Serpost
El Correo del Perú

NORMAS

PARA LA ADMINISTRACIÓN DE ACCESOS INFORMÁTICOS, HARDWARE, SOFTWARE Y MEDIDAS DE SEGURIDAD

SD-N-012.00

I. OBJETIVO

Establecer las normas para el otorgamiento y utilización de los accesos a los sistemas informáticos de la Empresa, aplicación de las medidas de seguridad de la información y uso y control de hardware y software.

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

3.1. Decreto Legislativo Nº 685 Ley de Creación de SERPOST S.A.

3.2. Estatuto de SERPOST S.A.

3.3. Resolución de Contraloría N° 320-2006-CG-Normas de Control Interno

3.4. Ley N° 29733 Ley de Protección de Datos Personales

3.5. Norma Técnica Peruana NTP-ISO/IEC 27001:2022 Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de seguridad de la información. Requisitos.

3.6. Lineamientos del Sistema de Gestión de la Seguridad de la Información en SERPOST S.A.

3.7. Normativa interna.

IV. DEFINICIONES

1. **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.
2. **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.
3. **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.
4. **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.
5. **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.
6. **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.

7. **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.
8. **Delitos:** Se puede citar fraudes, falsificación, venta de información.
9. **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.
10. **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.
11. **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.
12. **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.
13. **Red:** El conjunto de computadoras y otros equipos interconectados, que comparten información, recursos y servicios informáticos.
14. **Riesgo:** Proximidad o posibilidad de un daño, peligro, amenaza, contingencia, emergencia, urgencia.
15. **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 1 7799:2007)
16. **Usuario final:** Es la persona que tiene una vinculación con la Empresa y que utiliza los equipos y servicios informáticos ofrecidos por la misma.

V. NORMA

5.1. 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 con 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.

5.1.1. Administración de Accesos de Usuarios

5.1.1.1 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 de aprobación en un plazo no mayor a veinticuatro (24) horas posteriores a la conformidad de la creación de usuario por parte del proveedor del Centro de Datos Corporativo, asimismo, 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; además, 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 podrá solicitar la actualización 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. El Departamento de Administración de Personal, los Administradores Postales 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 con un máximo de las veinticuatro (24) horas siguientes. El Jefe del Departamento de Tecnología y Comunicaciones, a través de la Mesa de Ayuda, coordinará 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.

5.1.1.2 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 provisionales para el inicio de la primera sesión del usuario 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, el compromiso para no compartir la contraseña a los usuarios y un instructivo, previa verificación de la identidad del usuario. El usuario deberá cambiar la contraseña provisional inmediatamente cuando ingresen a su primera sesión, guardando la debida confidencialidad (no compartirla ni divulgarla).

   Asimismo, los usuarios deberán firmar un acuse de lo recibido (según Anexo 1 y/o 2 y Anexo 5), 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.

   En caso algún colaborador olvide su clave de acceso, el Jefe inmediato, salvo excepciones (oficinas unipersonales y personal directivo), solicitará el reemplazo al Departamento de Tecnología y Comunicaciones a través del Equipo de Mesa de Ayuda (sistema de atención de tickets) al correo electrónico mesadeayuda@serpost.com.pe; el colaborador inmediatamente después de recibir su nueva clave de acceso deberá modificarla.

5.1.1.3 Administración de contraseñas críticas:

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

<u>SERVIDORES ADMINISTRADOS POR SERPOST</u>

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 semestralmente, dentro de los primeros cinco (5) días hábiles de cada semestre 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 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 mediante un correo electrónico 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 una copia del correo electrónico con las claves de acceso a los servidores como medida de contingencia y un informe sobre las actividades realizadas respecto al cambio de claves.

b. 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 mediante un correo electrónico 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 semestral, dentro de los primeros cinco (5) días hábiles de cada semestre 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 a través de un correo electrónico, las mantendrá en custodia hasta el próximo cambio y/o para la posterior entrega al personal asignado a esta función.

- Mediante un correo electrónico, se entregará al Jefe del Departamento de Sistemas de Información las claves de acceso a los servidores en ambiente de Desarrollo, para que realice el cambio respectivo en los aplicativos. 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), asimismo, realizará las pruebas respectivas en un ambiente de calidad de software.

- Entregar al Subgerente de Tecnologías de la Información una copia del correo electrónico con las claves de acceso respectivas como medida de contingencia.

b. El Jefe del Departamento de Sistemas de Información deberá entregar las claves de acceso a los aplicativos en el ambiente de Desarrollo al personal a su cargo debiendo firmar dicho personal 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), debiendo comunicar mediante correo electrónico al Subgerente de Tecnologías de la Información respecto a la actualización realizada.

c. El Jefe del Departamento de Tecnología y Comunicaciones, comunicará mediante correo electrónico al Subgerente de Tecnologías de la Información respecto a la actualización de la nueva clave en los aplicativos en ambiente de Producción.

d. De requerirse el acceso de la clave de Producción para otro personal del Departamento de Tecnología y Comunicaciones, el Jefe del Departamento de Tecnología y Comunicaciones deberá solicitar la aprobación a la Subgerencia de Tecnologías de la Información; de ser aprobado, el Jefe del Departamento de Tecnología y Comunicaciones entregará a dicho personal la clave mediante correo electrónico y el documento de acuerdo de confidencialidad para la firma respectiva. (utilizar el Anexo 4).

5.1.1.4 Revisión de Permisos de Acceso a Usuarios

a. El Departamento de Tecnología y Comunicaciones y el Departamento de Sistema de Información, de acuerdo a su

competencia, revisarán los accesos a la red, los sistemas desarrollados por Serpost S.A. y los sistemas externos con una periodicidad de seis (6) meses de acuerdo a la información proporcionada por el Departamento de Administración de Personal, los Administradores Postales y los Jefes de cada área, debiendo coordinar y comunicar a todas las áreas sobre los usuarios activos en el sistema a fin de contar con la relación de usuarios, perfiles y permisos actualizados. Asimismo, las áreas deberán proporcionar la información que les sea solicitada para realizar la depuración de los usuarios que no correspondan en un plazo máximo de diez (10) días calendarios, bajo responsabilidad.

b. Las áreas usuarias que tienen autonomía para administrar los accesos de usuarios a sus aplicaciones (IFS, sistema de Recursos Humanos, Formulación Presupuestal) serán los responsables de los permisos otorgados.

5.1.2. Responsabilidades de los colaboradores:

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 para el cumplimiento de sus funciones.
b. Los colaboradores 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, de acuerdo con lo señalado en la Directiva sobre "Acceso a Internet y uso del Correo Electrónico".
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 colaboradores de la Empresa cuidarán que las contraseñas o claves de acceso se mantengan en estricta confidencialidad, ya que éstos son la principal protección contra el ingreso no autorizado a los servicios de red y sistemas.
e. Todos los colaboradores 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 deberán 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 con 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.

h. Cuando los Gerentes o Subgerentes soliciten la habilitación de los servicios de acceso a la red de datos, internet, correo electrónico o acceso a los sistemas para los trabajos específicos que desarrollarán el personal contratado por Locación de Servicios, tendrán la responsabilidad de verificar el buen uso de los mismos, en caso de incumplimiento deberán comunicar al Departamento de Tecnología y Comunicaciones para la deshabilitación de los servicios.

5.2. Medidas de Seguridad en los Sistemas Informáticos:

a. Los miembros del Equipo de Respuesta a Incidentes de Seguridad Digital de Serpost comunicarán las incidencias de Seguridad y las propuestas de solución a la Subgerencia de Tecnologías de la Información quien como líder del equipo de respuesta ante incidentes de seguridad de SERPOST (CSIRT - **Computer Security Incident Response Team**) coordina las tareas de respuesta entre las partes involucradas en el incidente a fin de determinar el grado de criticidad del incidente.

b. La Subgerencia de Tecnologías de la Información y el equipo CSIRT de SERPOST S.A., comunicará las incidencias de Seguridad y las propuestas de solución al Comité de Gobierno Digital de la Empresa para las acciones correspondientes.

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, asimismo, deberá de hacer de conocimiento del Área de Seguridad.

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 del interior del país, 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 realizar, validar y monitorear, en conjunto con el proveedor, las pruebas de restauración de la información relevante (backup) para la Empresa y almacenarlos en lugares adecuadamente preparados para ese fin.

5.3. Uso y control de hardware y software

La Subgerencia de Tecnologías de la Información a través del Departamento de Tecnología y Comunicaciones:

1. Será la responsable de proporcionar las especificaciones técnicas del hardware, software de Sistema Operativo, antivirus, dispositivos de almacenamiento auxiliar (discos externos, memorias usb, tarjetas de memoria), licencias de software y accesorios informáticos en general a la Subgerencia de Logística, quien tiene a su cargo la adquisición de los mismos.
2. Será responsable de verificar, en coordinación con el responsable del Almacén Central de la Gerencia de Administración de Recursos, que los equipos informáticos adquiridos cumplan con las especificaciones técnicas y garantías solicitadas.
3. Es la única autorizada para retirar del almacén el hardware y software (incluyendo las licencias correspondientes). En los casos que correspondan, dicha Subgerencia solicitará la custodia de los equipos pertinentes en el almacén central.
4. Es la única autorizada para la asignación, distribución y entrega de hardware, así como también de la instalación de software de carácter corporativo, teniendo en consideración que todo el software instalado en cada equipo de computo deberá contar con su respectiva licencia de uso para lo cual coordinará con el Departamento de Control Patrimonial y Seguros Generales para el control respectivo.
5. Es responsable de:
   a) Reparar y repotenciar los equipos de cómputo (*).
   b) Instalar y ampliar las redes de área local (*).
   c) Dar acceso a redes públicas.
   d) Programar periódicamente el mantenimiento preventivo de los equipos de la Empresa a nivel nacional (*).
   e) Instalar y estandarizar el uso de software de oficina a nivel de la Empresa.

   (*) Con apoyo de servicio de terceros, de ser necesario.
6. La custodia física de las licencias de software será responsabilidad de la Gerencia de Administración de Recursos a través de la Subgerencia de Finanzas la cual las almacenará en su bóveda. El Departamento de Tecnología y Comunicaciones, para efectos de control, sólo manejará el cargo de recepción de las licencias depositadas en la bóveda, de corresponder.
7. Es responsable de la seguridad lógica del sistema, estableciendo restricciones de acceso a los archivos y programas para los programadores, analistas u operadores; claves de acceso por usuario y actualización del programa antivirus.
8. Es responsable de la seguridad física de los equipos ubicados en la sala de servidores, previniendo todas las circunstancias que hagan peligrar el funcionamiento del sistema, mediante alarmas, extintores y fuentes de poder suplementarios (UPS).

9. Será responsable del almacenamiento de los datos e información procesada y generada a través de los sistemas informáticos de la Empresa y almacenada en los servidores conectados a la red de la sede central, así como de la realización de los procesos de backup y copias de seguridad respectivas, proceso que se realizará diariamente.
10. Será responsable de realizar el seguimiento para detectar el uso de software no autorizado, debiendo proceder a su eliminación respectiva. Asimismo, verificará que no ocurra movimiento de Hardware no autorizado. En ambos casos informará del hecho, mediante memorando, a las gerencias involucradas.
11. Será responsable del control y seguimiento de las prestaciones accesorias comprometidos por los proveedores en los servicios informáticos contratados a través de la subgerencia de Logistica, así como el de comunicar oportunamente los incumplimientos para la aplicación de penalidades o la elevación a los órganos de control correspondientes.

La Subgerencia de Tecnologías de la Información a través del Departamento de Sistema de Información:

12. Es responsable de la concepción, el análisis y diseño de sistemas de información automatizados, así como del mantenimiento de éstos (actualización de programas) en función a la Norma para el Desarrollo de Aplicaciones, los cuales serán requeridos o propuestos a este Departamento. Las áreas usuarias del sistema son responsables de la administración y actualización de la información procesada en los sistemas implementados como apoyo a su gestión.
13. Toda solicitud de Servicios Informáticos (Sistemas o Soporte Técnico) deberá estar visada por el responsable del área (Gerente, Subgerente o Jefe de Departamento, según corresponda); en el caso de Administraciones Postales, éstas deberán estar visadas por el Administrador Postal respectivo.
14. Tanto el Departamento de Sistemas de Información como el Departamento de Tecnología y Comunicaciones coordinarán e informarán mensualmente a la Subgerencia de Tecnologías de la Información sobre el desarrollo y avances de las actividades propias de cada área.

La Subgerencia de Tecnologías de la Información es responsable de:

15. Elaborar y actualizar el Plan de Contingencia Informático, Plan de Recuperación de Desastres de TIC (DRP), documentos que describen los procedimientos que deben seguir los Departamentos de Sistemas de Información y Tecnología y Comunicaciones para actuar en caso se presente una emergencia que interrumpa el normal funcionamiento de los sistemas e infraestructura informática. La aplicación de estos Planes permite operar de manera aceptable cuando las facilidades de procesamiento de información no estén disponibles.

Los Responsables de cada Centro Gestor:

16. Serán responsables de velar por la correcta utilización de software estándar autorizados por la empresa en los equipos informáticos asignados a sus respectivos ámbitos. En el caso de las Administraciones Postales esta responsabilidad recaerá directamente en el Administrador Postal respectivo.
17. Acatarán las indicaciones efectuadas por la Subgerencia de Tecnologías de la Información para efectuar las pruebas del Plan de Contingencia.

Los Usuarios:

18. Son responsables de efectuar periódicamente el mantenimiento de la data e información que procesan localmente (no en la red), depurando archivos obsoletos y conservando exclusivamente en sus equipos informáticos los archivos con información actualizada, debiendo también velar por mantener las copias de seguridad y backup de dicha información.
19. Es responsabilidad de cada usuario que cuente con el software de correo electrónico instalado en los equipos a su cargo, utilizarlo para comunicaciones relacionadas con la Empresa, dándole un correcto uso al recurso informático y evitando la utilización excesiva de papelería.
20. Las Administraciones Postales en Lima y las de provincias que cuenten con equipo informático deberán utilizar el correo electrónico asignado para enviar reportes e informes puntuales. Toda área que requiera efectuar un traslado o transferencia de equipos informáticos, deberá contar con la autorización del Departamento de Tecnología y Comunicaciones, tanto para la verificación de las condiciones de trabajo necesarias, como para el control administrativo correspondiente, para lo cual el Departamento de Tecnología y Comunicaciones llevará un inventario de los equipos por ubicación física, sin menoscabo de la responsabilidad que le compete al Departamento de Control Patrimonial y Seguros Generales por esta función.

5.1.3. PROCEDIMIENTO

1. SOLICITUD DE SOFTWARE DE DESARROLLO PROPIO

   Será utilizada para los requerimientos de desarrollo de un nuevo sistema, mejoras o modificación en el sistema existente.

   a. PRESENTACIÓN DE LA SOLICITUD

      La solicitud para la automatización de un sistema de información (Software de desarrollo propio) mejoras y modificaciones de los sistemas existentes, se hará a través de la Solicitud de Servicios de Sistemas (Anexo – 1) la misma que deberá estar visada por el responsable del área y dirigida al Subgerente de Tecnologías de la Información en caso de tratarse de la necesidad de desarrollar un nuevo sistema o al Jefe del Departamento de Sistemas de Información en caso de tratarse de mejoras o modificaciones a sistemas en producción, quienes según sea el caso evaluarán la

factibilidad y priorización del requerimiento. Se presentará en original y copia, distribuyéndose de la siguiente forma:

Original : Subgerencia Tecnologías de la Información.
Copia : Área solicitante.

b. ACTA DE COMPROMISO

El Acta de Compromiso es un documento redactado por el Departamento de Sistemas de Información que en coordinación con la Jefatura del área solicitante deberá establecer lo siguiente:

- Etapas en el desarrollo del sistema y tiempos de ejecución por etapa.
- Rol de entrevistas, especificando fecha y hora.
- Relación del personal del Departamento de Sistemas de Información a cargo del Desarrollo del Proyecto y entrevistas.
- Relación del personal designado por el área solicitante para las entrevistas. Las personas seleccionadas deberán estar a cargo de los procesos que se quieren automatizar.

El final de cada etapa implica la firma de aprobación por parte de la Jefatura del Área solicitante.

2. SOLICITUD DE SERVICIOS DE SOPORTE TÉCNICO

a. Los servicios de mantenimiento se canalizarán telefónicamente a través del área de Mesa de Ayuda, que atenderá las solicitudes (Anexo – 2) por orden de llegada y diagnosticará el equipo a reparar.

b. Los servicios de repotenciación de equipos de cómputo, uso de correo electrónico (E-Mail), acceso a redes públicas, se pedirán a través de la Solicitud de Servicios de Soporte Técnico (Anexo – 2) visada por el responsable del área y dirigida al Jefe del Departamento de Tecnología y Comunicaciones la cual será numerada y atendida de acuerdo al orden de llegada. La distribución se hará de la siguiente manera:

Original : Departamento de Tecnología y Comunicaciones.
Copia : Área solicitante.

3. REQUERIMIENTO DE PARTES Y ACCESORIOS

a. En el caso de que la reparación y/o repotenciación de equipos de cómputo implique la adquisición de un repuesto, el Departamento de Tecnología y Comunicaciones emitirá un informe detallando las especificaciones técnicas del bien requerido. La copia de este documento deberá estar adjunto a la Solicitud de Compra / Contratación de Servicios o SOLPE para el trámite correspondiente por el área solicitante.

b. El Departamento de Tecnología y Comunicaciones verificará la compra de bienes y/o contratación de servicios solicitados a terceros de acuerdo con el diagnóstico realizado.

4. MANTENIMIENTO PREVENTIVO DE EQUIPOS

   a. Para los equipos de servicio de la sede central y administraciones postales de Lima, el mantenimiento preventivo estará a cargo de los técnicos del Departamento de Tecnología y Comunicaciones o de un servicio de terceros cuando las circunstancias así lo requieran.

   b. Para los equipos a nivel nacional, la supervisión del servicio de mantenimiento estará bajo la responsabilidad del administrador postal previa coordinación con el Dpto. de Tecnología y Comunicaciones, asimismo otorgará la conformidad del servicio por terceros.

   c. La frecuencia a realizar el mantenimiento dependerá de la ubicación del equipo y del cronograma preestablecido por el Departamento de Tecnología y Comunicaciones.

VI. DISPOSICIONES COMPLEMENTARIAS

1. El presente documento deroga a la Directiva N° 002-G/20 **"Acceso a Sistemas Informáticos y Medidas de Seguridad"**, aprobada con fecha 11 de agosto de 2020 y a la **"Norma y Procedimiento para la Utilización de Software, Hardware y Solicitudes de Servicios Informáticos"**, aprobado con fecha 13 de diciembre de 2013.
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.
5. HISTORIAL DE CAMBIOS

CÓDIGO	NOMBRE	APROBACIÓN
002-G/20	Acceso a Sistemas Informáticos y Medidas de Seguridad	11.08.2020
002-G/16	Acceso a Sistemas Informáticos y Medidas de Seguridad	11.02.2016
004-G/15	Acceso a Sistemas Informáticos y Medidas de Seguridad	24.03.2015
007-G/14	Acceso a Sistemas Informáticos y Medidas de Seguridad	07.11.2014
010-G/10	Acceso a Sistemas Informáticos y Medidas de Seguridad	31.08.2010
SD-NP-003.01	Utilización de software, hardware y solicitudes de servicios informáticos	13.12.2013
SD-NP-003.00	Utilización de software, hardware y solicitudes de servicios informáticos	25.11.2004

VII. AUTORIZACIÓN

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

Lima, 15 DIC. 2023

ALEXANDER INFANTES POMAR
Gerente General
Serpost

ANEXO 1

Formato de Solicitud de Acceso a Sistemas Informáticos (Versión 1.0)

N°		(Llenado por TI)
Fecha	19/10/2023	(dd/mm/aaaa)

1. Datos Generales del Usuario

Cod. del Trabajador		Cargo	
Nombres		Centro de Responsabilidad	Centro de Clasificación Postal de Lima
Apellido Paterno			
Apellido Materno		Descripción del Dpto.	

2. Motivo de la Solicitud

Usuario Nuevo		Cambio de Área		Nuevas Funciones	

Otros (Especificar) _____

3. Servicio de Red

¿Usuario posee cuenta de Red? NO ☐ SI ☐ Colocar Cuenta de Red: _____

	C	E	M
Internet			
Correo Electrónico			
Carpeta de Servidor			
Otros			

C	Creación
E	Eliminación
M	Modificación

4. Consultas / Sugerencias

Jefe/Sub G./Gerente Área:

Firma y Sello del Solicitante

ANEXO 2

Formato de Solicitud de Acceso a Sistemas Informáticos (Versión 1.0)		
N°		(Llenado por TI)
Fecha	19/10/2023	(dd/mm/aaaa)

1. Datos Generales del Usuario			
Cod. del Trabajador		Cargo	
Nombres		Centro de Responsabilidad	Centro de Clasificación Postal de Lima
Apellido Paterno			
Apellido Materno		Descripción del Dpto.	

Glosario	
C	Creación
E	Eliminación
M	Modificación

2. Accesos a 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**
SAP - ERP			
PRJ_ANAQUELADO(CEDSUM)			
PRJ_FACTURACION EMPRESARIAL			
SISTEMA INTEGRADO POSTAL - SIP			

3. Consultas / Sugerencias

Gerente General V°B° Serpost ALEXANDER INFANTES TOMAR

Gerente Legal (e) V°B° Serpost LILIANA SOLDEVILLA NARVAEZ

Gerente de Desarrollo Corporativo V°B° Serpost CARLOS OBERTI CORNEJO

Subgerente de Tecnologías de la Información V°B° Serpost Ing. SHIRLEY MUÑOZ AZNARAN

Jefe del Dpto. Organización y Procesos V°B° Serpost JUAN PABLO FERNANDEZ-MART

Jefe/Sub G./Gerente

Área:

Firma y Sello del Solicitante

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.

ANEXO 5

INSTRUCTIVO: USO DE CUENTA DE RED Y CLAVE ASIGNADA

1. Los usuarios son responsables del cambio de contraseña de su cuenta de acceso a la red de Serpost S.A., la cual deberá realizarse inmediatamente de reciba la misma o en cualquier otro momento que por temas de seguridad considere necesario.
2. Asimismo, el sistema caducara la contraseña de forma automática con una periodicidad de noventa (90) días calendarios a partir del último cambio de contraseña.
3. Las contraseñas deberán tener una cadena mínima de ocho (8) caracteres, la cual deberá contar con letras, números y caracteres especiales por Política de Seguridad de la Información.

Ejemplos:

Claves Incorrectas X	**Claves Correctas** √
- 123456987 - JordanMendoza123	- 4543014Lo- - Cal@894,P♦

4. El cambio de contraseña se realizará dentro de las instalaciones de la empresa, desde la máquina que tiene asignada, presionando Ctrl+Alt+Supr y seleccionando la opción Cambiar Contraseña, en ella colocara la contraseña actual y la nueva contraseña, de acuerdo con lo señalado en el punto 3.
5. Se deberán mantener secretas las contraseñas asignadas y evitar guardarlas en papel, archivos u otros dispositivos por motivos de seguridad de la información.
6. Bajo ningún concepto está permitido compartir cuentas de usuarios con otros trabajadores, bajo responsabilidad.
7. El usuario bloqueara su máquina asignada cuando no se encuentre en su sitio de trabajo presionando Ctrl+Alt+Supr y seleccionando Bloquear Equipo
8. En caso alguno se olvide su clave de acceso, se comunicará con su Jefe inmediato por lo cual este 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, de acuerdo a lo señalado en el punto 1.
9. Información adicional al respecto lo encontrara en la Intranet de la empresa, sección informática – Catálogo de servicios: http://intranet.serpost.com.pe

Dejo constancia de haber recibido y leído el presente Instructivo y me comprometo a aplicarlo en mis labores cotidianas en SERPOST S.A.

Ciudad y Fecha ; / /