# DIRECTIVA Nº 007-G/14

**PARA** : Todas las Gerencias

**ASUNTO** : Acceso a sistemas informáticos y medidas de seguridad

## I. OBJETIVO

Establecer las normas para el otorgamiento y utilización de los accesos a los sistemas informáticos de la Empresa y aplicar las medidas de seguridad de la información.

## II. ALCANCE

El presente documento está dirigido para todos los trabajadores de la Empresa con acceso a los sistemas informáticos de la misma.

## III. BASE LEGAL

1. Decreto Legislativo Nº 685 Ley de Creación de SERPOST S.A.
2. Estatuto de SERPOST S.A.
3. Resolución de Contraloría N° 320-2006-CG-Normas de Control Interno
4. Norma Técnica Peruana NTP-ISO/IEC 17799:2007 EDI. Tecnología de la Información. Código de Buenas Prácticas para la gestión de la seguridad de la información 2ª Edición en todas las entidades integrantes del Sistema Nacional de Informática.
5. Norma Técnica Peruana NTP-ISO/IEC 27001:2008 EDI. Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. Normativa interna

## IV. DEFINICIONES

1. **Riesgo:** Proximidad o posibilidad de un daño, peligro, amenaza, contingencia, emergencia, urgencia.
2. **Seguridad de la información:** Se refiere a las medidas tomadas con la finalidad de preservar los datos o información que en forma no autorizada, sea accidental o intencionalmente, puedan ser modificados, destruidos o divulgados, así como la preservación de otras características como la autenticidad, no rechazo, responsabilidad y confiabilidad. [NTP ISO/IEC 17799:2007]
3. **Delitos:** Se puede citar fraudes, falsificación, venta de información.
4. **Privacidad:** Se define como el derecho que tienen los individuos y organizaciones para determinar, ellos mismos, a quién, cuándo y qué información referente a ellos serán difundidas o transmitidas a otros.
5. **Integridad:** Se refiere a que los valores de los datos se mantengan tal como fueron puestos intencionalmente en un sistema. El concepto de integridad abarca la precisión y la fiabilidad de los datos, así como la discreción que se debe tener con ellos.

6. **Datos:** Los datos son hechos y cifras que al ser procesados constituyen una información, sin embargo, muchas veces datos e información se utilizan como sinónimos. Los datos pueden ser cualquier forma de información: campos de datos, registros, archivos y bases de datos, texto (colección de palabras), hojas de cálculo (datos en forma matricial), imágenes (lista de vectores o cuadros de bits), video (secuencia de tramas), otros.
7. **Base de Datos:** Una base de datos es un conjunto de datos organizados, entre los cuales existe una correlación y que además, están almacenados con criterios independientes de los programas que los utilizan.
8. **Acceso:** Es la recuperación o grabación de datos que han sido almacenados en un sistema de computación. Cuando se consulta a una base de datos, los datos son primero recuperados hacia la computadora y luego transmitidos a la pantalla del terminal.
9. **Ataque:** Término general usado para cualquier acción o evento que intente interferir con el funcionamiento adecuado de un sistema informático o intento de obtener de modo no autorizado la información confiada a una computadora.
10. **Ataque activo:** Acción iniciada por una persona que amenaza con interferir el funcionamiento adecuado de una computadora, o hace que se difunda de modo no autorizado información confiada a una computadora personal. Ejemplo: El borrado intencional de archivos, la copia no autorizada de datos o la introducción de un virus diseñado para interferir el funcionamiento de la computadora.
11. **Ataque pasivo:** Intento de obtener información o recursos de una computadora personal sin interferir con su funcionamiento, como espionaje electrónico, telefónico o la intercepción de una red. Todo esto puede dar información importante sobre el sistema, así como permitir la aproximación de los datos que contiene.
12. **Amenaza:** Causa potencial de un incidente no deseado que pueda interferir con el funcionamiento adecuado de una computadora personal o sistema informático, así como causar la difusión no autorizada de información confiada en las mismas. Ejemplo: Fallas de suministro eléctrico, virus, saboteadores o usuarios descuidados.
13. **Incidente:** Cuando se produce un ataque o se materializa una amenaza, se tiene un incidente, como por ejemplo las fallas de suministro eléctrico o un intento de borrado de un archivo protegido. Tiene una gran probabilidad de comprometer las operaciones del negocio y de amenazar la seguridad de la información.
14. **Golpe (breach):** Es una violación con éxito de las medidas de seguridad, como el robo de información, el borrado de archivos de datos valiosos, el robo de equipos, PC, entre otros.
15. **Usuario final:** Es la persona que tiene una vinculación con la Empresa y que utiliza los equipos y servicios informáticos ofrecidos por la misma.
16. **Red:** El conjunto de computadoras y otros equipos interconectados, que comparten información, recursos y servicios informáticos.

## V. NORMA

## 1. Acceso a los Sistemas Informáticos:

La Subgerencia de Tecnologías de la Información a través del Departamento de Tecnología y Comunicaciones, proporcionará los accesos a los distintos grupos de usuarios fijados de acuerdo a las funciones que realizan y las características del entorno en el que trabajan:

a. Acceso a Equipos Informáticos para el Usuario final.
b. Acceso a los Sistemas de la Empresa (Sistemas externos adquiridos a proveedores o Sistemas propios desarrollados por el Departamento de Sistemas de la Información)
c. Acceso a la Base de Datos (Base de datos corporativa u otras bases de datos que utiliza cada área de la Empresa)
d. Acceso a la red, correo electrónico, internet, carpetas compartidas, otros.

### 1.1. Administración de Accesos de Usuarios

#### 1.1.1. Registro y anulación de cuentas de usuarios:

a. Cada Jefe de Departamento, Administrador Postal o cargo superior, será responsable de solicitar al Departamento de Tecnología y Comunicaciones, a través del Equipo de Mesa de Ayuda, la creación de una cuenta de usuario de los recursos informáticos para el personal nuevo de la Empresa, vía el sistema de atención de tickets, correo electrónico u hoja de coordinación, la misma que deberá precisar el perfil de usuario requerido, es decir, las características necesarias para la elaboración de sus funciones, nivel de acceso a internet, otros. (Utilizar el Anexo 1 y/o 2 según sea necesario).

b. El Departamento de Tecnología y Comunicaciones deberá evaluar las solicitudes correspondientes y coordinar con el Departamento de Sistemas de Información o Centro de Datos Corporativo a fin de dar respuesta a ellas en un plazo no mayor a veinticuatro (24) horas. En caso de aprobarlas, deberá proporcionar la cuenta de usuario, con su respectiva contraseña, para acceso a los recursos solicitados, junto con una relación de todos los derechos de accesos que poseen para la conformidad del usuario; asimismo el usuario final deberá firmar el Acta de Confidencialidad (Utilizar Anexo 3). Las contraseñas de acceso a los equipos informáticos deberán tener una cadena mínima de 8 caracteres. El cambio de contraseña es responsabilidad del usuario y se efectuará con una periodicidad de 90 días calendarios; asimismo lo podrá actualizar en cualquier otro momento, que por temas de seguridad considere necesario.

c. En caso de rechazar la solicitud, se deberá indicar los motivos de esta decisión y brindar recomendaciones para una correcta asignación del perfil al nuevo usuario. La atención a solicitudes rechazadas deberá darse en un periodo no mayor a veinticuatro (24) horas.

d. Las áreas de la Empresa que cuenten con un Administrador de red solicitarán el acceso por intermedio de éste, el mismo que solicitará a través de Mesa de Ayuda el acceso a los sistemas informáticos con los permisos correspondientes de acuerdo al desarrollo de sus funciones; la diferencia que existe entre permisos está referido al acceso a los diferentes módulos de los sistemas de la Empresa.

e. El Departamento de Administración de Personal y los Jefes de cada área comunicarán al Departamento de Tecnología y Comunicaciones, bajo responsabilidad, el cese de los trabajadores y los cambios de área, según corresponda, inmediatamente después de haberse producido estas acciones. El Departamento de Tecnología y Comunicaciones coordinará con el Administrador del Centro de Datos de SERPOST, con el Departamento de Sistemas de Información y/o Centro de Datos Corporativo a fin de que se efectúe el mantenimiento de los sistemas de administración de usuarios dentro de las veinticuatro (24) horas siguientes. Los derechos de acceso para todos los usuarios de información serán removidos a la culminación del contrato, en caso de cambio de área de trabajo se deberá ajustar los permisos y perfiles según corresponda.

### 1.1.2. Administración de contraseñas de usuario:

a. Los usuarios son responsables del cambio de contraseña de sus cuentas, la cual deberá realizarse apenas la reciba y con una periodicidad de 90 días calendarios; asimismo, deberán mantener secretas las contraseñas asignadas y evitar guardarlas en papel, archivos u otros dispositivos. Bajo ningún concepto está permitido compartir cuentas de usuarios con otros trabajadores, bajo responsabilidad.

b. Las contraseñas serán entregadas a los Jefes de cada área o a los encargados de la administración u oficina postal a través del correo electrónico, los cuales deberán, por seguridad, entregarse de manera personal a cada usuario, junto con una relación de los derechos otorgados y un compromiso para no compartir la contraseña a los usuarios, previa verificación de la identidad del usuario. Por su parte, los usuarios deberán portar un documento que permita identificarlos y firmar un acuse de lo recibido (según Anexo 1 y/o 2), el cual deberá ser remitido por los Jefes de cada área o los encargados de la administración u oficina postal a través del correo electrónico en un periodo no mayor a veinticuatro (24) horas en formato digital al Departamento de Tecnología y Comunicaciones para el control y resguardado respectivo.

c. En caso algún usuario olvide su clave de acceso, el Jefe inmediato solicitará el reemplazo al Departamento de Tecnología y Comunicaciones a través del Equipo de Mesa de Ayuda, mediante el sistema de atención de tickets, correo electrónico a la cuenta mesadeayuda@serpost.com.pe u hoja de coordinación; el usuario apenas reciba su nueva clave de acceso deberá modificarla.

### 1.1.3. Administración de contraseñas críticas:

Para el caso de las contraseñas de los servidores y base de datos se deberá realizar lo siguiente:

***SERVIDORES ADMINISTRADOS POR SERPOST***

La Subgerencia de Tecnologías de la Información a través del Departamento de Tecnología y Comunicaciones deberá actualizar periódicamente las

claves de acceso a los servidores que son administrados por SERPOST y que se encuentran en su Centro de Datos, las cuales se deberán efectuar con una periodicidad de noventa (90) días calendarios, dentro de los primeros cinco (5) días hábiles de cada trimestre del año; asimismo se deberá actualizar en cualquier otro momento que se considere necesario, sin que esta modifique el cronograma, como en el caso de la ocurrencia del cese o cambio de área de algún personal que se le hizo entrega de la última clave actualizada, para lo cual se procederá de la siguiente manera:

a. El Jefe del Departamento de Tecnología y Comunicaciones, deberá:

   - Solicitar al Centro de Datos Corporativo el cambio de la clave de acceso a los servidores, la misma que no deberá repetirse con ninguna clave anterior utilizada, una vez recibida la nueva clave las mantendrá en custodia en un sobre lacrado hasta el próximo cambio y/o para la posterior entrega al personal asignado a esta función.

   - Entregar al personal responsable de la administración del Centro de Datos de SERPOST las claves de acceso a los servidores en un sobre lacrado a través de un Memorándum para que realice el cambio respectivo. Asimismo, dicho personal deberá firmar un acuerdo de confidencialidad en el cual se compromete a no revelar, comentar, suministrar o transferir de cualquier forma, tal información a terceros puesto que esta clave permite el acceso a datos e información confidencial y privilegiada (utilizar el Anexo 4).

   - Entregar al Subgerente de Tecnologías de la Información en un sobre lacrado las claves de acceso a los servidores como medida de contingencia.

b. El personal responsable de la administración del Centro de Datos de SERPOST deberá comunicar mediante un informe al Jefe del Departamento de Tecnología y Comunicaciones con copia a la Subgerencia de Tecnologías de la Información las actividades realizadas respecto al cambio de clave realizado.

c. De requerirse el acceso a los servidores administrados por SERPOST para otro personal del Departamento de Tecnología y Comunicaciones, deberá ser solicitado por el Jefe del Departamento de Tecnología y Comunicaciones a la Subgerencia de Tecnologías de la Información para su aprobación; de ser aprobado, el Jefe del Departamento de Tecnología y Comunicaciones entregará la clave en sobre lacrado y el documento de acuerdo de confidencialidad para la firma respectiva. (utilizar el Anexo 4).

***USUARIOS DE BASE DE DATOS PARA CONFIGURACION DE LOS APLICATIVOS DE SERPOST***

La Subgerencia de Tecnologías de la Información a través del Departamento de Tecnología y Comunicaciones deberá actualizar periódicamente las claves de los usuarios para la conexión a las Bases de Datos de los

aplicativos desarrollados por el Departamento de Sistemas de Información, las cuales se deberán efectuar con una periodicidad de noventa (90) días calendarios, dentro de los primeros cinco (5) días hábiles de cada trimestre del año; asimismo se deberá actualizar en cualquier otro momento que se considere necesario, sin que esta modifique el cronograma, como en el caso de la ocurrencia del cese o cambio de área de algún personal al cual se le hizo entrega de la última clave actualizada, para lo cual se procederá de la siguiente manera:

a. El Jefe del Departamento de Tecnología y Comunicaciones, deberá:

- Solicitar al Centro de Datos Corporativo el cambio de las claves de los usuarios para la conexión de los aplicativos a las Bases de Datos, la misma que no deberá repetirse con ninguna clave anterior utilizada, una vez recibida las nuevas claves las mantendrá en custodia en un sobre lacrado hasta el próximo cambio y/o para la posterior entrega al personal asignado a esta función.

- Entregar al Jefe del Departamento de Sistemas de Información las claves de acceso correspondientes en un sobre lacrado y a través de un Memorándum para que realice el cambio respectivo. Dicho personal deberá firmar un acuerdo de confidencialidad en el cual se compromete a no revelar, comentar, suministrar o transferir de cualquier forma, tal información a terceros puesto que esta clave permite el acceso a datos e información confidencial y privilegiada. (Utilizar el Anexo 4).

- Entregar al Subgerente de Tecnologías de la Información en un sobre lacrado las claves de acceso respectivas como medida de contingencia.

b. El Jefe del Departamento de Sistemas de Información comunicará mediante un informe al Subgerente de Tecnologías de la Información respecto a la actualización de la nueva clave en los aplicativos.

c. De requerirse el acceso de la clave para otro personal del Departamento de Sistemas de Información, el Jefe del Departamento de Sistemas de Información deberá solicitar a la Subgerencia de Tecnologías de la Información para su aprobación; de ser aprobado, el Jefe del Departamento de Sistemas de Información entregará a dicho personal la clave en sobre lacrado y el documento de acuerdo de confidencialidad para la firma respectiva. (utilizar el Anexo 4).

### 1.1.4. Revisión de Derechos de Acceso de Usuarios

a. El Departamento de Tecnología y Comunicaciones revisará periódicamente el sistema de administración de acceso a la red y sistemas externos o adquiridos, a fin de obtener la relación de usuarios, perfiles y permisos actualizados. Deberá coordinar y comunicar a todas las áreas sobre los usuarios activos en el sistema, a fin de que sean depurados los

que no correspondan, las cuales se deberán efectuar con una periodicidad de seis (6) meses dentro de los primeros diez (10) días hábiles de cada semestre, bajo responsabilidad. Asimismo, las áreas deberán proporcionar la información que les sea solicitada para dicho fin, bajo responsabilidad.

b. El Departamento de Sistemas de Información revisará periódicamente el sistema de administración de acceso a los sistemas desarrollados por SERPOST, a fin de obtener la relación de usuarios, perfiles y permisos actualizados. Deberá coordinar y comunicar a todas las áreas sobre los usuarios activos en el sistema, a fin de que sean depurados los que no correspondan, las cuales se deberán efectuar con una periodicidad de seis (6) meses dentro de los primeros diez (10) días hábiles de cada periodo, bajo responsabilidad. Asimismo, las áreas deberán proporcionar la información que les sea solicitada para dicho fin, bajo responsabilidad.

**1.2. Responsabilidades de los usuarios:**

a. Los servicios de acceso a la red, sistemas, correo electrónico, internet y documentos que existen en los equipos informáticos son de responsabilidad de los usuarios asignados y solo podrán utilizarse para propósitos lícitos, responsables y en cumplimiento de sus funciones.

b. Los usuarios que tengan acceso a internet deberán acceder a sitios seguros y no descargarán contenido ni programas no autorizados, sin licencias o de procedencia no confiable.

c. Está prohibido utilizar los recursos informáticos de la Empresa para fines que no estén relacionados con el desarrollo de sus funciones, así como, la creación e introducción de virus o cualquier otro software perjudicial o nocivo que puedan ser utilizados para atacar los sistemas informáticos de la Empresa.

d. Los usuarios de la Empresa cuidarán que las contraseñas o claves de acceso se mantengan en estricta confidencialidad, ya que estos son la principal protección contra el ingreso no autorizado a los servicios de red y sistemas.

e. Todos los trabajadores que tengan asignados recursos informáticos y acceso a sistemas son únicos responsables de todos los efectos del uso que se derive de ellas; por tal motivo deberá cerrar la sesión o bloquear su estación de trabajo al momento de ausentarse.

f. La divulgación de la información y la manipulación indebida de las claves de acceso de los sistemas y los daños de información que pudiera ser generado será responsabilidad directa de los usuarios autorizados de dicha información, tal hecho será sancionado de acuerdo a la normativa vigente.

g. Cuando los usuarios detecten cualquier incidente, acceso indebido o problema de seguridad de información que surjan en el uso de los equipos de la Empresa deben comunicar al Departamento de Tecnología y Comunicaciones o a los administradores de red a nivel nacional.

**2. Medidas de Seguridad en los Sistemas Informáticos:**

a. El Jefe del Departamento de Tecnología y Comunicaciones y el Jefe del Departamento de Sistemas de la Información comunicarán las incidencias de

Seguridad y las propuestas de solución a la Subgerencia de Tecnologías de la Información.

b. La Subgerencia de Tecnologías de la Información, comunicará las incidencias de Seguridad y las propuestas de solución al Comité de Seguridad de Información de la Empresa.

c. El Departamento de Tecnología y Comunicaciones es el único autorizado para la instalación de software en los equipos de cómputo de la Empresa. Los programas informáticos deben contar con licencia o autorización del uso válido a nombre de la Empresa.

d. Está prohibido cualquier retiro de equipo de cómputo de la Empresa salvo autorización del Jefe del Departamento de Tecnología y Comunicaciones o Subgerente de Tecnologías de la Información, previa gestión de desplazamiento ante el Departamento de Control Patrimonial y Seguros Generales.

e. El Departamento de Tecnología y Comunicaciones es responsable de difundir las reglas de seguridad para el manejo, funcionamiento y cuidado de los equipos de cómputo, asimismo, distribuir avisos sobre la Seguridad de la Información y aparición de nuevos virus informáticos que son difundidos a través de Internet.

f. El Departamento de Tecnología y Comunicaciones es responsable del mantenimiento de los equipos de cómputo, el mismo que se efectuará de forma periódica en las diferentes áreas de la Empresa, este mantenimiento podrá efectuarse a través de terceros, cuando corresponda. En caso de Provincias la supervisión del servicio de mantenimiento estará bajo la responsabilidad del administrador de la Administración Postal.

g. El Departamento de Tecnología y Comunicaciones es responsable de hacer backups de la información relevante para la Empresa y almacenarlos en lugares adecuadamente preparados para ese fin.

## VI. DISPOSICIONES COMPLEMENTARIAS

1. El presente documento deroga a la Directiva N° 010-G/10 **"Acceso a Sistemas Informáticos y Medidas de Seguridad"**, aprobada con fecha 31/08/10.
2. Todos los trabajadores con acceso a los sistemas informáticos deberán cumplir lo establecido en la presente Directiva desde el momento en que hacen uso de los recursos informáticos ofrecidos por la Empresa.
3. Los aspectos no contemplados en la presente directiva, serán resueltos por la Subgerencia de Tecnología de la Información.
4. La Empresa aplicará las sanciones correspondientes de acuerdo con lo establecido en el Reglamento Interno de Trabajo, cuando el usuario no cumpla con las medidas de seguridad establecida en la presente Directiva.

## VII. AUTORIZACION

La presente Directiva queda aprobada por Gerencia General y entrará en vigencia a partir de la fecha de su suscripción.

**Lima, 7 de noviembre de 2014**

**Original firmado por FRIBERG QUISPE GRAJEDA**
**Gerente General (e)**

# Anexo 1

## Formato de solicitud de Acceso a Sistemas Informáticos (Versión 1.0)

### Formato de solicitud de Acceso a Sistemas Informáticos (Versión 1.0)

N° 2014 - xxx (Llenado por TI)

Fecha / / (dd/mm/aa)

### 1.Datos Generales del Usuario

| | | | |
|---|---|---|---|
| Cod. del Trabajador | | Cargo | |
| Nombres | | Centro de Responsabilidad | |
| Apellido Paterno | | | |
| Apellido Materno | | Descripción del Dpto. | |

### 2.Motivo de la Solicitud

| | | | | | |
|---|---|---|---|---|---|
| Usuario Nuevo | | Cambio de Area | | Nuevas Funciones | |

Otros (Especificar): _____

### 3.Servicio de Red

Usuario posee cuenta de Red? NO [ ] SI [ ] Colocar Cuenta de red: _____

| | C | E | M |
|---|---|---|---|
| Internet | | | |
| Correo Electronico | | | |
| Carpeta de Servidor | | | |
| Otros | | | |

(Marcar con una X)

| Glosario | |
|---|---|
| C | Creación |
| E | Eliminación |
| M | Modificación |

### 4.Consultas/Sugerencias

Jefe/Sug G./ Gerente

Firma y Sello del Solicitante

Area:

# Anexo 2

## Formato de solicitud de Acceso a Sistemas Informáticos (Versión 1.0)

| Formato de solicitud de Acceso a Sistemas Informáticos (Versión 1.0) | |
|---|---|
| N° | 2014 - xxx (Llenado por TI) |
| Fecha | / / (dd/mm/aa) |

| 1.Datos Generales del Usuario | | | |
|---|---|---|---|
| Cod. del Trabajador | | Cargo | |
| Nombres | | Centro de Responsabilidad | |
| Apellido Paterno | | | |
| Apellido Materno | | Descripción del Dpto. | |

| Glosario | |
|---|---|
| **C** | Creación |
| **E** | Eliminación |
| **M** | Modificación |

| 2.Acceso de Sistemas | Marcar con x | | |
|---|---|---|---|
| **Servicio Postal Tradicional** | **C** | **E** | **M** |
| Sistemas de Cuentas Internacionales | | | |
| Sistema Operativo Postal (SOP) | | | |
| SOP-Modulo de Tramite Aduanero de Despachos Simplificados | | | |
| Sistema de Apartados Postales | | | |
| Sistema de Soporte de Administraciones Postales -SSAP | | | |
| Modulo de Chasqui | | | |
| International Postal System -IPS | | | |
| **Servicio Postal de Clientes Empresariales** | **C** | **E** | **M** |
| Sistema Integrado de Mensajeria -SIM version 2.0 | | | |
| SIM- Modulo Sunat Lima | | | |
| SIM- Modulo Sunat Cuzco | | | |
| Sim- Modulo SUNARP | | | |
| SIM -Modulo PRJ -Judicial | | | |
| **Sistema Giros** | **C** | **E** | **M** |
| SSAP -Modulo de Giros Electronicos | | | |
| Internacional Financial System -IFS | | | |
| **Sistemas Administrativos** | **C** | **E** | **M** |
| Sistema de Soporte e Inventario de Equipos Imformaticos | | | |
| Sistema de Tramite Documentario | | | |
| Sistema de Presupuestos- Modulo Formulacion Presupuestal | | | |
| Modulo de Fondo Presupuestal | | | |
| SPRING - Recursos Humanos | | | |
| **Otros** | **C** | **E** | **M** |
| | | | |

| 3.Consultas/Sugerencias |
|---|
| |

Jefe/Sug G./ Gerente

Firma y Sello del Solicitante

Area:

| GLOSARIO | |
|---|---|
| **Sistema y /o Aplicativo** | **Breve Descripción de la funcionalidad** |
| Sistema de Cuentas Internacionales | El Sistema de Cuentas Internacionales contempla el registro del seguimiento y generación de toda la documentación de sustento de la Cobranza Internacional por Concepto de Distribución de Correspondencia Internacional, de los diferentes servicios; como son: Gastos Terminales (Servicio Postal Universal), EMS, Encomiendas Internacionales y (Envíos) Mal Encaminados. |
| Sistema Soporte e Inventario de Equipos Informáticos | Este sistema ha sido desarrollado para el uso exclusivo del Departamento de Tecnología y Comunicaciones para registrar el inventario de los equipos informáticos de la Empresa.<br>Como otra funcionalidad tendrá el control del soporte que tendrá un alcance a nivel de toda la Empresa a través del módulo de Requerimientos, el cual proporcionará información sobre las necesidades en lo que respecta a la operatividad del hardware y software (comercial o propio). |
| Sistema Operativo Postal | Este sistema ha sido diseñado para dar soporte a las labores operativas del CCPL en el tratamiento de la correspondencia registrable (Correspondencia Certificada, EMS, Encomiendas Internacionales, Pequeños Paquetes), de la carga postal internacional y nacional, tanto de llegada como salida. |
| Módulo de Trámite Aduanero de Despachos Simplificados | Este sistema da soporte a las actividades que son realizadas por el servicio TADS Express, el cual realiza el Desaduanaje de los envíos postales Internacionales de llegada, que son aforables por la SUNAT – ADUANA POSTAL DEL CALLAO.<br>Tiene también como función las transmisiones electrónicas de reexpediciones de las sacas en tránsito, entre otras. |
| Sistema Integrado de Mensajería versión 2.2 | Este sistema ha sido desarrollado para dar soporte a las actividades del servicio empresarial de los clientes captados por la Gerencia Comercial, estas actividades son las siguientes:<br>- Transferencia de la data del cliente<br>- Emisión de cargos<br>- Registro del resultado de la distribución<br>- Transferencia de la data con los resultados de la distribución al cliente<br>- Entre otras. |
| Sistema de Apartados Postales | Este sistema tiene como función principal la administración del servicio de Apartados Postales en las Administraciones Postales, registrando los apartados nuevos, que se encuentran de baja, así como, las transacciones en los pagos del alquiler de los mismos. |
| Sistema de Tramite Documentario | Este sistema desarrollado por la Empresa INNOVA, a solicitud de la Gerencia General, el cual da soporte a las actividades secretariales de una Gerencia o Subgerencia e integrado con la mesa de partes de la Empresa. |
| Modulo Servicio Expreso Seguro | Este módulo forma parte del SSAP y como función principal es la admisión y facturación de los envíos del servicio Expreso Seguro. |
| Módulo de Atención al Cliente SUNAT | El módulo de atención al cliente SUNAT cuenta con las siguientes características:<br>- Importación de la información del cliente en archivos DBF's<br>- Impresión de Etiquetas<br>- Generación de Hojas de ruta<br>- Liquidación de Hojas de ruta<br>- Consultas y Reportes<br>- Generación de archivos de exportación para SUNAT<br>- Registro en línea por medio de aplicativo móvil<br>- Registro manual de información del resultado de la distribución. |
| Sistema De Soporte de Administraciones Postales | Este sistema comprende el circuito completo en el procesamiento de envíos, desde su ingreso por ventanilla, la contabilidad en la caja de la Administración y el respectivo despacho, el cual además permite trabajar con el proceso de distribución.<br>Se ha repontenciado las propiedades de los sistemas anteriores a este, y se han estandarizado muchos procedimientos, como por ejemplo el control de los depósitos bancarios. |
| Módulo de Giros Electrónicos Local | Este módulo ha sido desarrollado para estar integrado con el SSAP y dará soporte en la gestión de la entrega del encaje a cada Administración Postal, Gestión en las cajas, admisión y pago del servicio de Correo Giro Nacional. |
| Sistema de Recursos Humanos – SPRING | Sistema adquirido en el 2010 a la empresa Royal System, este sistema denominado SPRING abarca las actividades siguientes:<br>- Generación de Planillas de Haberes Mensual<br>- Control de asistencia del personal<br>- Registro de información de Bienestar social<br>- Registro de información de Capacitación<br>- Entre otras. |
| International Postal System versión 5.0 | Este sistema ha sido desarrollado por la Unión Postal Universal UPU e implementado en el CCPL para el procesamiento de la correspondencia con destino Internacional. |
| Sistema de Giros Postales | Este sistema tiene la característica principal de dar soporte a la administración de giros postales enviados al Perú por las oficinas internacionales. |
| International Financial System – IFS | Este sistema ha sido desarrollado por la Unión Postal Universal UPU e implementado en el Departamento de Giros Postales y en la oficinas postales a nivel nacional para admisión y pagos de los giros electrónicos internacionales con los países España, Chile, Uruguay, Costa rica, Ecuador y Colombia. |
| Carpeta de servidor | Es una carpeta de acceso que contiene normas, procedimientos, directivas, reglamentos y proyectos internos. |

# Anexo 3

## Acuerdo de Confidencialidad Para Personal / Locador de Servicios Postales del Perú S.A.

_____, ____ de _____ de _____
<Nombre de Ciudad> <Día> <Mes> <Año>

Yo, _____, con DNI _____, personal ( ) / locador ( ) de Servicios Postales del Perú S.A. del área de _____ en la sede de _____, suscribo el presente acuse de recibo de credenciales y acuerdo de confidencialidad.

Declaro ser consciente de la importancia de las credenciales que me fueron asignadas y acepto que las mismas solo serán utilizadas para los propósitos de mis funciones, en la red y sistemas de Servicios Postales del Perú S.A.

Adicionalmente, entiendo que la publicación, traspaso no autorizado o mal uso de las mismas están sujetos a sanciones definidas por la Subgerencia de Recursos Humanos y, en algunos casos, puede ser un crimen penado por ley.

Debido a ello, durante la vigencia del vínculo laboral o contrato de locación, me comprometo a no compartir mis claves de acceso a los recursos institucionales y me responsabilizo en comunicar por escrito o correo electrónico a mi superior jerárquico y al Departamento de Tecnología y Comunicaciones en caso de detectar el uso no autorizado de los mismos, a fin de que se tomen los correctivos necesarios.

El compromiso indicado en el párrafo precedente incluirá un periodo de cinco (5) años posteriores a la finalización del vínculo laboral con SERPOST o término del contrato de locación.

Dejo constancia por escrito a través de este documento, de mi aceptación a los términos y condiciones, aquí expresados.

Colaborador

# Anexo 4

## Acuerdo de Confidencialidad Para Personal / Locador de la Subgerencia de Tecnologías de la Información

_____, ____ de _____ de _____
<Nombre de Ciudad> <Día> <Mes> <Año>

Yo, _____, con DNI _____, personal ( ) / locador ( ) de Servicios Postales del Perú S.A. del área de _____ en la sede de _____, suscribo el presente acuse de recibo de credenciales y acuerdo de confidencialidad.

Declaro ser consciente de la importancia de las credenciales, códigos fuentes, recursos informáticos e información que me fue asignada y acepto que las mismas sólo serán utilizadas para los propósitos de mis funciones, en la red y sistemas de Servicios Postales del Perú S.A.

Adicionalmente, entiendo que la publicación, traspaso no autorizado o mal uso de las mismas están sujetos a sanciones definidas por la Subgerencia de Recursos Humanos y, en algunos casos, puede ser un crimen penado por ley.

Debido a ello, durante la vigencia del vínculo laboral o contrato de locación, me comprometo a:

a. No compartir con terceros mis claves de acceso a los recursos institucionales, bajo ningún motivo, puesto que esta clave permite el acceso a datos e información confidencial y privilegiada.
b. No compartir códigos fuentes, recursos informáticos e información que me fue asignada, salvo me encuentre laborando y tenga la aprobación expresa de la Subgerencia de Tecnologías de Información.
c. Comunicar por escrito o correo electrónico a mi jefe inmediato y a la Subgerencia de Tecnología de Información, en caso de detectar el uso no autorizado de los mismos, a fin de que se tomen las medidas correctivas necesarias.

Los compromisos a y b indicados en los párrafos precedentes incluirá un periodo de cinco (5) años posteriores a la finalización del vínculo laboral con SERPOST o término del contrato de locación.

Dejo constancia por escrito a través de este documento, de mi aceptación a los términos y condiciones, aquí expresados.

Colaborador