DIRECTIVA N° 003 -G/18

PARA : Todo el personal de la Empresa que hace uso de los servicios de Internet, Intranet y correo electrónico

ASUNTO : **ACCESO A INTERNET, INTRANET Y USO DEL CORREO ELECTRÓNICO**

I. OBJETIVO

Establecer las políticas y lineamientos para la adecuada asignación, instalación y utilización de los servicios de acceso a Internet, Intranet y correo electrónico, en aras del mejor aprovechamiento de las plataformas de trabajo instaladas y de los recursos asignados para ello.

II. ALCANCE

El presente documento está dirigido para todos los trabajadores de la empresa con acceso a Internet, Intranet y/o que cuenten con correo electrónico de la empresa.

III. BASE LEGAL

3.1. Estatuto de SERPOST S.A.

3.2. Decreto Legislativo N° 685 Ley de Creación de SERPOST S.A.

3.3. Directiva 001-2008-PCM/SG. Normas y Procedimientos para el uso adecuado de los equipos de cómputo y servicios informáticos en la Presidencia del Consejo de Ministros

3.4. 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.

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

3.6. Reglamento Interno de Trabajo R.I.T.

3.7. Normativa interna.

IV. NORMAS

IV.1 LINEAMIENTOS PARA UTILIZACIÓN DE ACCESOS A INTERNET

1. La Subgerencia de Tecnologías de la Información permitirá el acceso a las páginas Web que cada Gerente o Subgerente indique como necesarias para el desempeño de las funciones de los colaboradores de las áreas que la integran.

2. Toda asignación de acceso a Internet debe ser autorizada por el Gerente o Subgerente de área a los colaboradores, para lo cual deben enviar firmados los formatos establecidos en la Directiva "ACCESO A SISTEMAS INFORMATICOS Y MEDIDAS DE SEGURIDAD" indicando de acuerdo a las funciones que va a desempeñar el colaborador el nivel de Internet a asignar conforme a la siguiente tabla:

Grupos de usuarios	Accesos	Restricciones por Grupo	Restricción General
Usuarios Nivel 1	Acceso sites de gobierno(gob.pe)	Resto de contenidos	No acceso a contenido no productivo (chat, pornografía, terrorismo, apuestas, violencia, juegos, P2P)
Usuarios Nivel 2	Sites web autorizados	No redes sociales	
Usuarios Nivel 3	Streaming y redes sociales	No descarga de archivos	
Usuarios Nivel 4	Acceso completo (descarga de zip y exe)	N/A	

3. Se considera uso indebido del servicio de acceso a Internet cualquier acceso cuyo contenido o finalidad no tenga vinculación con la función u otra actividad que el colaborador desempeñe.

4. Cada colaborador con acceso a Internet será responsable del mal uso que pudiera darle a este servicio, entre ellos almacenamiento en disco de imágenes, programas, música, videos, juegos, otros, que indiquen utilización no permitida o mal intencionada en el acceso a Internet. Los colaboradores con equipo asignado deberán examinar periódicamente el disco duro de sus equipos, a través del software antivirus que para tal efecto haya sido instalado por el personal del Departamento de Tecnología y Comunicaciones, a fin de prevenir la existencia de virus informáticos, especialmente cuando se trabaje archivos descargados de Internet o correo electrónico, siendo de absoluta responsabilidad de los colaboradores con acceso a Internet el realizar actividades inherentes a sus funciones durante el periodo de navegación.

5. No estará permitido:

   a. El empleo de recursos y facilidades de la Red de Información con fines comerciales o lucrativos.
   b. El uso de la Red de Datos en servicios recreativos provistos por sistemas remotos, la instalación y uso de juegos y/o programas recreativos.
   c. Facilitar, prestar, rentar o vender a otra persona su cuenta personal de acceso a la red para la navegación en Internet (usuario y contraseña) para obtener los diferentes servicios de la Empresa.
   d. La instalación de aplicaciones descargadas desde Internet para actividades que no corresponden a sus funciones.
   e. La instalación de aplicativos que permitan la vulnerabilidad de las políticas de acceso a Internet que generen accesos a páginas no autorizadas.
   f. El acceso a Internet con dispositivos móviles que no pertenezcan a la empresa.

6. La administración de la red de datos, no ejerce control sobre el contenido de información que se propague por la red de datos, o de quien la utilice, quedando bajo la responsabilidad del colaborador que la está utilizando. No obstante a lo indicado, la Subgerencia de Tecnologías de la Información podrá poner en funcionamiento herramientas de control que posibiliten analizar y detectar usos indebidos.

IV.2 LINEAMIENTOS PARA UTILIZACIÓN DE ACCESOS A INTRANET

1. El servicio de intranet es una herramienta de uso interno de SERPOST, mediante la cual se facilita la comunicación e interrelación entre el personal, permitiendo la distribución masiva, acceso oportuno y en tiempo real a la información de interés general (Portal Web) y de carácter interno (Intranet).
2. La Subgerencia de Marketing y Filatelia es el órgano encargado de autorizar la publicación y de verificar la actualización de la información en el servicio de la intranet.
3. La Subgerencia de Tecnologías de la Información a través del Departamento de Sistemas de Información es el órgano encargado de brindar el soporte y asistencia técnica para el funcionamiento del servicio de Intranet.
4. El uso de Intranet queda establecido como medio de acceso a la información electrónica de interés para SERPOST y sólo deberá ser utilizado para fines oficiales, bajo responsabilidad de cada usuario.
5. La naturaleza de la información a ser publicada y el proceso de publicación están regulados por el procedimiento del Anexo 1.

IV.3 LINEAMIENTOS PARA LA UTILIZACIÓN DEL CORREO ELECTRÓNICO

1. El correo electrónico o e-mail es un servicio diferenciado, que se brinda a través de Internet y constituye una herramienta que la Empresa pone a disposición de sus colaboradores para facilitar la comunicación, al interior y exterior de la misma.
2. Toda asignación de cuentas de correo electrónico debe ser autorizada por el Gerente o Subgerente de área a los colaboradores, para lo cual deben enviar firmados los formatos establecidos en la Directiva "ACCESO A SISTEMAS INFORMATICOS Y MEDIDAS DE SEGURIDAD" indicando de acuerdo a las funciones que va a desempeñar el colaborador el nivel de correo electrónico a asignar conforme a la siguiente tabla:

Nivel de Acceso a Correo Electrónico	Descripción
Tipo 0	Servicio RPC, OWA y buzón de correo de 8 GB
Tipo 1	Servicio RPC, OWA y buzón de correo de 4 GB
Tipo 2	Servicio OWA y buzón de correo de 2 GB
Tipo 3	Buzón de correo de 1 GB

3. Solo los gerentes, subgerentes y personal autorizado por el gerente de área tendrán acceso para el envío de correos a Listas de Distribución (correos masivos).
4. La Subgerencia de Recursos Humanos hará entrega de la presente Directiva a todos los colaboradores de la Empresa con cargo de recepción, debidamente firmado por el colaborador.

5. Será responsabilidad de cada titular de cuenta de correo efectuar el mantenimiento periódico de la cuenta asignada, para este efecto las rutinas a seguir periódicamente serán las siguientes:
   a. Revisar que el volumen de correo electrónico diario permanezca dentro del límite de su cuota de tamaño asignado.
   b. Borrar mensajes no deseados inmediatamente, debido a que ocupan espacio de almacenamiento innecesariamente.
   c. Mantener en un mínimo los mensajes guardados en su buzón de correo electrónico. Cualquier necesidad de mantener copias de seguridad deberá ser coordinada con el Departamento de Tecnología y Comunicaciones a fin de aplicar el procedimiento para hacer replicaciones en sus equipos asignados.
6. Cada colaborador con acceso al servicio de correo electrónico será responsable del mal uso que pudiera darle a este servicio, entre ellos envío de programas, música, videos, juegos, otros, que indiquen utilización no permitida o mal intencionada en su uso.
7. El tamaño máximo para archivos adjuntos ("attachments") a un correo electrónico será de 20 MB. Cualquier archivo que exceda esta capacidad NO será trasmitido por el sistema el cual emitirá una alerta al respecto.
8. Se suspenderá el servicio de correo electrónico cuando se detecte a usuarios que realicen envíos de mensajes masivos que den como resultado:
   a. La pérdida de trabajo del destinatario o de sus sistemas.
   b. El envío de "Cartas Cadena".
   c. La transmisión de mensajes a listas.
   d. Otros tipos de uso que causen congestión en la red.
9. Deberá tomarse en cuenta la utilización de palabras en mayúscula sólo para destacar un punto importante o distinguir un título o cabecera. El usar palabras en mayúscula que no sean títulos o estén escritas en color "rojo" serán considerado como GRITOS.
10. Los colaboradores serán responsables de la información que emitan a través del correo electrónico de la Empresa, debiendo ser utilizado solamente para realizar actividades inherentes a las funciones asignadas.
11. Los colaboradores deberán bloquear el acceso a su cuenta de correo electrónico cuando no lo estén utilizando, a fin de mantener los niveles de seguridad de la información.
12. Todo requerimiento de información a los centros de responsabilidad deberán ser solicitados a través de las líneas de coordinación y niveles de autoridad establecidos por la Empresa.
13. En caso que el colaborador deje de laborar, el Departamento de Administración de Personal y el Jefe inmediato notificará al Departamento de Tecnología y Comunicaciones, a efecto de que su cuenta de correo sea eliminada de acuerdo a lo establecido en la Directiva "ACCESO A SISTEMAS INFORMATICOS Y MEDIDAS DE SEGURIDAD".

V. DISPOSICIONES COMPLEMENTARIAS

1. El presente documento deroga a la Directiva N° 001-G/16 "**ACCESO A INTERNET Y USO DEL CORREO ELECTRÓNICO**", aprobada con fecha 11 de febrero de 2016
2. Debido al alto nivel de seguridad con el que se debe contar en la Empresa, las claves de acceso al servicio de correo electrónico deberán ser estrictamente confidenciales y personales.
3. La suplantación o el uso no autorizado de la cuenta de otra persona serán considerados como falta grave conforme a Ley.
4. No está permitido el acceso a sitios que distribuyan libremente material obsceno, pornográfico, material subversivo u ofensivo en perjuicio de terceros, así como la redistribución de dicho material a través del correo electrónico o medio similar.
5. Está prohibido intentar apoderarse de claves de acceso de otros usuarios, acceder y/o modificar archivos de otro usuario, decodificar el tráfico de la red o cualquier otro intento de obtención de información de correo confidencial que se transmita a través de la misma.
6. La Empresa aplicará las medidas disciplinarias pertinentes de acuerdo con lo establecido en el Reglamento Interno de Trabajo, cuando el usuario contravenga - por acción u omisión – lo establecido en la presente Directiva.

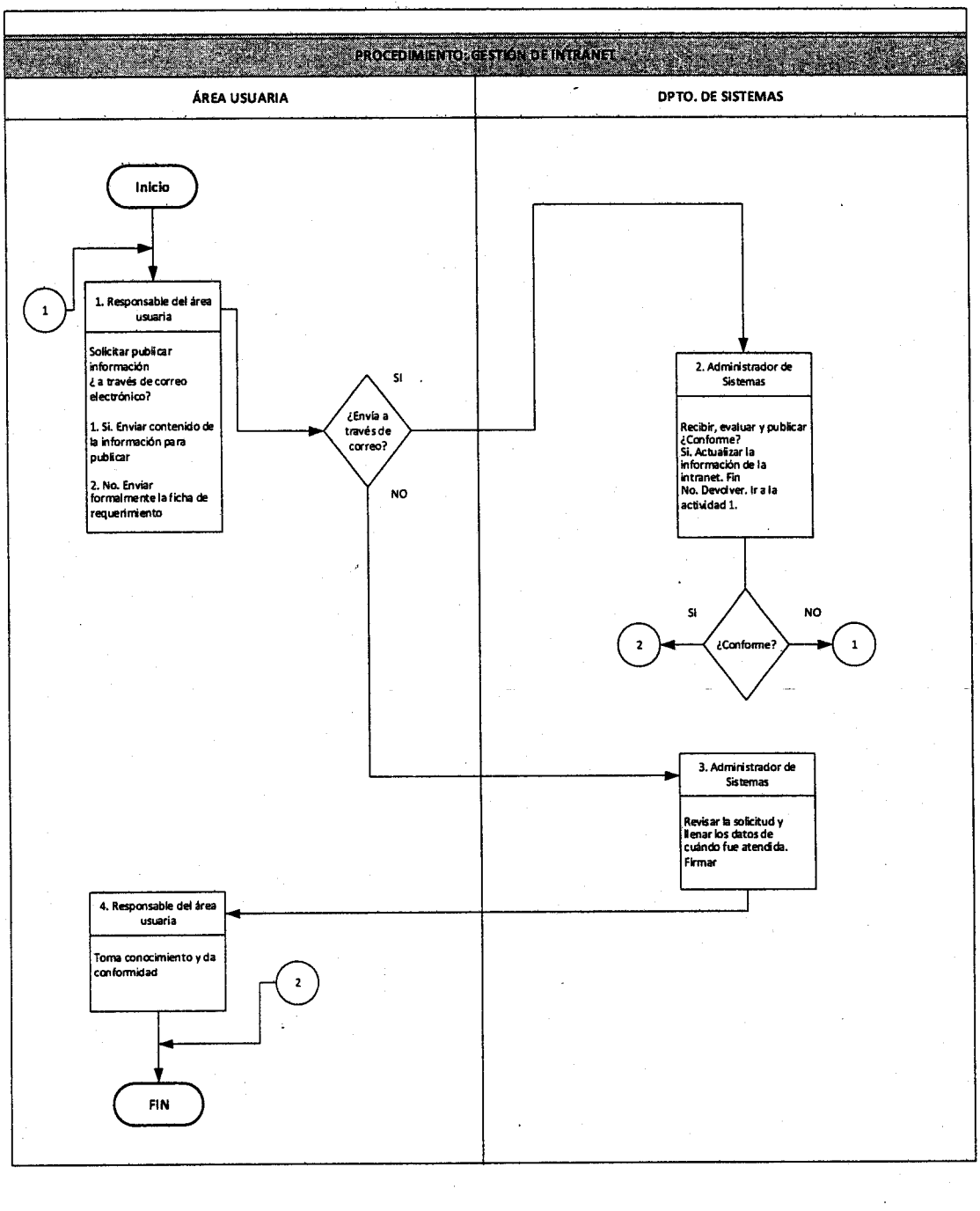
VI. AUTORIZACIÓN

El presente documento queda aprobado por Gerencia General y entrará en vigencia a partir de la fecha de su suscripción.

Lima, 13 FEB. 2018

ENRIQUE CABALLERO ELCORROBARRUTIA
Gerente General (e)
Serpost
El Correo del Perú

ANEXO – 1


PROCEDIMIENTO: GESTIÓN DE INTRANET
ÁREA USUARIA
DPTO. DE SISTEMAS
Inicio
1
1. Responsable del área usuaria
Solicitar publicar información
¿ a través de correo electrónico?
1. Si. Enviar contenido de la información para publicar
2. No. Enviar formalmente la ficha de requerimiento
¿Envía a través de correo?
SI
NO
2. Administrador de Sistemas
Recibir, evaluar y publicar
¿Conforme?
Si. Actualizar la información de la intranet. Fin
No. Devolver. Ir a la actividad 1.
SI
NO
2
¿Conforme?
1
3. Administrador de Sistemas
Revisar la solicitud y llenar los datos de cuándo fue atendida.
Firmar
4. Responsable del área usuaria
Toma conocimiento y da conformidad
2
FIN