creación, actualización o desactivación de cuentas de usuarios de red" (ver Anexo N° 1), el cual debe ser firmado por el/la Jefe/a o Director/a del Órgano o Unidad Orgánica al que pertenece. La Oficina de Tecnologías de la Información debe brindar una contraseña de acceso.

### 8.1.9 Acceso remoto por VPN.

8.1.9.1 Todo/a usuario/a TI que requiera el acceso remoto por VPN a la red interna de la Sunedu, podrá solicitar su acceso mediante el "Formato de creación, actualización o desactivación de cuentas de usuarios de red" (ver Anexo N° 1) , el cual debe ser firmado por el/la Jefe/a o Director/a del Órgano o Unidad Orgánica al que pertenece. La Oficina de Tecnologías de la Información debe brindar a el/la usuario/a y contraseña correspondiente mediante correo electrónico a el/la usuario/a responsable de la cuenta.

8.1.9.2 Todo/a usuario/a TI debe considerar las buenas prácticas de seguridad de la información y recomendaciones en la conexión remota por VPN a la red interna de la Sunedu dadas por la Oficina de Tecnologías de la Información, para salvaguardar la información y los activos informáticos que usa en sus labores diarias.

## 8.2 Del uso incorrecto de los activos informáticos

Las siguientes acciones son consideradas como mal uso de los activos informáticos:

a) Dejar prendida las estaciones de trabajo sin bloqueo operativo durante la ausencia del usuario/a TI.
b) Almacenar música, videos, audio, ejecutables y otra información que no sean de carácter institucional en las unidades de red asignados a cada usuario/a TI u Órgano o Unidad Orgánica según corresponda
c) Ingerir y dejar alimentos y/o bebidas cerca y/o encima de los activos informáticos.
d) Mover o transferir los equipos informáticos y/o periféricos de un lugar a otro, sin autorización correspondiente.
e) Enviar correos masivos sin previa autorización por parte de la Oficina de Tecnologías de la Información.
f) Cambiar la configuración base de los activos informáticos definidos por la Oficina de Tecnologías de la Información.
g) Conectar ventiladores, lustradoras, cafeteras, hervidores u otros equipos eléctricos en los mismos enchufes o líneas de los activos informáticos.
h) Acceder a la red y/o al servicio de internet con activos informáticos que no pertenecen a la institución sin autorización (computadoras personales, modem USB, tabletas, entre otros).
i) Instalar o utilizar herramientas en la red para evadir los controles de seguridad implementados.

j) Utilizar el correo electrónico o internet para cualquier propósito comercial, financiero o ajeno a la institución o del Sector.
k) Distribuir mensajes, signos, figuras, dibujos, fotografías, videos y demás; con contenidos impropios y/o lesivos a la moral o relacionados a la delincuencia o terrorismo.
l) Facilitar, compartir u ofrecer la cuenta y contraseña de usuario/a TI de red, correo o sistemas de información a otras personas.
m) Utilizar la cuenta del correo electrónico institucional para registrarse en empresas u organizaciones con fines personales (medios de publicación, comercio, etc.)
n) Acceder a páginas webs que vayan en perjuicio o pongan en riesgo la seguridad de las redes y sistemas de la institución.
o) Realizar escaneos no autorizados, que saturen y perjudique la disponibilidad de las redes y sistemas de la institución de la Institución.
p) Realizar descargas de software que perjudiquen los activos informáticos.
q) Desinstalar el software base de los equipos informáticos.

## 9 PROCEDIMIENTOS

### 9.1 De la creación, actualización y desactivación de cuentas para el acceso y uso de los activos informáticos

9.1.1 Todo Órgano y Unidad Orgánica que requiera que su personal tenga acceso a algún activo informático debe solicitar la creación de cuentas de usuarios para su personal. Para tal efecto debe llenar, imprimir y firmar (en caso de no contar con firma digital), caso contrario puede ser firmado digitalmente el "Formato de creación, actualización o desactivación de cuentas de usuarios de red", (ver Anexo N° 1) y remitirlo a través del Sistema de Mesa de Ayuda de la Oficina de Tecnologías de la Información para su atención. La Oficina de Tecnologías de la Información en un plazo máximo de tres (3) días hábiles contados desde la recepción de la solicitud, debe crear las cuentas de usuario/a TI correspondientes, respetando la siguiente estructura:

| Uno de sus nombres + apellido paterno |
|---|

9.1.2 Los nombres y apellidos serán siempre en letra minúscula, sin acentos, ni caracteres especiales, ni espacios en blanco, ejemplo:

- Nombre del usuario : Pedro Jesús Pérez Carranza
- Cuenta de usuario : pedroperez o jesusperez

9.1.3 En caso de duplicidad o inconvenientes para la generación de la cuenta de red y correo institucional con el primer nombre y el primer apellido se agregará la inicial del segundo apellido, ejemplo:

- Nombre del usuario : Pedro Pérez Carranza
- Cuenta de usuario : pedroperezc o jesusperezc

Luego de la creación de las cuentas, La Oficina de Tecnologías de la Información a través del personal de Mesa de Ayuda debe realizar la entrega de las cuentas y sus respectivas contraseñas a cada usuario/a TI mediante el Sistema de Mesa de Ayuda o correo institucional. El/la usuario/a TI tiene derecho definir una contraseña distinta a la generada por la Oficina de Tecnologías de la Información, para ello debe considerar las indicaciones establecidas en el numeral 9.2 de la presente directiva.

9.1.4 El acceso a cualquier activo informático se realizará a través de la cuenta de usuario/a asignado/a y su respectiva contraseña.

9.1.5 En el caso de terceros (locadores de servicios) tendrán acceso contemplando las limitaciones y permisos que los Órganos y Unidades Orgánicas contratantes les permitan, en razón a la naturaleza de las funciones para las cuales han sido contratados.

9.1.6 Todo Órgano y Unidad Orgánica solicitará la actualización o desactivación de las cuentas de usuarios de su personal mediante el "Formato de creación, actualización o desactivación de cuentas de usuarios de red", (ver Anexo N° 1) y lo remitirá a través del Sistema de Mesa de Ayuda de la Oficina de Tecnologías de la Información para su atención. La Oficina de Tecnologías de la Información atenderá la solicitud en un plazo máximo de dos (2) días hábiles contados desde su recepción.

9.1.7 La Oficina de Tecnologías de Información actualizará los/las usuarios/as TI vigentes de manera mensual en el directorio activo, verificando con la información del personal por contrato CAS y practicantes remitida por la Oficina de Recursos Humanos, y con la Información de las órdenes de servicio de los Locadores de Servicios remitida por la Unidad de Abastecimiento.

### 9.2 De la gestión y uso de las contraseñas

9.2.1 El/la usuario/a TI al momento de definir una nueva contraseña debe considerar lo siguiente:

- Contendrá mínimo ocho (8) caracteres.
- La contraseña debe contener mínimo tres de los siguientes caracteres: mayúsculas, minúsculas, números o caracteres alfanuméricos.
- La contraseña no debe contener la totalidad o parte del nombre de la cuenta de usuario.
- No debe utilizar algún dato relacionado a su entorno personal y tampoco institucional, por ejemplo: nombre de los hijos, mascotas, números de teléfonos, fecha de nacimiento, Sunedu, licenciamiento, supervisión, etc.
- Cuando cambia o modifica la contraseña, no debe reutilizar las últimas tres (3) contraseñas usadas.

9.2.2 Los/las usuarios/as TI mantendrán las contraseñas en secreto, la confidencialidad de las mismas estará bajo su responsabilidad, considerando que estas son intransferibles.

9.2.3 La Oficina de tecnologías de la Información debe configurar los activos informáticos para que se permita como mínimo ocho (8) caracteres. Asimismo, configuraciones como:

- Programar que no se permita contraseñas simples, es decir solo números o letras; las contraseñas deben cumplir lo señalado en el punto 9.2.1.
- Programar para que automáticamente cada tres (3) meses se solicite cambio de la contraseña.
- Permitir solo seis (6) intentos de acceso con una contraseña incorrecta, en el séptimo intento se debe bloquear el acceso al activo.
- No permitir que, por lo menos, las últimas tres (3) contraseñas sean reutilizadas.

### 9.3 De la solicitud, instalación y configuración de hardware o equipamiento informático

9.3.1 Los Órganos o Unidades Orgánicas que requieran de hardware o equipamiento informático adicional, deben solicitarlo a la Oficina de Tecnologías de la Información mediante memorando o por el Sistema de Mesa de Ayuda, indicando la justificación de la necesidad.

9.3.2 La Oficina de Tecnologías de la Información, si se cuenta con los equipos informático, en un plazo máximo de tres (3) días hábiles contados desde la recepción de la solicitud, a través de su personal de soporte procederá a la instalación y la configuración de los equipos informáticos en la oficina o lugar de trabajo remoto; caso contrario, elabora los Términos de Referencia (TdR) o Especificaciones Técnicas (EETT).

9.3.3 En caso no se cuente con los equipos informáticos en stock, se le informa mediante memorando o por el Sistema de Mesa de Ayuda, adjuntando los TdR o EETT, al Órgano o Unidad Orgánica solicitante, de la no disponibilidad de dichos equipos y esta pueda continuar con el trámite correspondiente ante la Unidad de Abastecimiento a fin de que se realicen las adquisiciones respectivas.

### 9.4 De los incidentes en los activos informáticos

9.4.1 Todo/a usuario/a TI debe solicitar apoyo técnico a la Oficina de Tecnologías de la Información, ante cualquier inconveniente que se le presente en los activos informáticos, mediante el Sistema de Mesa de Ayuda.

9.4.2 Para ello debe ingresar a https://mesadeayuda.sunedu.gob.pe/ y digitar su nombre de usuario/a y su contraseña que ha sido entregado al momento de la creación de su cuenta de red.

9.4.3 Al ingresar su solicitud en el Sistema de Mesa de Ayuda, este será derivado al personal de la Oficina de Tecnologías de la Información para su atención.

9.4.4 Toda solicitud de atención en cuanto a los activos informáticos, así como la habilitación de los mismos, será atendida según su orden de llegada o urgencia de atención, según el procedimiento de Gestión de Incidentes y Problemas de TI de la Oficina de Tecnologías de la Información.

9.4.5 Luego de atender la solicitud, el personal de la Oficina de Tecnologías de la Información comunica al usuario/a TI mediante el Sistema de Mesa de Ayuda, la culminación de la

atención; el usuario/a solicitante remite su conformidad a través del mismo medio; y el personal de la Oficina de Tecnologías de la Información procede a cerrar el ticket dando por atendido la solicitud.

9.4.6 Para consultas técnicas, el/la usuario/a TI puede comunicarse al anexo 2003, WhatsApp de mesa de ayuda: 933671949/933671974/933671990, la Plataforma de comunicación Teams Microsoft o al correo: mesadeayuda@sunedu.gob.pe de la Oficina de Tecnologías de la Información.

### 9.5 Del monitoreo de cumplimiento de la directiva

9.5.1 La Oficina de Tecnologías de la Información, a través del Oficial de Seguridad Digital debe realizar revisiones inopinadas para evaluar el cumplimiento de la presente directiva.

9.5.2 El Oficial de Seguridad Digital debe elaborar los informes técnicos y remitirlos a el/la Jefe/a de la Oficina de Tecnologías de la Información dos (2) veces al año, haciendo las recomendaciones de mejora, según el resultado de las revisiones, para que estas sean implementadas por Oficina de Tecnologías de la Información, en busca de cumplir con el objetivo de la presente directiva.

## 10 DISPOSICIONES COMPLEMENTARIAS

10.1 La Oficina de Tecnologías de la Información pondrá en conocimiento de el/la Jefe/a o Director/a del Órgano o Unidad Orgánica todo mal uso de los activos informáticos que realicen sus usuarios TI, a fin de que se adopten las medidas que correspondan, según la normativa vigente sobre la materia.

10.2 La Oficina de Tecnologías de la Información debe implementar controles de seguridad informática a las estaciones de trabajo, laptops y tabletas como las siguientes:

- Solución de seguridad corporativa (antivirus).
- Mantener actualizado la solución de seguridad corporativa y el sistema operativo.
- Bloqueo de acceso a la configuración del sistema base.
- Bloqueo de instalación de software.
- Activación del bloqueo automático de 20 minutos de inactividad de las estaciones de trabajo o laptops, evitando accesos no autorizados.
- Agente de inventario de hardware y software de los activos informáticos.
- Un software legal que administrará el uso de los dispositivos de almacenamiento móviles como USB, DVDs, Tablets, entre otros, minimizando la fuga de la información institucional. Este software permitirá indicar las acciones realizadas con dichos dispositivos, mostrando solo la cantidad y tipo de información copiada en los mismos.
- A nivel de correo electrónico, la Oficina de Tecnologías de la Información, implementará una herramienta o filtro de correos electrónicos, evitando los correos no deseados (SPAM).

## 11 ANEXOS

11.1 Anexo N° 1: “Formato de creación, actualización o desactivación de cuentas de usuarios de red”.

11.2 Anexo N° 2: Diagrama de procesos

**ANEXO N.° 1**

**FORMATO DE CREACIÓN, ACTUALIZACIÓN O DESACTIVACIÓN DE CUENTAS DE USUARIOS DE RED**

| DÍA | MES | AÑO |
|---|---|---|
| | | |

| | |
|---|---|
| I. SOLICITANTE | |
| Dirección ( ) Oficina ( ) Unidad ( ) | |
| II. RELACIÓN DE USUARIO (S) | |

| N° | El Personal CAS/ Practicante es el responsable de la cuenta asignada. Para el caso de cuenta del locador el responsable del dueño del proceso o servicio (Directores/as y jefes/as). | | DNI | Cargo o Servicio | CAS o Locador | Crear (C) Actualizar (A) Desactivar (E) | ACCESO A | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | RED | INTERNET | CORREO ELECTRÓNICO | Servicio de telefonía | | | | Sistemas de Información (colocar número) | | | Otros |
| | APELLIDOS (Deberá de consignar los 02 Apellidos) | NOMBRES | | | | | | | | Fijos | Celulares | Nacionales | Internacionales | Operador | Administrador | Consulta | |
| 1 | | | | | | | | | | | | | | | | | |
| 2 | | | | | | | | | | | | | | | | | |
| 3 | | | | | | | | | | | | | | | | | |
| Observaciones: Se puede especificar la carpeta compartida u otras observaciones. | | | | | | | | | | | | | | | | | |

III. FIRMA Y SELLOS

A través de la siguiente firma autorizo la creación, actualización o desactivación del usuario a los servicios de red especificados.

| |
|---|
| |
| Firma |
| Jefe de la Unidad / Oficina / Dirección |

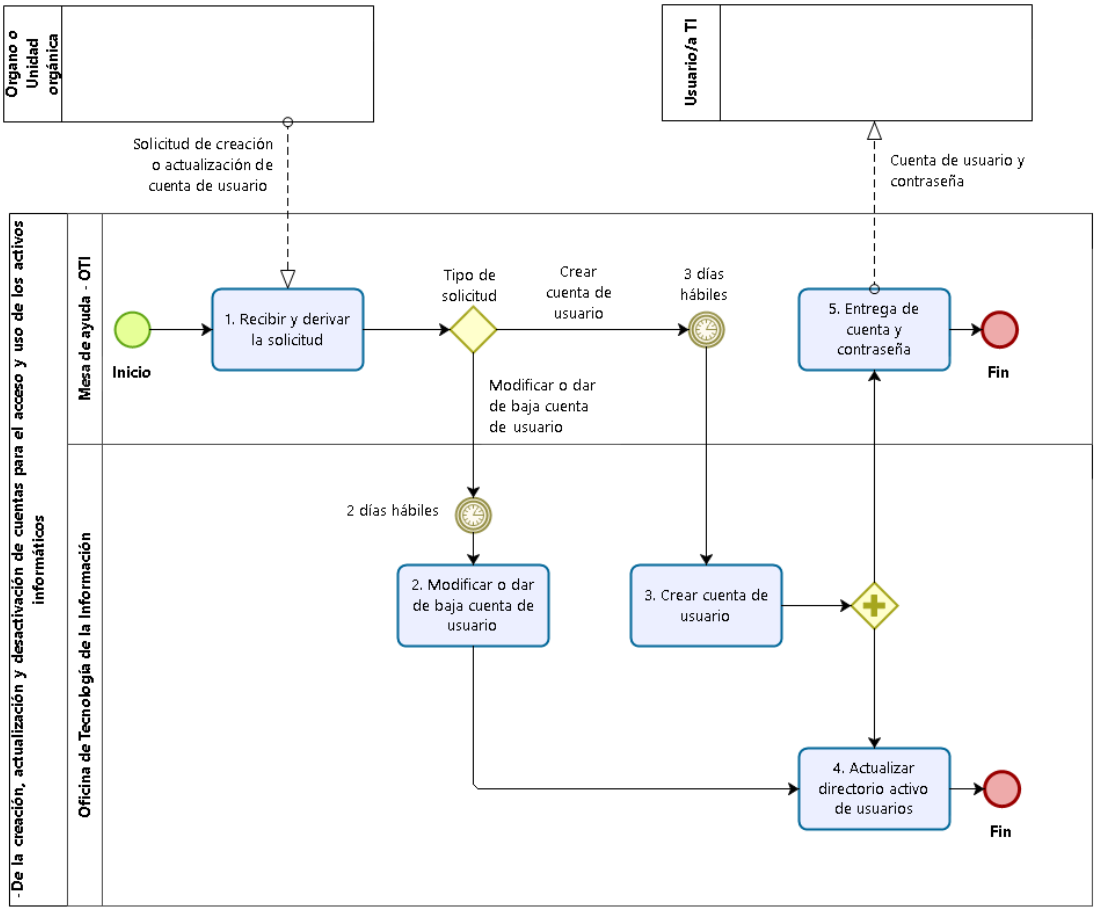
Lista de Sistemas de Información

| | |
|---|---|
| 1 | REGISTRO NACIONAL DE TRABAJOS DE INVESTIGACIÓN - **(RENATI)** |
| 2 | FORMULARIO VIRTUAL DE SOLICITUD DE ACCESO A LA INFORMACIÓN PÚBLICA - **(V-INFO)** |
| 3 | SISTEMA DEL PROCESO DE LICENCIAMIENTO INSTITUCIONAL - **(SIPLIC)** |
| 5 | SISTEMA DE INTEGRACIÓN DE ACCESOS - **(SIA)** |
| 6 | INTRANET INSTITUCIONAL - **(INTRANET)** |
| 7 | SISTEMA DE REGISTRO DE GRADOS Y TÍTULOS - **(SRGT)** |
| 8 | INTEGRACIÓN DE SERVICIO WEB - **(WSBN)** |
| 9 | PORTAL INSTITUCIONAL DE SERVICIOS EN LINEA - **(ENLINEA)** |
| 11 | SISTEMA DE REGISTRO DE DENUNCIAS - **(SUDENUNCIA)** |
| 12 | SISTEMA DE INFORME BIENAL - **(SIBE)** |
| 13 | SISTEMA DE GRADOS Y TÍTULOS - **(GRADOS)** |
| 14 | SISTEMA DE ADMINISTRACIÓN DOCUMENTARIA - **(SISAD)** |
| 16 | PORTAL INSTITUCIONAL - **(PORTAL)** |
| 17 | SISTEMA DE REGISTRO DE INFRACTORES Y SANCIONES - **(REGINSA)** |
| 18 | SISTEMA DE INFORMACIÓN UNIVERSITARIA ADMINISTRACIÓN - **(SIU)** |
| 19 | SISTEMA LICENCIAMIENTO DE PROGRAMAS DE PREGRADO DE MEDICINA - **(LICPRO)** |
| 20 | SISTEMA INTEGRACIÓN CON PIDE - **(WSPIDE)** |
| 22 | SISTEMA DE CONSULTAS DE SERVICIOS PIDE - **(CONSULTASPIDE)** |
| 23 | SISTEMA DE CESE DE UNIVERSIDADES - **(CESEU)** |

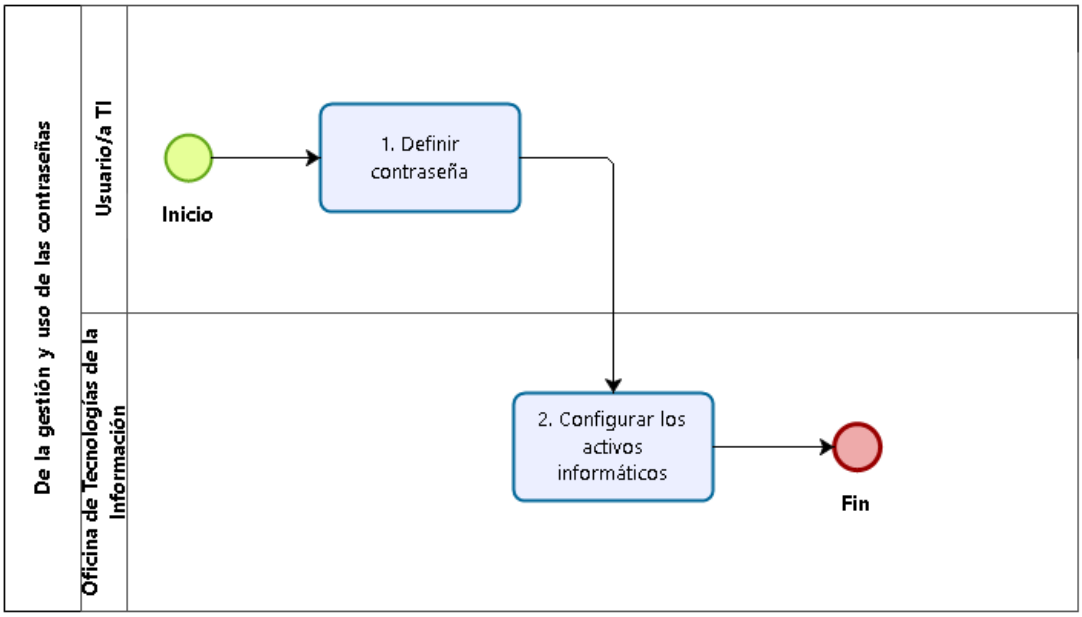
| | |
|---|---|
| 24 | SISTEMA DE SEGURIDAD - **(PUNKU)** |
| 25 | PORTAL DE INFORMACIÓN UNIVERSITARIA (TUNI.PE) - **(TUNI)** |
| 26 | SISTEMA DE REGISTRO DE VISITAS - **(VISITAS)** |
| 28 | SISTEMA PARA CONVOCATORIA DE PRACTICANTES - **(PRACTICA)** |
| 29 | MÓDULO DE CREACIÓN DE CASILLAS ELECTRÓNICAS - **(CASILLA)** |
| 30 | BANDEJA DE ATENCIÓN GRADOS Y TÍTULOS - **(ATENCIONGYT)** |
| 31 | SERVICIO WEB VALIDACIÓN DE PERSONAS PJ - **(WS_VALIDAPJ)** |
| 33 | SISTEMA DE CONVOCATORIA DE CONCURSOS PÚBLICOS - **(TALENTO)** |
| 34 | PROYECTO BASE DE DATOS INTEGRADA - **(BDI)** |
| 35 | CONSULTA RENIEC VIA LINEA DEDICADA - **(LDRENIEC)** |
| 36 | SISTEMA DE SELECCIÓN DE PERSONAL PARA LA OFICINA DE RECURSOS HUMANOS - (**SELECCIONORH)** |
| 37 | SISTEMA DE VALIDACIÓN BIOMÉTRICA - **(BIOMETRICO)** |
| 39 | MÓDULO DE VERIFICACIÓN DE DOCUMENTOS ELECTRÓNICOS EMITIDOS - **(CONSULTA_DOC)** |
| 40 | WS_UNIVERSIDADES_PROGRAMAS - **(WSUNIPRO)** |
| 41 | MÓDULO DE MESA DE PARTES VIRTUAL - **(MPVIRTUAL)** |
| 42 | SISTEMA DE LICENCIAMIENTO DE UNIVERSIDADES - **(LINU)** |
| 43 | PORTAL INFORMATIVO TRASLADATE - (**METRASLADO)** |
| 45 | SISTEMA DE DENUNCIAS POR FALTA ENTREGA DE DOCUMENTACIÓN ACADÉMICA - **(DENUNCIA_ACERVO)** |
| 46 | SUNEDU LEGAL - **BUSCADOR LEGAL** |

**ANEXO N.° 2**
**DIAGRAMA DE PROCESOS**

- **De la creación, actualización y desactivación de cuentas para el acceso y uso de los activos informáticos**

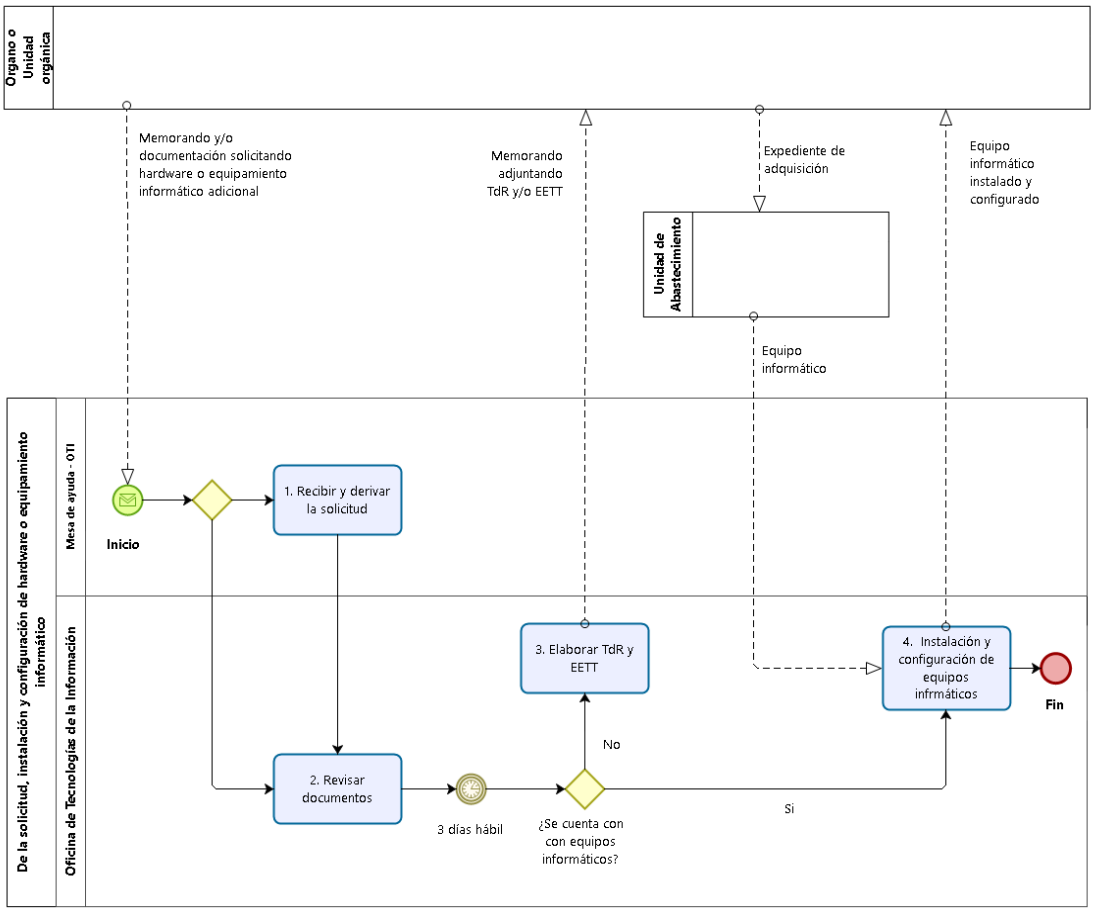


- **De la gestión y uso de las contraseñas**




-

- **De la solicitud, instalación y configuración de software y hardware o equipamiento informático**



- **De los incidentes en los activos informáticos**