Trabajando para ti

Entidad Prestadora de Servicios de Saneamiento TACNA S.A.

RESOLUCION DE GERENCIA GENERAL N°501 -2021-300-EPS TACNA S.A.

TACNA, 24 DIC 2021

VISTO:

El Informe Nro. 171-2021-450-EPS TACNA S.A., Mediante el cual El JEFE DE LA OFICINA DE TECNOLOGIA DE LA INFORMACION hace llegar el Proyecto de Reglamento de Uso de la Red de Datos de la EPS TACNA S.A. para su aprobación.

CONSIDERANDO:

Que el Decreto Legislativo Nº 604 - Ley de Organización y Funciones del Instituto Nacional de Estadística e Informática, tiene por finalidad asegurar, en sus respectivos campos, que sus actividades se desarrollen en forma integrada, coordinada, racionalizada y bajo una normatividad técnica común, contando para ello con autonomía técnica y de gestión.

Que Decreto Supremo Nº 043-2001-PCM - Reglamento de Organización y Funciones del Instituto Nacional de Estadística e Informática, tiene como objetivo lograr que los administradores de los sistemas de información de las Entidades de la Administración Pública, tomen las medidas necesarias para proteger la información publicadas en las páginas web institucionales y en el Portal del Estado Peruano.

Que, con Informe de los vistos, la Oficina de Tecnología de la Información hace llegar el de Proyecto de Reglamento de Uso de la Red de Datos de la EPS TACNA S.A. para el año 2021, por lo que luego de revisarlo es pertinente emitir Resolución;

Que, estando conferidas las facultades al Gerente General de dictar y emitir resoluciones y con VºBº de la Gerencia de Administración y Finanzas, Oficina de Asesoría Legal y la Oficina de Tecnología de la Información;

SE RESUELVE:

ARTÍCULO PRIMERO: Aprobar El Reglamento de Uso de la Red de Datos de la Entidad Prestadora de Servicios de Saneamiento Tacna S.A, el mismo que a folios (14) forma parte integrante de la presente Resolución.

ARTICULO SEGUNDO: Encargar a la Oficina de Tecnología de la Información el cumplimiento de la presente Resolución.

REGISTRESE Y COMUNIQUESE

ING. JUAN ALBERTO SEMINARIO MACHUCA
GERENTE GENERAL
EPS TACNA S.A.

Cc. GAF, OAL, OTI
Archivo

Av. Dos de Mayo N° 372 – Tacna
Telf. (052) 583446 – Fax (052) 583453
Mail: eps.informes@epstacna.com.pe

Trabajando para ti

EPS

Entidad Prestadora de Servicios de Saneamiento TACNA S.A.

OFICINA DE TECNOLOGIA DE LA INFORMACION

REGLAMENTO DE USO DE LA RED DE DATOS

Versión 1.0

2021

REGLAMENTO PARA EL USO DE LA RED DE DATOS EPS TACNA S.A.

Introducción

La Entidad Prestadora de Servicios de Saneamiento EPS Tacna S.A. cuenta con una Red de Datos que permite el eficiente desarrollo de las actividades laborales que involucra la Gerencia General, Gerencia Comercial, Gerencia Administrativa, Gerencias de Operaciones y Gerencia de Ingeniería facilitando el envío, procesamiento y recepción de información. Provee además a los usuarios en la red interna de datos, el acceso a Internet, así como un servicio de correo electrónico. La instalación y el mantenimiento de estos servicios requieren de una cantidad significativa de recursos, y por lo tanto se espera que los usuarios mantengan una conducta responsable cuando las utilicen. El presente documento establece las políticas de uso aceptable de los servicios de la Red de Datos, a las cuales deben ajustarse los usuarios.

La utilización de estos servicios de cómputo conlleva la responsabilidad de aceptar las políticas de uso adecuado que se establecen en el presente documento.

1. Red interna de datos

1.1 Para acceder a la red interna es necesario obtener una clave de usuario y una contraseña. Esta clave debe ser conocida solamente por el usuario y es intransferible. En caso de cualquier olvido la única persona autorizada para proporcionar una nueva clave y/o contraseña es el Administrador de la Red previa autorización de la Jefatura de la Oficina de la Tecnología de la Información. Si el usuario sospecha que algún otro usuario está haciendo uso de su clave debe reportarlo al Administrador de la Red. En ocasiones una clave de usuario y su respectiva contraseña pueden ser compartidas por varios usuarios pertenecientes a un mismo grupo. Es responsabilidad de los miembros de ese grupo no proporcionar su clave y contraseña compartida a ningún otro usuario.

1.2 Ningún usuario deberá permitir el acceso a la red interna de la EPS TACNA a personas externas al mismo o a personal no autorizado, mediante el uso de la cuenta que le ha sido asignada.

1.3 Los servicios de impresión en red deben ser utilizados únicamente para imprimir documentos relacionados con las labores administrativas del usuario.

1.4 Todos los usuarios de los servicios de cómputo deberán responsabilizarse de tener su información debidamente respaldada, y deberán hacer uso de sus unidades de red para este propósito, pero siempre dentro de los límites de espacio en la red.

1.5 Las unidades de red no se deberán utilizar para guardar archivos de música (mp3, wav, wma, etc.), o videos de uso personal (avi, mpg, wmv, mov, etc). Queda estrictamente prohibido tener imágenes o videos pornográficos, o software ajenos a la entidad.

1.6 La información almacenada en las unidades de red se organizará en carpetas. Cada usuario tendrá una carpeta para su uso exclusivo, y los límites de espacio serán fijadas por la OTI de acuerdo al espacio total de almacenamiento disponible en la red de datos. Estas unidades serán respaldadas mensualmente y anualmente.

1.7 Habrá una unidad compartida, que será designada la unidad V:, a la que tendrán acceso todos los usuarios de la red. Esta unidad tiene como propósito facilitar el intercambio de archivos e información entre los mismos usuarios de la red. La información de esta unidad deberá ser eliminada periódicamente, y no será respaldada. Todo archivo que no esté en una carpeta o que sea muy antiguo será borrado automáticamente.

1.8 Debe considerarse que la Unidad donde se crean las carpetas personales o por cada usuario, solo debe contener información de trabajo, dicha información tiene su respaldo correspondiente, a la vez debe precisare que cada Pc esta particionada en dos unidades, la unidad D tiene espacio donde también pueden guardar información. Igualmente queda estrictamente prohibido tener imágenes o videos pornográficos, o software ajenos a la entidad. Se considera información no relevante a los archivos multimedia, software ajenos o información de carácter personal o privado sin relación a las labores que desempeña el usuario.

1.9 Cada Pc debe tener un password de ingreso a la misma, los únicos que pueden saber la clave es el usuario de la Pc, el Administrador de Red y el Jefe de Informática. Los usuarios del equipo fuera del dominio son controlados por el administrador de red y el jefe de informática, estos usuarios son usados netamente para el mantenimiento lógico del PC.

2. Correo electrónico

2.1 Todos los usuarios que deseen tener una cuenta de correo electrónico deberán solicitar a su Jefe Inmediato el cual mediante correo electrónico redactará la solicitud dirigida a la Jefatura de la Oficina de Tecnologías de la Información y este derivara el correo al administrador de red para su creación y configuración de la cuenta del usuario.

2.2 La cuenta de correo electrónico es personal e intransferible su tamaño de buzón consta de 10 Megabytes, la cual debe ser administrada eficientemente. La clave y contraseña para acceder al mismo deberán ser conocidas solamente por el usuario y no deberán ser compartidas con nadie, por lo que si se detecta que el servicio es utilizado por otra persona que no sea el titular se podrá cancelar el servicio.

2.3 El servicio de correo electrónico no deberá ser utilizado para enviar mensajes en forma masiva, o para enviar mensajes ofensivos o de hostigamiento a otras personas. Se prohíbe utilizar la cuenta de correo para enviar o reenviar mensajes que pertenezcan a "cadenas". Queda estrictamente prohibido el uso de las cuentas para fines comerciales.

2.4 El usuario no debe utilizar la cuenta de correo para enviar o recibir archivos ejecutables que comprometan la seguridad del sistema. En caso de que sea necesario enviar o recibir datos adjuntos a un mensaje de correo electrónico el usuario tiene la responsabilidad de comunicar a la Oficina de Tecnología de la Información a fin de analizarlos para detectar la posible presencia de virus informáticos. Cualquier posible infección debe ser reportada de inmediato al Administrador de Red.

2.5 Las Normas para el uso del Correo Electrónico contemplan una base legal o Directiva que en este caso sería aplicable:

DIRECTIVA USO CORREO ELECTRONICO

I. FINALIDAD

Normar los procedimientos de gestión de los servicios de correo electrónico en la EPS Tacna S.A.

II. OBJETIVO

Dar lineamientos para el uso correcto del servicio de correo electrónico oficial.

III. ALCANCE

La presente Directiva es de cumplimiento obligatorio para todos los usuarios que hagan uso del Correo Electrónico en forma interna o con otras Entidades.

IV. BASE LEGAL

- Decreto Legislativo Nº 604 - Ley de Organización y Funciones del Instituto Nacional de Estadística e Informática.
- Decreto Supremo Nº 043-2001-PCM - Reglamento de Organización y Funciones del Instituto Nacional de Estadística e Informática.
- Ley Nº 27444 - Ley del Procedimiento Administrativo General.
- Ley Nº 27269 - Ley de Firmas y Certificados Digitales.
- Decreto Supremo Nº 019-2002-JUS - Reglamento de la Ley de Firmas y Certificados Digitales.

V. DISPOSICIONES GENERALES

5.1. El correo electrónico institucional es una herramienta de comunicación e intercambio de información oficial entre personas, no es una herramienta de difusión indiscriminada de información, con la excepción de las listas de interés establecidas por las instituciones para fines institucionales.

5.2. Cada institución establecerá, de acuerdo a su política institucional, la asignación de cuentas de correo electrónico institucional a parte de, o a todos sus trabajadores.

5.3. La Oficina de Informática (o la que haga sus veces) de cada institución será la responsable de capacitar al personal en el uso del correo electrónico institucional, sobre cómo asignar contraseñas a su correo y sobre las diferencias entre el correo electrónico institucional y el correo electrónico privado.

5.4. El tener una cuenta de correo institucional compromete y obliga a cada usuario a aceptar las normas establecidas por la institución y a someterse a ellas.

5.5. Los usuarios de las cuentas de correo electrónico son responsables de todas las actividades que realizan con sus cuentas de correo electrónico proporcionado por la institución donde laboran. Cualquier usuario que deje su cuenta de correo abierta en un lugar público es responsable de todo aquello que se realice desde dicha cuenta.

5.6. Las cuentas de correo para empleados de las instituciones públicas deben usarse para actividades que estén relacionadas con el cumplimiento de su función en la institución.

5.7. La institución debe garantizar la privacidad de las cuentas de correo electrónico institucional de todos los usuarios. Sólo en el caso de que se detecte que un usuario está cometiendo una falta grave contra lo establecido por la institución por medio de su cuenta de correo, la Oficina de Informática (o quien haga sus veces) podrá tomar las medidas que más le convenga respecto de dicha cuenta de correo. La Oficina de Informática (o quien haga sus veces) establecerá los procedimientos para la detección de faltas graves cometidos por los usuarios mediante correo electrónico.

5.8. El nombre de la cuenta de correo electrónico institucional para cada usuario debe estar formado por la letra inicial del nombre de pila del usuario seguido inmediatamente del apellido paterno, ligado con el símbolo @ al nombre de dominio de la institución (establecido por la Directiva Nº 010-2002-INEI/DTNP "Normas Técnicas para la Asignación de Nombres de Dominio de las entidades de la Administración Pública"). En caso de existir dos construcciones similares, el Administrador de Correo Electrónico en coordinación con las personas involucradas, acordarán el nombre de la cuenta tratando de seguir la regla aquí definida.

VI. DISPOSICIONES ESPECÍFICAS

6.1 DEL BUEN USO DEL CORREO ELECTRÓNICO

6.1.1 Uso de Contraseñas

- Los usuarios que tienen asignada una cuenta de correo electrónico institucional, deben establecer una contraseña para poder utilizar su cuenta de correo, y esta contraseña la deben mantener en secreto para que su cuenta de correo no pueda ser utilizada por otra persona.
- Cuando el usuario deje de usar su estación de trabajo deberá de cerrar el software de correo electrónico, para evitar que otra persona use su cuenta de correo.

6.1.2 Lectura de Correo

- Los usuarios que tienen asignada una cuenta de correo electrónico institucional, deben mantener en línea el software de correo electrónico (si lo tiene disponible todo el día), y activada la opción de avisar cuando llegue un nuevo mensaje, o conectarse al correo electrónico con la mayor frecuencia posible para leer sus mensajes.
- Se debe eliminar permanentemente los mensajes innecesarios.

- Se debe mantener los mensajes que se desea conservar, agrupándolos por temas en carpetas personales.
- Al recibir un mensaje que se considere ofensivo, se debe reenviar el mensaje hacia el Administrador de Correo Electrónico de la institución, con el fin de que se pueda tomar las acciones respectivas.

6.1.3 Envío de Correo

- Utilizar siempre el campo "asunto" a fin de resumir el tema del mensaje.
- Expresar las ideas completas, con las palabras y signos de puntuación adecuados en el cuerpo del mensaje.
- Enviar mensajes bien formateados y evitar el uso generalizado de letras mayúsculas.
- No utilizar tabuladores, ya que existen softwares administradores de correo que no reconocen este tipo de caracteres, lo que puede introducir caracteres no válidos en el mensaje a recibirse.
- Evite usar las opciones de confirmación de entrega y lectura, a menos que sea un mensaje muy importante, ya que la mayoría de las veces esto provoca demasiado tráfico en la red.
- Evite enviar mensajes a personas que no conoce, a menos que sea por un asunto oficial que los involucre.
- Evite enviar mensajes a listas globales, a menos que sea un asunto oficial que involucre a toda la institución.
- Antes de enviar el mensaje revisar el texto que lo compone y los destinatarios, con el fin de corregir posibles errores de ortografía, forma o fondo.

6.1.4 Reenvío de Mensajes

- Para el reenvío de un mensaje, incluir el mensaje original, para que el destinatario conozca el contexto en que se está dando el mensaje que recibe. No incluir ningún archivo adjunto que se pueda haber recibido originalmente, a no ser que se haya realizado modificaciones al(los) archivo(s).

6.1.5 Autofirmas.

- La firma debe ser breve e informativa, no debiendo ocupar más de tres líneas.
- No incluir la dirección de correo en la firma, porque ésta ya fue incluida de manera automática en la parte superior del mensaje.

6.1.6 Tamaño de los mensajes

- La Oficina de Tecnologia de la Información determinará el tamaño máximo que deben tener los mensajes del correo electrónico institucional.

6.1.7 Vigencia de los mensajes

- Los mensajes tendrán una vigencia no mayor de 30 días desde la fecha de entrega o recepción de los mismos, o de acuerdo a la política establecida por la Oficina de Informática (o la que haga sus veces) de cada institución. Superada la fecha de vigencia, los mensajes deberán ser eliminados del servidor de correo.
- Si se desea mantener un mensaje en forma permanente, éste debe almacenarse en carpetas personales.

6.1.8 Listas de Correos

- Al enviar un mensaje a una lista o grupo de usuarios, revisar que el mensaje sea enviado a los usuarios correctos.
- Evitar en lo posible enviar mensajes con archivos adjuntos a grupos de usuarios.
- Evitar suscribirse por Internet a listas ajenas a la función institucional, para evitar saturación en la recepción de mensajes.

6.1.9 Uso del Correo Institucional desde fuera del local de la Institución

- La Oficina de Informática (o la que haga sus veces) de cada institución mediante una directiva establecerá las políticas de uso del correo institucional desde fuera del local de la institución, de acuerdo a los métodos de trabajo establecidos por la institución.

6.2 DEL MAL USO DEL CORREO ELECTRÓNICO

6.2.1 Se considera falta grave facilitar u ofrecer la cuenta y/o buzón del correo electrónico institucional a terceras personas. Los usuarios deben conocer la diferencia de utilizar cuentas de correo electrónico institucionales y cuentas privadas ofrecidas por otros proveedores de servicios en Internet.

6.2.2 Se considera como mal uso del correo electrónico institucional las siguientes actividades:

- Utilizar el correo electrónico institucional para cualquier propósito comercial o financiero ajeno a la institución.
- Participar en la propagación de mensajes encadenados o participar en esquemas piramidales o similares.
- Distribuir mensajes con contenidos impropios y/o lesivos a la moral.
- Falsificar las cuentas de correo electrónico.
- Utilizar el correo electrónico institucional para recoger los mensajes de correos de otro proveedor de Intemet.

6.2.3 Se penalizará con la cancelación de la cuenta de correo, el envío de mensajes a foros de discusión (listas de distribución y/o newsgroups) que comprometan la información de la

institución o violen las leyes del Estado Peruano, sin perjuicio de poder ser sujeto de otras sanciones y/o penalidades derivadas de tal actividad.

6.2.4 Se considera, adicionalmente, malas prácticas en el uso de correo electrónico:

6.2.4.1 Difusión de contenido inadecuado.

- Son considerados contenidos inadecuados todo lo que constituya complicidad con hechos delictivos, por ejemplo: apología del terrorismo, uso y/o distribución de programas piratas, todo tipo de pornografía, amenazas, estafas, esquemas de enriquecimiento piramidal, virus o código hostil en general.
- Contenido fuera de contexto en un foro temático.

6.2.4.2 Difusión a través de canales no autorizados.

- Uso no autorizado del servidor de correo institucional para enviar correo personal. Aunque el mensaje en sí sea legítimo, se están utilizando los recursos de la institución sin consentimiento de directiva interna que la autorice.

6.2.4.3 Difusión masiva no autorizada

- Enviar de forma masiva publicidad o cualquier otro tipo de correo no solicitado, "spam".

6.2.4.4 Ataques con objeto de imposibilitar o dificultar el servicio, "mail bombing".

- Dirigir a un usuario o al propio sistema de correo electrónico, mensajes que tengan el objetivo de paralizar el servicio por saturación de las líneas, de la capacidad del servidor de correo, o del espacio en disco del usuario.
- Suscripción indiscriminada a listas de correo. Es una versión de "mail bombing", en que los ataques no vienen de una sola dirección, sino de varias, los cuales son mucho más difíciles de controlar.

6.3 DE LA SEGURIDAD DEL CORREO ELECTRÓNICO

6.3.1 Las instituciones públicas deben contar con políticas de seguridad para el uso de correo electrónico, las que serán establecidas por la Oficina de Informática (o la que haga sus veces) de cada institución.

6.3.2 Uso del Antivirus

- Los antivirus de la institución, para servidores y estaciones de trabajo, deben activarse de tal forma que se verifiquen todos los archivos, aún los que se encuentren compactados, y la acción por defecto a seguir será la de eliminar el virus automáticamente.
- Los servidores de correo deben contar con antivirus para correo. Si el mensaje que detecta contiene un virus o "troyano" - "caballo de troya" que no puede ser

removido, debe eliminarse el mensaje inmediatamente. Así mismo se deberá informar, al destinatario de correo, el nombre del remitente y que su mensaje fue borrado por contener virus.

- Revisar en forma constante la computadora para evitar remitir virus al momento de enviar documentos adjuntos. En tal sentido, se responsabilizará a los usuarios por los archivos adjuntos que envíen.
- La Oficina de Informática (o la que haga sus veces) de cada institución se encargará de verificar la presencia de virus en el servidor de correo.

6.4 DE LA VALIDEZ OFICIAL DEL CORREO ELECTRÓNICO

6.4.1 La institución podrá establecer, mediante una directiva interna, la validez oficial de los mensajes que se transmitan entre sus trabajadores, así como la validez en el intercambio de información entre otras instituciones públicas y los ciudadanos.

6.4.2 Para el intercambio de información entre instituciones públicas, se deberá propender a la utilización del correo electrónico seguro, para lo que se podrá utilizar la firma y certificados digitales u otro medio de seguridad y verificación

6.4.3 Los mensajes de correo electrónico y sus archivos adjuntos, tendrán validez legal si están firmados digitalmente, bajo el marco de la Ley Nº27269, "Ley de Firmas y Certificados Digitales" y de su Reglamento aprobado mediante Decreto Supremo Nº 019-2002-JUS.

VII. DISPOSICIONES COMPLEMENTARIAS

7.1 Las notificaciones institucionales pueden efectuarse mediante correo electrónico conforme el numeral 20.1.2 de la Ley Nº 27444, Ley del Procedimiento Administrativo General.

7.2 Los correos electrónicos que adjunten documentos que no son propios del remitente, deberán citar siempre la fuente de origen y/o los autores, a fin de respetar los derechos de propiedad intelectual.

7.3 Si se recibe algo cuestionable o ilegal, comunicar a la Oficina de Informática (o la que haga sus veces) de la institución para que se tome las acciones del caso.

7.4 Toda institución pública que disponga de correo electrónico deberá asignar la función de administración del correo electrónico a su Oficina de Informática (o la que haga sus veces).

7.5 La Oficina de Recursos Humanos de cada institución debe comunicar a la Oficina de Informática (o la que haga sus veces) la relación de trabajadores que hayan ingresado a laborar y de los que han dejado de hacerlo, para la activación o desactivación de las cuentas de correo respectivas.

7.6 La Oficina de Informática (o la que haga sus veces) de cada institución es la responsable de que el personal de la institución cumpla con lo dispuesto en la presente directiva y podrá elaborar un código de ética adicional a esta directiva.

3. Acceso a Internet

3.1 El acceso a Internet debe ser utilizado fundamentalmente para visitar sitios relacionados con la actividad laboral.

3.2 El acceso a Internet contará con restricciones para sitios inseguros, y será particularmente importante que los usuarios tengan un comportamiento responsable en aquellos sitios que no queden restringidos, ya que un uso inadecuado puede comprometer seriamente la seguridad de la Información de la Red de la EPS Tacna S.A., así como afectar el trabajo de otros usuarios.

3.3 Queda prohibido terminantemente:

- El uso de programas para "bajar" o copiar de Internet archivos de procedencia no segura o ilegal, tales como aquellos que aparecen en el anexo 1.
- Instalar y ejecutar programas que permitan el intercambio de archivos (anexo 2).
- Utilizar los recursos de cómputo junto con el internet para actividades no administrativas o de trabajo, como pláticas en línea o "chat" y la reproducción de radios o tv en línea.
- Instalar programas gratuitos del Internet, tales como salvapantallas, pues estos frecuentemente instalan programas indeseables como espías.
- La instalación de servidores Web o páginas Web en las computadoras de la Entidad, a excepción de aquellas que pertenecen al portal de la EPS Tacna S.A.
- Queda prohibido además utilizar los servicios cómputo de la entidad para realizar actividades comerciales ajenas a la EPS Tacna S.A.

3.4 Todos los equipos de cómputo de la Entidad deberán acceder a Internet a través del Firewall para seguridad del sistema de red. Cada PC tiene un perfil de acceso a internet (anexo 3) de acuerdo al usuario y puede ser modificado por el Administrador de red si no es usado correctamente.

3.5 Toda máquina a la que se detecte algún incidente de seguridad podrá ser desconectada físicamente de la red en tanto se corrija el problema, y deberá ser nuevamente autorizada por la Oficina de Tecnología de la Información para poder operar con acceso a Internet.

3.6 La Oficina de Tecnología de Información deberá configurar y certificar los equipos para que se puedan conectar a la red. Todo equipo que se vaya a conectar deberá contar con antivirus y con las actualizaciones al sistema operativo que permitan asegurar que no existan vulnerabilidades que pongan en riesgo la integridad y seguridad de la red de la entidad.

3.7 Queda estrictamente prohibido cambiar el IP asignado o usar un IP que no haya sido asignado por la Oficina de Tecnología de la Información. También está prohibido configurar equipos y conectarlos a la red sin que hayan sido revisados y certificados por la Oficina de Tecnología de la Información. Lo anterior incluye la prohibición de instalar y configurar concentradores. En caso de existir la necesidad de instalar puntos de acceso a la red, se deberá remitir una solicitud por escrito a la Oficina de Tecnología de la Información, para que personal correspondiente lleve a cabo las acciones necesarias para garantizar la seguridad de la red.

3.8 Las máquinas que estén dispersando virus deberán ser desconectadas de la red hasta que se resuelva el problema y los virus sean eliminados. Los usuarios que detecten virus en sus equipos deberán apagarlos y dar aviso a la Oficina de Tecnología de la Información, que deberá darle máxima prioridad a la solución de este tipo de problemas.

3.9 Todos los perfiles de acceso (Anexo 2) tienen control de antivirus, antispam y filtros de acceso a paginas no productivas. Los Gerentes, Jefes de Oficina y Jefes de División, están en el perfil más alto y tienen acceso a internet con varios privilegios. Si algún usuario que no pertenezca a este grupo necesitara este tipo de acceso. Se deberá solicitar a su superior para que este justifique su uso y comunique al Jefe de Oficina de Tecnología de la Información para generar su acceso.

3.10 Cualquier excepción a los puntos anteriores puede ser válida siempre y cuando se proporcione una clara justificación y autorización, excepto los puntos de prohibición estricta que no deberán ser transgredidos por ningún motivo.

4. Monitoreo

4.1 La Oficina de Tecnología de la Información se reserva el derecho de monitorear el uso de los servicios con el fin de detectar el posible mal uso de los mismos. Durante el monitoreo se tomarán todas las medidas necesarias para garantizar la privacidad del usuario. Por ningún motivo se examinará el contenido de comunicaciones individuales de correo electrónico.

4.2 En caso de sospechas de abuso por parte de algún usuario se le pedirá una explicación sobre la actividad detectada, lo cual se hará en estricta confidencialidad.

4.3 En caso de abusos reiterados de los servicios informáticos por parte de algún usuario se podrá negar al mismo el uso de dichos servicios de cómputo, por decisión de la Jefatura de la Oficina de Tecnología de la Información.

5. Servicios de Computo

5.1 Toda solicitud de servicios o requerimientos en materia de cómputo o informático, deberá hacerse a través de un correo electrónico, el cual deberá contener la firma digital y enviada por la Jefatura del área correspondiente. Las cuestiones muy urgentes podrán ser atendidas mediante una llamada telefónica o una visita del interesado a la Oficina de Tecnología de la Información.

5.2 La Oficina de Tecnología de la Información canalizara órdenes de servicio a proveedores externos siempre que lo considere conveniente, pero en todos los casos deberá revisar primero el equipo de cómputo para evaluar la necesidad de enviarlo a un servicio externo. El usuario no puede decidir enviar el equipo a reparación directamente ya que deberá requerirlo a la Oficina de Tecnología de la Información.

5.3 Cada usuario es responsable de los programas que se instalen en el equipo de cómputo asignado. La Oficina de Tecnología de la Información solamente instalará programas de procedencia legal que cuenten con la licencia respectiva.

5.4 La Oficina de Tecnología de la Información se reserva el derecho de desconectar equipos de la red por mal uso de la computadora: equipo con programas inseguros de música o video, programas de Internet espías, programas de descarga de música, entrada repetitiva de virus a través de correo externo no filtrado, entre otros motivo de desconexión.

Anexo 1.

Lista de extensiones de archivos no permitidas para actividades administrativas en la entidad:

ASF --> Windows Media
AVI--> BSPlayer
MOVIE --> (mov)
MP2V --> (mpeg)
MP3 --> Música comprimida
MP4 --> (MPEG-4)
MPA --> (mpeg)
MPE --> (mpeg)
MPEG --> (mpeg)
MPG --> (mpeg)
MPV2 --> (mpeg)
QT --> QuickTime
QTL --> QuickTime
RPM --> RealPlayer
SMK --> RAD Video Tools
VIV --> Video VIV
WAV --> Música digital
WM --> Windows Media
WMA --> Música comprimida para Windows Media
WMV --> Windows Media
WOB --> PowerDVD

Anexo 2.

Lista de Programas para Intercambio de Música prohibidos

3ECS
Adult Media Swapper
AppleJuice
Ares
Atomwire
AudioGalaxy
AudioGalaxy Satelite
AudioGnome
BadBlue
Bearshare
BlackWindow
Blipster Fast Find
BlubsterBoDeTella
BuddyShare
CatNap
Dagsta
DC++
DC:Pro
DietKazaa
DirectConnectDBNapster
Dopeflish Satellite
Earth Station
eDonkey Client
eDonkey Server Spy
eDonkeyboot Lite
eDonkey
ELF
eMule pHoeniX
eMule Plus
eMule
Evolution
Exware
ExoSee
FANtastic PLayer
File Freedom
Filemaze
FIlenavigator
FIlerouge
FIleShare Client
FIleSpree
Filetopia
Filetopia
FolderShare
Freewire
FTP++P2P
Gnutella
Gnotella
Gnucleus

Groskter	NapiMX	RighteousMP3
iMesh	Napshack	Shareaza
Inoize	Napster	ShareSniffer
intelliMP3	Natural Born Chatter	SideKick
Jungle Monkey	Neo Modus Direct Connect	SlavaNap
Kast	Neo Napster	Smirck
Kazaa Lite	Netbrilliant	SongSpy XE
Kazaa Kontrol Leech Killer	NetMess	SoulSeek
Kazaa Lite Advanced	Newtella	SpookShare
Kaza Lite Cracked	NTella	Swapnut
Kazaa Cracked K++	Nudester	Swaptor
Kaza Media Desktop	Nuzzly	Taxee
Kazearch	OHAHA	The Circle
Kceasy	OMNI	The PornTrader
Limewire	OpenCola	The Qube
Limewire Sparky	OpenNap	ToadNode
Locutus	Overnet	TrustyFiles
IPhant	PeerGenius	URLBlaze
Madster	Phex	Varvar
MediaSeek	Phosphor	VexTV
Mercora	Piolet	Wanafile
Mnet	Plebio	Wannafree
Mojonation	PornDigger	WinMX
Morpheus	Private Peer to Peer	Wippit
MP3Mystic	QtraxMax	WWW Filre Share Pro
MXlinx	QueerPeer	Xolox
MyNapster	Rapigator	Yaga Share
Myster R8	Razius Express	Yoink
NapAmp	Renapster	Zalzah
Napigator	RiffShare	

Anexo 3.

ID	PERFIL	DESCRIPCIÓN
1	Acceso Autorizado	Acceso total a todo tipo de páginas
2	Acceso Institucional	Acceso a todo tipo de páginas de índole laboral excepto páginas de redes sociales, chat, correo y entrenamiento. Acceso a GoogleEarth
3	Acceso Comunicación Social	Acceso a Redes Sociales con el fin de Administrar los canales virtuales de Facebook y Whatsapp de la entidad
4	Acceso Operador Central Telefónica	Acceso WhatsApp Web del Numero Celular de la Central Emergencias.

Trabajando para ti

Entidad Prestadora de Servicios de Saneamiento TACNA S.A.

EPS TACNA S.A.
GERENCIA GENERAL
24 DIC 2021
Registro: 58886
Hora: Firma:

INFORME Nº 171-2021-450-EPS TACNA S.A

A : ING. JUAN ALBERTO SEMINARIO MACHUCA
GERENTE GENERAL

ASUNTO : APROBACION REGLAMENTO RED DE DATOS

FECHA : Tacna, 24 de Diciembre del 2021

Es grato dirigirme a Ud, para saludarlo cordialmente, y remitir a su despacho el Proyecto de Reglamento de Uso de la Red de Datos, ha sido elaborado en base a:

- Decreto Legislativo Nº 604 - Ley de Organización y Funciones del Instituto Nacional de Estadística e Informática.
- Decreto Supremo Nº 043-2001-PCM - Reglamento de Organización y Funciones del Instituto Nacional de Estadística e Informática.

El mismo que debe ser aprobado con Resolución de Gerencia General, con el fin de poner en conocimiento de todo el usuario dicho reglamento a través de nuestra página web, se adjunta Proyecto de Resolución.

Atentamente,

EPS TACNA S.A.
Ing. EDUARDO S. CHOQUE CHACOLLA
CIP 101550
Jefe Ofic. Tecnología de la Información

Se Adjunta:
1. Reglamento Red de Datos
2. Proyecto de Resolución

c.c. Archivo

E.P.S. TACNA S.A.
Gerencia General
Proveído Nº ..... Fecha: 24 DIC 2021
Dirigido a: SEGC
Asunto: Para su Trámite
Firma
Entidad Prestadora de Servicios de Saneamiento EPS TACNA S.A. GERENCIA GENERAL Tacna S.A.

Av. Dos de Mayo N° 372 – Tacna
Telf. (052) 583446 – Fax (052) 583453
Mail: eps.informes@epstacna.com.pe