INEI INSTITUTO NACIONAL DE ESTADISTICA E INFORMATICA

OFICINA TÉCNICA DE INFORMÁTICA

POLÍTICA DE USO ACEPTABLE

Código:	PLT-001-OTIN-2016-V01
Versión:	Versión 1.0
Fecha de la versión:	
Creado por:	Arlett Vanessa Agüero Vargas Unidad de Calidad y Seguridad de la Información
Aprobado por:	Ing° Manuel Matos Alvarado Director Técnico de la Oficina Técnica de Informática

Historial de modificaciones

Fecha	Versión	Creado por	Descripción de la modificación
	0.1	Arlett Agüero Vargas	Descripción básica del documento

INEI

Tabla de contenido






1. Objetivo, alcance y usuarios

El objetivo del presente documento es definir reglas claras para el uso de los sistemas y de otros activos de información en la Oficina Técnica de Informática – OTIN del Instituto Nacional de Estadística e Informática - INEI.

Este documento se aplica a todo el alcance del Sistema de Gestión de Seguridad de la Información (SGSI); es decir, a todos los sistemas y demás activos de información utilizados dentro del alcance del SGSI correspondiente a la OTIN.

Los usuarios de este documento son todos los colaboradores de la Oficina Técnica de Informática – OTIN del Instituto Nacional de Estadística e Informática - INEI.

2. Documentos de referencia

- Norma ISO/IEC 27001, capítulos:
  A.6.2.1, Política de dispositivos móviles
  A.6.2.2, Teletrabajo
  A.8.1.2, Propiedad de los activos
  A.8.1.3, Uso aceptable de los activos
  A.8.1.4, Retorno de activos
  A.9.3.1, Uso de información de autentificación secreta
  A.11.2.5, Remoción de activos
  A.11.2.6, Seguridad de equipos y activos fuera de las instalaciones
  A.11.2.8, Equipos de usuario desatendidos
  A.11.2.9, Política de escritorio limpio y pantalla limpia
  A.12.2.1, Controles contra códigos maliciosos
  A.12.3.1, Respaldo de la información
  A.12.5.1, Instalación de software en sistemas operacionales
  A.12.6.2, Restricciones sobre la instalación de software
  A.13.2.3, Mensajes electrónicos
  A.18.1.2, Derechos de propiedad intelectual
- Política de Seguridad de la Información
- Procedimiento Administrativo para la Gestión de Incidentes, Amenazas y Debilidades de la Seguridad de la Información en OTIN (PRA-011-OTIN-2016-V01)
- Procedimiento Administrativo para la Administración de Cuentas de Usuario para lo OTIN (PRA-009-OTIN-2016-V01).
- Inventario de activos de OTIN
- Resolución Jefatural N° 391-2015-INEI que aprueba la Directiva N° 007-2015-INEI, "Normas para el uso de correo electrónico y del internet en el Instituto Nacional de Estadística e Informática".

3. Uso aceptable de los activos de información

3.1. Definiciones

Sistema de información: incluye todos los servidores y clientes, infraestructura de red, software del sistema y aplicaciones, datos y demás subsistemas y componentes que pertenecen o son utilizados por la institución, o que se encuentran bajo responsabilidad de la institución. El uso de un sistema de información también incluye el uso de todos los servicios internos o externos, como el acceso a Internet, correo electrónico, etc.

Activos de información: en el contexto de esta Política, el término activos de información se aplica a los sistemas de información y demás información o equipos, incluyendo documentos en papel, teléfonos móviles, ordenadores portátiles, soportes de almacenamiento de datos, etc.

Sistema de gestión de seguridad de la información (SGSI): un conjunto de políticas de administración de la información y es para una organización el diseño, implantación, mantenimiento de un conjunto de procesos para gestionar eficientemente la accesibilidad de la información, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de información minimizando a la vez los riesgos de seguridad de la información.

Propietario del activo: El término "propietario" identifica a un individuo o entidad responsable, que cuenta con la aprobación del órgano de dirección, para el control de la producción, desarrollo, mantenimiento, uso y seguridad de los activos. El término "propietario" no significa que la persona disponga de los derechos de propiedad reales del activo.

Ordenador local: este término se utiliza para referirse al ordenador que el usuario utiliza para conectarse a la red Internet.

Administrador de red: persona designada por el Director Técnico de la Oficina Técnica de Informática para establecer accesos y configuración de la plataforma tecnológica que permita acceder o no a los servicios informáticos del INEI; además, se encarga de proteger la información de la distribución, acceso, modificación, destrucción y/o uso no autorizado.

Cuenta de usuario: es una colección de información que indica al sistema operativo los archivos y carpetas a los que puede tener acceso un determinado **usuario** del equipo, los cambios que puede realizar en él y sus preferencias personales, como el fondo de escritorio o el protector de pantalla.

Copia de seguridad: "copia de respaldo" o también llamado "backup" (su nombre en inglés) en tecnologías de la información e informática es una copia de los datos originales que se realiza con el fin de disponer de un medio para recuperarlos en caso de su pérdida.

Software antivirus: programa que ayuda a proteger su computadora contra la mayoría de los virus, worms, troyanos y otros invasores indeseados que puedan infectar el ordenador.

Escritorio: pantalla principal que podemos observar una vez que se inicializa el sistema, pantalla que contiene los íconos de muchos de los programas que utilizamos más frecuentemente.

Incidente: Según la norma ISO 27035, un Incidente de Seguridad de la Información es indicado por un único o una serie de eventos seguridad de la información indeseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones de negocio y de amenazar la seguridad de la información.

3.2. Uso aceptable

Los activos de información solamente pueden ser utilizados a fines de satisfacer necesidades de negocios con el objetivo de ejecutar tareas vinculadas con la institución.

3.3. Responsabilidad sobre los activos

Cada activo de información tiene designado un propietario en el Inventario de Activos. El propietario del activo es el responsable de la confidencialidad, integridad y disponibilidad de la información en el activo en cuestión.

3.4. Actividades prohibidas

Está prohibido utilizar los activos de información de manera tal que ocupen innecesariamente capacidad, que disminuya el rendimiento del sistema de información o que presente una amenaza de seguridad. También está prohibido:

- Descargar archivos de imágenes o vídeos que no tienen objetivos de negocios, enviar cadenas de correos electrónicos, jugar juegos, etc.
- Instalar software en un ordenador local sin el permiso explícito del Jefe inmediato y del Director Técnico de la OTIN.
- Utilizar aplicaciones Java, controles Active X y otros códigos móviles, excepto cuando esté autorizado por el Jefe inmediato y/o el Director Técnico de la OTIN.
- Descargar códigos de programa de soportes externos.
- Instalar o utilizar dispositivos periféricos como módems, tarjetas de memoria u otros dispositivos para almacenamiento y lectura de datos (por ej., dispositivos USB) sin el permiso explícito del Jefe inmediato y/o del Director Técnico de la OTIN.

3.5. Uso de activos fuera de las instalaciones

Los equipos, la información o software, independientemente de su formato o soporte de almacenamiento, no pueden ser retirados de las instalaciones sin el permiso escrito u Orden de Salida, según corresponda, con la firma de Jefe inmediato y/o del Director Técnico de la OTIN. Mientras los activos en cuestión permanecen fuera de la institución, deben ser controlados por la persona a la que se le concedió el permiso para retirarlo.

Los activos como equipos informáticos, salen fuera de la institución en los siguientes casos:

1) A otra institución, por reparación o trabajo.
2) A otra sede, por cambio de ubicación física.
3) Fuera de la institución, por trabajo de campo.

Es inusual que los equipos informáticos se retiren de la institución hacia el domicilio de los colaboradores responsables.

Para realizar la salida los activos (equipos informáticos, servidores), el área solicitante dirige un correo electrónico al responsable del área de Control Patrimonial, indicando:

a) Código Patrimonial
b) Lugar de origen y lugar de destino
c) Motivo
d) Responsable del traslado
e) Responsable del equipo

Del Área de Control Patrimonial se recibe la Orden de Salida que sigue su trámite y acompaña a la salida y el retorno de los equipos.

3.6. Devolución de activos a la finalización de un contrato

Al finalizar un contrato de empleo, o de otro tipo, a raíz del cual se utilizan diversos equipos, software o información en formato electrónico o papel, el usuario debe devolver todos esos activos de información a la persona designada para la recepción de entrega de cargo o Jefe inmediato de la OTIN.

3.7. Procedimiento para copias de seguridad

El usuario debe mantener copias de seguridad de toda la información sensible almacenada en su ordenador, como mínimo, una vez por día y de acuerdo a la importancia de la misma.

3.8. Protección antivirus

En cada ordenador debe estar instalado el software antivirus con actualización automática activada.

3.9. Facultados para el uso de sistemas de información

Los usuarios de los sistemas de información solamente pueden acceder a los activos de sistemas de información para los cuales han sido explícitamente autorizados por el propietario del activo.

Los usuarios pueden utilizar los sistemas de información únicamente para las actividades para las cuales han sido autorizados; es decir, para las cuales les han sido otorgados derechos de acceso.

Los usuarios no deben participar en actividades que puedan ser utilizadas para eludir controles de seguridad de los sistemas de información.

3.10. Responsabilidades sobre la cuenta de usuario

El usuario no debe, directa ni indirectamente, permitir que otra persona utilice sus derechos de acceso; es decir, su nombre de usuario; y no debe utilizar el nombre de usuario y/o clave de otra persona. El uso de nombres de usuario grupales está prohibido.

El personal que reciba una cuenta de usuario para el acceso de activos, es el propietario de dicha cuenta de usuario, quien deberá hacer uso adecuado de sus contraseñas de acceso manteniendo la confidencialidad de la misma y siendo responsable de su uso y de todas las transacciones realizadas con dicha cuenta de usuario.

La administración de cuentas de usuario deberá realizarse conforme al Procedimiento Administrativo para la Administración de Cuentas de Usuario para la OTIN (PRA-009-OTIN-2016-V01). Asimismo es responsabilidad de la inactivación de las cuentas de usuario el administrador de red, el Jefe inmediato de cada unidad funcional debe solicitar en el menor tiempo posible la inactivación de cuentas de usuario del personal que deje de prestar servicios en la OTIN y entidades externas que cuenten con acceso al servicio brindado.

3.11. Responsabilidades sobre la clave

Los usuarios deben aplicar buenas prácticas de seguridad en cuanto a la elección y uso de claves:

- No se deben revelar las claves a otras personas, incluyendo las direcciones, gerencias y los administradores del sistema.
- No se debe llevar un registro de las claves, a menos que un método seguro haya sido aprobado por la Oficina Técnica de Informática.
- Las claves generadas por el usuario no deben ser distribuidas por ningún medio (oral, escrito, electrónico, etc.).
- Las claves deben ser cambiadas si existen indicios de su vulnerabilidad, de que puedan estar en riesgo las mismas claves o el sistema (en ese caso, se debe informar un incidente de seguridad).
- Se deben escoger claves con un nivel adecuado de complejidad y seguras de la siguiente forma:
    - utilizando al menos ocho caracteres;
    - utilizando al menos un carácter numérico;
    - utilizando al menos un carácter alfabético en mayúscula y uno en minúscula;
    - utilizando al menos un carácter especial;
    - una clave no debe ser una palabra que se encuentre en el diccionario, en un dialecto o jerga de ningún idioma; como tampoco ninguna de estas palabras escritas hacia atrás;
    - las claves no deben estar relacionadas con datos personales (por ej., fecha de nacimiento, domicilio, nombre de un familiar, etc.);
    - no se deben usar nuevamente las últimas tres claves.
- Se deben cambiar las claves como mínimo cada 3 meses.
- Se deben cambiar las claves en el primer ingreso al sistema.
- Las claves no deben ser almacenadas en un sistema de registro automatizado (por ej., macros o explorador).
- No se deben utilizar las mismas claves personales para fines privados y para fines comerciales.

Sobre la creación de claves seguras, además puede consultar el "Procedimiento Administrativo para la Administración de Cuentas de Usuario para la OTIN (PRA-009-OTIN-2016-V01)".

3.12. Política de pantalla y escritorio limpio

Toda la información clasificada como "Uso interno", "Restringido" y "Confidencial" de acuerdo a la Clasificación de la Información que se efectúe en la Oficina Técnica de Informática - OTIN, es considerada sensible para este punto.

3.12.1. Política de escritorio limpio

Es de responsabilidad del usuario no dejar sus estaciones de trabajo desatendidas.

Si la persona autorizada no se encuentra en su puesto de trabajo, todos los documentos impresos, como también los soportes de almacenamiento de datos, etiquetados como sensibles, deben ser retirados del escritorio o de otros lugares (impresoras, equipos de fax, fotocopiadoras, etc.) para evitar el acceso no autorizado a los mismos.

Este tipo de documentos y soportes deben ser archivados de forma segura, de acuerdo a la Clasificación de la Información según corresponda.

3.12.2. Política de pantalla limpia

Si la persona autorizada no se encuentra en su puesto de trabajo, se debe quitar toda la información sensible de la pantalla, y se debe denegar el acceso a todos los sistemas para los cuales la persona tiene autorización.

En el caso de una ausencia corta (hasta 30 minutos), la política de pantalla limpia se implementa finalizando o cerrando la sesión en todos los sistemas o bloqueando la pantalla. Si la persona se ausenta por un período más prolongado (superior a 30 minutos), la política de pantalla limpia se implementa finalizando o cerrando la sesión en todos los sistemas y apagando el equipo informático.

3.12.3. Protección de instalaciones y equipos compartidos

Los documentos que contienen información sensible deben ser retirados inmediatamente de las impresoras, equipos de fax y fotocopiadoras.

Las instalaciones para envío y recepción de correo de cada usuario están protegidas siempre que el usuario no olvide bloquear la pantalla, cerrar la sesión o apagar el ordenador.

Los equipos de fax compartidos dentro de las instalaciones de la institución están protegidos con el cierre de las instalaciones o con el acceso limitado del personal en tanto el personal a cargo esté ausente.

El uso no autorizado de impresoras, fotocopiadoras, escáneres y demás equipamiento compartido para copiado dentro de las instalaciones de la institución se evita limitando el acceso a solo personal autorizado y a brindar acceso de impresión solo al personal que trabaja documentación.

3.13. Uso de Internet

Sólo se puede acceder a Internet a través de la red local de la institución, con la infraestructura y protección de cortafuegos adecuadas. El acceso directo a Internet mediante módems, Internet móvil, red inalámbrica u otros dispositivos de acceso directo a Internet, está prohibido.

El Administrador de red designado por la Dirección Ejecutiva de Soporte Técnico de la OTIN puede bloquear el acceso a determinadas páginas de Internet para usuarios individuales, grupos de usuarios o para todos los colaboradores de la institución. Si el acceso a algunas páginas Web está bloqueado, el usuario puede elevar el Anexo 1 de la Directiva N° 007-2015-INEI, "Normas para el uso de correo electrónico y del internet en el Instituto Nacional de Estadística e Informática", firmada por el Director Técnico de la OTIN que autoriza este acceso. El usuario no debe intentar eludir por su cuenta esa restricción.

El usuario debe considerar como no confiable la información recibida a través de sitios web no verificados. Ese tipo de información puede ser utilizada con fines comerciales solamente después de haber verificado su autenticidad y veracidad.

El usuario es responsable por todas las posibles consecuencias que surjan por el uso no autorizado o inadecuado de servicios o contenidos de Internet.

Sobre el uso de internet adecuado, consultar la Resolución Jefatural N° 391-2015-INEI que aprueba la Directiva N° 007-2015-INEI, "Normas para el uso de correo electrónico y del internet en el Instituto Nacional de Estadística e Informática".

3.14. Correo electrónico y otros métodos de intercambio de mensajes

Entre los métodos de intercambio de mensajes, aparte del correo electrónico, se puede incluir la descarga de archivos desde Internet, la transferencia de datos por medio de protocolo de transferencia de archivos, teléfonos, equipos de fax, el envío de mensajes de texto por teléfonos móviles, soportes móviles y foros o redes sociales.

De acuerdo con procedimientos internos de OTIN, el Administración de red designado en la OTIN, determina el canal de comunicación que se puede utilizar para cada tipo de dato, como también las posibles restricciones sobre quién tiene permiso para utilizar los canales; es decir, define qué actividades están prohibidas.

Los usuarios solamente pueden enviar mensajes que contengan información veraz. Está prohibido enviar materiales perturbadores, desagradables, sexualmente explícitos, groseros, difamatorios o cualquier otro contenido inaceptable o ilegal. Los usuarios no deben enviar mensajes basura a personas con las cuales no se ha establecido relación de negocios o a personas que no solicitaron ese tipo de información.

Si un usuario recibe un correo electrónico basura, debe informarlo o reenviarlo a los correos electrónicos: administrador@inei.gob.pe, soporte@inei.gob.pe y seguridad.otin@inei.gob.pe.

El usuario debe guardar todos los mensajes que contienen datos importantes para los negocios de la institución utilizando la copia de seguridad, según se indica en la Directiva N° 007-2015-INEI, "Normas para el uso de correo electrónico y del internet en el Instituto Nacional de Estadística e Informática".

Cada correo electrónico debe incluir una exención de responsabilidad, salvo los mensajes enviados a través de los sistemas de comunicación determinados por la institución. Si un usuario envía un mensaje a través de un sistema de intercambio de mensajes (redes sociales, foros, etc.), debe declarar sin ambigüedades que no representa el punto de vista de la institución.

Sobre el uso de correo electrónico adecuado, consultar la Resolución Jefatural N° 391-2015-INEI que aprueba la Directiva N° 007-2015-INEI, "Normas para el uso de correo electrónico y del internet en el Instituto Nacional de Estadística e Informática".

3.15. Derechos de autor

Los usuarios no deben realizar copias no autorizadas del software que pertenece a la institución, excepto en los casos permitidos por ley, por el propietario o por el jefe del área que lo custodia y de conformidad con el Decreto Legislativo N° 822 Ley sobre el Derecho de Autor y modificatorias como son la Ley N° 28571 Ley que modifica los Artículos 188° y 189° del Decreto Legislativo N° 822, Decreto Legislativo N° 1076 Ley Modificatoria del Decreto Legislativo N° 822.

Los usuarios no deben copiar software ni otros materiales originales de otras fuentes, y son responsables por todas las consecuencias que pudieran surgir bajo la ley de propiedad intelectual.

3.16. Computación móvil

3.16.1. Introducción

Entre los equipos de computación móvil se incluyen todo tipo de ordenadores portátiles, teléfonos móviles, tarjetas de memoria y demás equipamiento móvil utilizado para almacenamiento, procesamiento y transferencia de datos.

3.16.2. Reglas básicas

Se debe tener especial cuidado cuando los equipos de computación móvil se encuentran en vehículos u otros medios de transporte, espacios públicos, habitaciones de hotel, salas de reunión, centros de conferencias y demás áreas no protegidas exteriores a las instalaciones de la institución.

La persona que se lleva equipos de computación móvil fuera de las instalaciones debe cumplir las siguientes reglas:

- El equipamiento de computación móvil que contiene información importante, sensible o crítica no debe ser desatendido y, en lo posible, debe quedar resguardado bajo llave o se deben utilizar trabas especiales para asegurarlo.
- Cuando se utiliza equipamiento de computación móvil en lugares públicos, el usuario debe tener la precaución de que los datos no puedan ser leídos por personas no autorizadas.
- Las actualizaciones de parches y demás configuraciones del sistema son realizadas por el personal de Soporte Técnico de la Oficina Técnica de Informática.
- La protección contra códigos maliciosos se instala y actualiza por el personal de Soporte Técnico de la Oficina Técnica de Informática.
- La persona que utiliza equipamiento de computación móvil fuera de las instalaciones es responsable de realizar periódicamente copias de seguridad de datos.
- La conexión a redes de comunicación y el intercambio de datos debe reflejar la sensibilidad de los datos y se realiza conforme a las indicaciones de seguridad del Administrador de red designado por la Dirección Ejecutiva de Soporte Técnico de la OTIN.
- La información que se encuentra en ordenadores portátiles debe estar encriptada, en caso de considerarse archivos con información sensible.
- En el caso que el equipamiento de computación móvil sea desatendido, se deben aplicar las reglas para equipamiento de usuario desatendido de acuerdo a la Política de pantalla y escritorio limpios.

La Oficina Técnica de Informática será la responsable de la capacitación y concienciación de las personas que utilizan equipamiento de computación móvil fuera de las instalaciones de la institución.

3.17. Tele-trabajo

Tele-trabajo significa que los equipos de información y comunicación se utilizan para permitir que los empleados realicen su trabajo fuera de la institución. El tele-trabajo no incluye el uso de teléfonos móviles fuera de las instalaciones de la institución.

El tele-trabajo debe ser autorizado por el Jefe de Proyecto, quien comunicará mediante correo electrónico dirigido al Director Técnico de OTIN, la autorización otorgada indicando el nombre completo del usuario, la dirección IP a la que el usuario se conectará, el motivo y el periodo de uso de este servicio remoto (fecha inicio y fecha fin).

El Administrador de red designado por la Dirección Ejecutiva de Soporte Técnico de la OTIN, es el responsable de preparar planes y procedimientos para garantizar lo siguiente:

- Protección del equipamiento de computación móvil, de acuerdo a lo indicado en la sección anterior.
- Evitar el acceso no autorizado de personas que viven o trabajan en la ubicación donde se realiza la actividad de tele-trabajo.
- Configuración adecuada de la red local utilizada para conectarse a la Internet.
- Protección de los derechos de propiedad intelectual de la institución, tanto por el software como por otros contenidos que puedan estar protegidos por derechos de propiedad intelectual.

- Proceso de devolución de datos y equipamiento en caso de finalización del empleo.
- Nivel mínimo de configuración de la instalación donde se realizarán las actividades de tele-trabajo.
- Tipos de actividades permitidas y prohibidas.

3.18. Supervisión del uso de sistemas de información y comunicación

Todos los datos creados, almacenados, enviados o recibidos a través del sistema de información, o de otro sistema de comunicación, de la institución, incluyendo diversas aplicaciones, correo electrónico, Internet, fax, etc., independientemente de si es personal o no, se considera propiedad del Instituto Nacional de Estadística e Informática – INEI.

Los usuarios aceptan que personas autorizadas de la institución puedan acceder a todos los datos de ese tipo y que el acceso de dichas personas no será considerado una violación de privacidad del usuario.

La institución puede utilizar herramientas especializadas para identificar y bloquear métodos prohibidos de comunicación y para filtrar contenidos prohibidos.

3.19. Incidentes

Cada colaborador, proveedor o tercero que esté en contacto con datos y/o sistemas del de la OTIN del Instituto Nacional de Estadística e Informática – INEI, debe reportar toda debilidad del sistema, incidente o evento que pudiera derivar en un posible incidente, de acuerdo a lo establecido en el "Procedimiento administrativo para la gestión de incidentes, amenazas y debilidades de la seguridad de la información en OTIN".

4. Gestión de registros guardados en base a este documento

Nombre del registro	Ubicación de archivo	Persona responsable del archivo	Controles para la protección del registro	Tiempo de retención
Formato de requerimiento de software – Anexo 1	Intranet institucional, Normas Legales, en la ruta: http://iinei.inei.gob.pe/nuevo/normas/AbrirVentana.asp?varDoc=Directiva Nº 005-2003-INEI&varURL=/DOCUMENTOS/DI200305.pdf	Director Ejecutivo de Soporte Técnico	Los registros no pueden ser editados, sólo por el Director Ejecutivo de Soporte Técnico puede guardar estos registros o quien designe	Los registros son almacenados por el plazo de 3 años.
Formulario de solicitud	Intranet institucional,	Director Ejecutivo	Los registros no pueden ser editados,	Los registros

de acceso a servicios informáticos – Anexo 2	Intranet institucional, Normas Legales, en la ruta: http://iinei.inei.gob.pe/nuevo/normas/AbrirVentana.asp?varDoc=Directiva Nº 005-2003-INEI&varURL=/DOCUMENTOS/DI2003005.pdf	de Soporte Técnico	sólo el Director Ejecutivo de Soporte Técnico puede guardar estos registros o quien designe	son almacenados por el plazo de 3 años.

5. Validez y gestión de documentos

Este documento es válido hasta la publicación de su nueva versión.

El propietario de este documento es el Director Ejecutivo de Soporte Técnico de la Oficina Técnica de Informática, que debe verificar, el documento por lo menos una vez al año y si es necesario coordinar su actualización. Al evaluar la efectividad y adecuación de este documento, es necesario tener en cuenta los siguientes criterios:

- Cantidad de incidentes relacionados con el uso inadecuado o no autorizado de los activos de información.
- Cantidad de incidentes relacionados con inadecuados programas de capacitación o de concienciación de empleados sobre el uso aceptable de los activo de información.

6. ANEXOS

6.1 ANEXO 1: Formato de requerimiento de software

6.2 ANEXO 2: Formulario de solicitud de acceso a servicios informáticos (Individual y Grupal)

ANEXO 1

FORMATO DE REQUERIMIENTO DE SOFTWARE

Requerimiento de software

Nombre:
DDNN/TT donde labora:
Autorización:
Fecha:
Número de serie y ubicación de la computadora:

Programa de software	Fabricante	Versión	Utilización (1, 2, 3 o 4)

Utilización (clave)
1 = Diaria, 2 = Semanal, 3 = Mensual, 4 = Nunca

- ¿Existe software que Usted necesita pero que no tiene y que le ayudaría en la realización de sus tareas y funciones? Por favor lístelo a continuación y sustente con una justificación de uso:

Programa de software requerido	Sustento y/o justificación de uso

FRANK BRAVO MENDOZA

(*) Firma del Solicitante

Firma y Sello del Jefe

(*) Administrativo de la DDNN/TT

ANEXO 2

ANEXO 1

Formulario de Solicitud de Acceso a Servicios Informáticos (INDIVIDUAL)

INSTITUTO NACIONAL DE ESTADÍSTICA E INFORMÁTICA

Formulario de Solicitud de Acceso a Servicios Informáticos

El usuario deberá llenar COMPLETAMENTE el formulario, obtener las firmas y sellos requeridos. Para remitir el formulario a la Oficina Técnica de Informática del Instituto Nacional de Estadística e Informática.

DATOS DEL USUARIO:

NOMBRADO	CAS	LOCADOR	OTROS

CONTRATO

Fecha Inicio :

Fecha Término:

Nombres y Apellidos:

Dirección/ Oficina ... Correo electrónico ...
(Si es usuario nuevo dejar en blanco)

Cargo / Función ... Anexo ... Sede ...

Documento de Identidad

Tipo de Solicitud.				¿Existe Físicamente un punto de Red identificado?	
Creación	Modificación	Baja	Activación	SI	NO

SERVICIOS / SISTEMAS QUE SOLICITA (Marcar con una "X" lo requerido

CUENTA DE USUARIO DE RED			INTERNET, INTRANET		Perfil
CUENTA DE CORREO INSTITUCIONAL	Perfil		AUMENTO DE CAPACIDAD BUZÓN		
SIGA			SIAF		
SIGA MEF			SISTEMA TRÁMITE DOCUM.		

Director Técnico / Director Nacional que Autoriza:

(Nombre Completo)

COMPROMISO DEL USUARIO

Reconozco que como USUARIO a los servicios y recursos informáticos del INEI, tendré acceso a muchos datos e información privilegiada los cuales, debo protegerlos. Reconozco mi responsabilidad en el uso de mis accesos a la información de la institución incluyendo el uso de software ilegal o autorizado y del equipamiento para procesar o generar información para fines propios de mis funciones o autorizados por la institución. Mantendré y protegeré mi "contraseña", haciéndolo exclusivamente para propio uso. Seré responsable por compartir mi usuario y contraseña, así como de mi PC.

Firma del Usuario | Firma y Sello del DDNN/ODTT | ___/___/___ Fecha

1. **Acceso a Internet Avanzado= Básico, correo web, internet, redes sociales, social media, descarga y streaming.**
2. **Acceso a Internet Intermedio= Básico + Correo web, internet, no streaming.**
3. **Acceso a Internet Básico= Internet (Gobierno, Educación, noticias, Búsqueda)**
4. **Acceso a Intranet= Internet sólo para accesos básicos a la red.**
5. **Acceso a Correo Avanzado= Correo con dominio INEI.**
6. **Acceso a Correo Básico= Correo con dominio INEI.**

ANEXO 2

Formulario de Solicitud de Acceso a Servicios Informáticos (GRUPAL)

Aprueban los "Lineamientos de Políticas Generales para promover la masificación del acceso a Internet en el Perú" Los usuarios deberán llenar COMPLETAMENTE el formulario, obtener las firmas y sellos requeridos. Para remitir el formulario a la Oficina Técnica de Informática del Instituto Nacional de Estadística e Informática.

INEI	FORMULARIO DE SOLICITUD DE ACCESO A SERVICIOS INFORMÁTICOS							Fecha:
Dirección / Oficina: Sede:					Tipo de Solicitud: 1. Creación 2. Modificación 3. Baja 4. Desactivación			
N°	NOMBRES	APELLIDOS	DNI	CARGO	PERFIL CORREO	PERFIL INTERNET	TIPO DE SOLICITUD	CONDICIÓN DE CONTRATO	FIRMA

Director Técnico / Director Nacional que Autoriza:

(Nombres Completo, Sello y Firma)

1. Acceso a Internet Avanzado= Básico, correo web, internet, redes sociales, social media, descarga y streaming.
2. Acceso a Internet Intermedio= Básico + Correo web, Internet, no streaming.
3. Acceso a Internet Básico= Internet (Gobierno, Educación, noticias, Búsqueda)
4. Acceso a Intranet= Internet sólo para accesos básicos a la red.
5. Acceso a Correo Avanzado= Correo con dominio INEI.
6. Acceso a Correo Básico= Correo con dominio INEI.