



TRIBUNAL CONSTITUCIONAL

N° 21 -2016-DIGA/TC

Lima, 31 de marzo de 2016

**VISTOS**

El Informe N.º 079-2015-OTI/TC, N.º 018-2016-OTI/TC y N.º 034-2016-OTI/TC, de la Oficina de Tecnologías de la Información, del 14 de diciembre de 2015 y 15 de febrero y 17 de marzo de 2016 de 16 de febrero de 2016, respectivamente; los Informes N.º 003-2016-OPD/2016 de 19 de enero de 2016 y N.º 005-2016-OPD/TC de 16 de febrero de 2016, expedidos por la Oficina de Planeamiento y Desarrollo, y los proveídos de la Dirección General de Administración, de fecha 8 de enero, 16 de febrero y 21 marzo de 2016; y,

**CONSIDERANDO**

Que, la Oficina de Tecnologías de la Información ha presentado los proyectos de Directiva sobre “Normas para el Uso del Correo Electrónico en el Tribunal Constitucional” y “Normas que regulan el uso de las tecnologías de la Información y Comunicaciones en el Tribunal Constitucional”;

Que, la directiva “Normas para el Uso del Correo Electrónico en el Tribunal Constitucional” tiene por finalidad normar los procedimientos para una gestión eficiente de los servicios de correo electrónico en el Tribunal Constitucional;

Que, por su parte, las “Normas que regulan el uso de las tecnologías de la Información y Comunicaciones en el Tribunal Constitucional”, pretenden normar el uso de las tecnologías de Información y Comunicaciones (TIC) en el Tribunal Constitucional;

Que, asimismo, ha preparado la “Política de utilización del Sistema de Video Vigilancia”, la misma que tiene el objetivo de garantizar la protección y seguridad de su personal, visitantes, edificaciones, bienes materiales e información;

Que, los referidos proyectos, ha merecido la conformidad de ésta Dirección General de Administración;

En uso de las facultades conferidas por el Reglamento de Organización y Funciones.

**SE RESUELVE**

**ARTÍCULO PRIMERO.-** Aprobar las siguientes Directivas:

- Directiva N.º 001-2016-DIGA/TC “Normas para el Uso del Correo Electrónico en el Tribunal Constitucional”; y,
- Directiva N.º 002-2016-DIGA/TC “Normas que regulan el uso de las tecnologías de la Información y Comunicaciones en el Tribunal Constitucional”.

El texto de las directivas, forman parte integrante de la presente resolución como anexos 01 y 02.

**ARTÍCULO SEGUNDO.-** Déjese sin efecto la Directiva N.º 002-2005 “Normas para el Uso del Servicio del Correo Electrónico en el TC”, aprobada mediante Resolución Administrativa N° 016-2005-P/TC.

**ARTÍCULO TERCERO.-** Aprobar la “Política de utilización del Sistema de Video Vigilancia”, que como anexo 03 forma parte de la presente resolución.





TRIBUNAL CONSTITUCIONAL

Nº 21 -2016-DIGA/TC

Lima, 31 de marzo de 2016

**ARTÍCULO CUARTO.-** Comunicar la presente resolución a la Secretaría General, a las Oficinas de Gestión y Desarrollo Humano, Tecnologías de la Información, Planeamiento y Desarrollo, y al Órgano de Control Institucional, para su conocimiento y fines de ley.

**ARTÍCULO QUINTO.-** Encargar a la Jefatura de la Oficina de Tecnologías de la Información, el cumplimiento y difusión de las directivas y la política aprobadas por la presente.

Regístrese y comuníquese.



*JLP*  
.....  
JOSÉ LUIS ZAVALETA PINEDO  
Director General de Administración  
TRIBUNAL CONSTITUCIONAL.



**DIRECTIVA N° 001-2016-DIGA/TC**  
**NORMAS PARA EL USO DEL SERVICIO DE CORREO ELECTRÓNICO EN**  
**EL TRIBUNAL CONSTITUCIONAL**

**I. FINALIDAD**

Normar los procedimientos para una gestión eficiente de los servicios de correo electrónico en el Tribunal Constitucional.

**II. OBJETIVOS**

Establecer los lineamientos para el uso correcto del servicio de correo electrónico.

**III. ALCANCE**

La presente Directiva es de cumplimiento obligatorio a todo el personal jurisdiccional y administrativo del Tribunal Constitucional que haga uso del correo electrónico, independientemente del contrato laboral suscrito.

**IV. BASE LEGAL**

- 4.1. Ley N° 27444, Ley del Procedimiento Administrativo General.
- 4.2. Ley N° 27269, Ley de Firmas y Certificados Digitales.
- 4.3. Decreto Supremo N° 052-2008-PCM, que aprueba el Reglamento de Firmas y Certificados Digitales.
- 4.4. Directiva N° 005-2003-INEI/DTNP, Normas para el uso del servicio de correo electrónico en las entidades públicas del país.

**V. DISPOSICIONES GENERALES**

- 5.1. El correo electrónico institucional es el medio de comunicación válido para difusión de información de carácter institucional, no siendo una herramienta de difusión indiscriminada de información, con la excepción de las listas de interés establecidas por las instituciones del estado para fines institucionales.
- 5.2. La Oficina de Tecnologías de la Información es responsable de la administración y asignación de las cuentas del servicio de correo electrónico institucional, de acuerdo a la política de la entidad, ésta determinará la asignación de cuentas de correo electrónico institucional a parte de, o a la totalidad de los trabajadores de la institución, con autorización previa de la Oficina de Administración de Personal, quien se encarga de realizar el trámite de alta y bajas de personal o, de la Secretaría General.

- 5.3. La Oficina de Tecnologías de la Información 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 personal proveído por terceros.
- 5.4. El tener una cuenta de correo institucional compromete y obliga a cada usuario a aceptar las normas establecidas en la presente Directiva y a someterse a ellas.
- 5.5. Los usuarios de las cuentas de correo electrónico institucional son responsables de todas las actividades y de los contenidos que realizan con sus cuentas de correo electrónico. Cualquier usuario que deje su cuenta de correo abierta en un lugar público o ambiente compartido, es responsable de todo aquello que se realice desde dicha cuenta.
- 5.6. Las cuentas de correo asignadas deben utilizarse para actividades que estén relacionadas con el cumplimiento de su función en la institución, siendo su asignación para fines estrictamente laborales, constituyéndose en responsables de todas las actividades que realicen con su cuenta de correo electrónico.
- 5.7. Teniendo en consideración que los bienes y servicios informáticos utilizados para la comunicación de correo son de propiedad de la institución, es importante precisar que toda información generada, almacenada o transmitida haciendo uso de éste medio (correo electrónico institucional) son de interés del Tribunal Constitucional.
- 5.8. La Oficina de Tecnologías de la Información establece los procedimientos para la detección de faltas cometidas por los usuarios a través de sus cuentas de correo electrónico. En caso se detectase que el usuario por medio de su cuenta de correo atente contra lo establecido en la presente Directiva, la Oficina de Tecnologías, dependiendo de la naturaleza de la falta, adoptará las siguientes medidas, no necesariamente en el orden siguiente:
  - a) Notificación de la falta cometida al usuario infractor mediante correo electrónico y telefónicamente.
  - b) Notificación de la falta mediante correo electrónico y telefónicamente, con envío de la copia del correo de notificación a su jefe inmediato superior.
  - c) Comunicación al infractor, al jefe inmediato superior y a la Oficina de Administración de Personal para el inicio del procedimiento administrativo sancionador, si así lo estime conveniente, de acuerdo a lo contemplado en la normatividad vigente y el Reglamento Interno de Trabajo. De ser el caso, se imponga una sanción que incluya procedimientos de carácter técnico y que impliquen la intervención

de la OTI, esta deberá ser comunicada a dicha oficina para su materialización.

- 5.9. La denominación de la cuenta de correo electrónico institucional para cada usuario debe estar formada por la letra inicial del primer nombre del usuario seguido inmediatamente del apellido paterno, ligado con el símbolo @ al nombre de dominio de la institución (tc.gob.pe). En caso de existir dos construcciones similares, el administrador de correo electrónico en coordinación con el usuario involucrado, acordarán el nombre de la cuenta tratando de regirse a la estructura definida.

## **VI. DISPOSICIONES ESPECÍFICAS**

### **6.1. DEL BUEN USO DEL CORREO ELECTRÓNICO**

#### **6.1.1. Uso de Contraseñas**

- Las cuentas de correo electrónico serán personales e intransferibles, por lo que únicamente pueden ser usadas por las personas propietarias de las mismas, siendo estas responsables directas de la confidencialidad de la contraseña correspondiente.
- El usuario poseedor de una cuenta de correo electrónico institucional está en la obligación de mantener en reserva la contraseña de correo respectiva, no debiendo compartirla con alguna otra persona sea interna o externa a la institución.
- Cuando por ausencia temporal el usuario deje de usar su estación de trabajo, deberá habilitar el bloqueo de su equipo de cómputo a fin de evitar que otra persona haga uso indebido de su cuenta de correo.

#### **6.1.2. Lectura de Correo**

- Los usuarios que tengan asignada una cuenta de correo electrónico institucional, deberán leer con la debida frecuencia sus mensajes de correo. Se le recomienda al usuario mantener activada la opción de notificación automática de correo que le alertará en caso de nuevos correos que ingresen a su bandeja de entrada.
- El tamaño de los buzones de las cuentas de correo dependerá del tipo de cuenta asignada: IMAP o POP3. En el caso del tipo POP3, el tamaño de la cuota de correo será de 50 MB debido a que los mensajes leídos por el usuario serán descargados al cliente de correo instalado en su computador.

En el caso del tipo IMAP el tamaño de la cuota será de 2 GB sujeto a evaluación previa de la Oficina de Tecnologías de la Información. En caso de requerirse mayor capacidad, este será solicitado previa sustentación ante su jefe inmediato superior para su gestión ante la Oficina de Tecnologías de la Información.

- Con la finalidad de optimizar el espacio de almacenamiento (límite de cuota) asignado a cada cuenta de correo, se recomienda eliminar permanentemente los mensajes innecesarios. En caso de mantener los mensajes recibidos, es recomendable agruparlos por temas en carpetas personales.
- Al recibir un mensaje que se considere ofensivo, se debe comunicar y reenviar el mensaje recibido al administrador del correo electrónico a fin de efectuar las acciones respectivas, comunicándole éste al usuario las acciones realizadas.
- Se recomienda a los usuarios no responder los mensajes de correo de origen desconocido ya que ello confirma sus direcciones electrónicas y genera correo no solicitado o SPAM.
- Comunicar a la Oficina de Tecnologías de la Información el ingreso excesivo o indiscriminado de correos no deseados, de origen desconocido o *SPAM* a fin de que tomen las acciones necesarias para su bloqueo y seguridad del correo afectado.

#### 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.
- Evitar el uso de 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.
- Evitar enviar mensajes a personas que no conoce, a menos que sea por un asunto oficial que los involucre.
- Evitar 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, a fin de que el destinatario conozca el contexto en que se está dando el mensaje que recibe. No incluya ningún archivo adjunto que pueda haber recibido originalmente, a no ser que haya realizado modificaciones a tales archivos.

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 Tecnologías de la Información ha determinado en 10 MB. como tamaño máximo permitido del adjunto (que involucra a uno o la suma de todos los archivos) al mensaje de correo electrónico institucional enviado, esto debido a que el envío de correos muy pesados (mayores a 10 MB.) saturan la red y ocupan demasiado espacio en el servidor de correos. Para el envío de archivos de mayor tamaño, deberá ponerse en contacto con la Oficina de Tecnologías de la Información a fin de brindarle las facilidades para concretar dicho envío.

6.1.7. Vigencia de los mensajes

- Se considera como criterio de buen uso del correo electrónico el otorgar vigencia máxima en el buzón del usuario a cualquier mensaje enviado o recibido no mayor a 30 días. Superada la fecha de vigencia, los mensajes deberán ser eliminados por el usuario.
- Si se desea mantener un mensaje en forma permanente, éste deberá almacenarse en carpetas personales, siendo consiente el usuario que estos correos almacenados ocuparán parte importante del espacio en buzón asignado.

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, salvo que por las funciones propias del trabajo así lo demanden.
- 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 Tecnologías de la Información será la encargada de proporcionar las credenciales para el acceso al correo institucional desde fuera del local del Tribunal Constitucional, para lo cual dicha oficina elaboró un manual de acceso, que se adjunta al presente. El enlace para el acceso al correo se encuentra ubicado en la parte superior derecha de la página web institucional.

## 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.

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

- Utilizar el correo electrónico institucional para cualquier propósito comercial, financiero u otro 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.

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

6.2.3.1. 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.

6.2.3.2. 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 la misma.

#### 6.2.3.3. Difusión masiva no autorizada

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

#### 6.2.3.4 Efectuar o facilitar el ataque con objeto de imposibilitar o dificultar el servicio de correo, “*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.
- Enviar 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 la aplicación de otras sanciones y/o penalidades derivadas de tal actividad.

6.2.4. En caso se detectase que en forma reiterativa, una cuenta de correo institucional sea afectada por el envío masivo de correos electrónicos de procedencia dudosa que ponga en peligro la operatividad del servicio de correo, la Oficina de Tecnologías de la Información procederá a bloquear definitivamente dicha cuenta y asignará una nueva, informando los motivos de dicha acción al usuario poseedor de la cuenta y de su jefe inmediato superior; asimismo notificará a la lista de usuarios institucional la asignación de la nueva cuenta de correo.

### 6.3. DE LA SEGURIDAD DEL CORREO ELECTRÓNICO

6.3.1. El servidor de correos del Tribunal Constitucional cuenta con software antivirus y políticas de seguridad que evitan el ingreso de virus adjunto a los mensajes de correo electrónico y del ingreso de correos no deseados denominados *SPAM*. En caso

exista la posibilidad de que algún correo de esta naturaleza logre atravesar estos controles, se recomienda reportar al Administrador de Correo a efectos de bloquear la dirección de origen.

6.3.2. Uso del Antivirus

- Los antivirus de la institución, para estaciones de trabajo, deben estar activados permanentemente.
- El servidor de correo del Tribunal Constitucional cuenta con mecanismos antivirales para correo. Si el servidor detectase que un mensaje contiene un virus o “troyano” - “caballo de troya” que no puede ser removido, el mensaje y adjunto será eliminado inmediatamente. Esta acción se informa al destinatario de correo, precisando que el mensaje fue borrado por contener virus.
- La Oficina de Tecnologías de la Información se encargará de verificar la presencia de virus en el servidor de correo electrónico.

**6.4. DE LA VALIDEZ OFICIAL DEL CORREO ELECTRÓNICO**

- 6.4.1. En el Tribunal Constitucional, el correo electrónico es un mecanismo de distribución y envío de información, aún cuando no se establecen los mecanismos que brinden validez oficial de los mensajes que se transmiten 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 N° 27269, “Ley de Firmas y Certificados Digitales” y de su Reglamento aprobado mediante Decreto Supremo N° 052-2008-PCM.

**VII. DISPOSICIONES COMPLEMENTARIAS**

- 7.1. Las notificaciones institucionales pueden efectuarse mediante correo electrónico conforme el numeral 20.1.2 de la Ley N° 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 algún mensaje de correo cuestionable o ilegal, comunicar a la Oficina de Tecnologías de la Información a fin de tomar las acciones pertinentes.
- 7.4. La función de administración del correo electrónico estará a cargo de la Oficina de Tecnologías de la Información.
- 7.5. Es responsabilidad de la Oficina de Administración de Personal comunicar a la Oficina de Tecnologías de la Información, la relación de altas y bajas del personal a fin de activar o desactivar las cuentas de correo respectivas.
- 7.6. La Oficina de Tecnologías de la Información es la responsable de brindar el apoyo técnico a los usuarios en la configuración y uso de las cuentas de correo y de monitorear el cumplimiento de las políticas de seguridad establecidas que impidan la pérdida de correos o propagación de virus en la red institucional.
- 7.7. La Oficina de Tecnologías de la Información podrá crear discrecionalmente, listas de usuarios según sea la necesidad: listas por modalidad contractual, según rol de los usuarios u otro que facilite el envío del mensaje a cada lista o grupo de interés específico. El envío del mensaje a cualquiera de estas listas, está sujeta a la aprobación de la Secretaría General o la Dirección General de Administración, y la materialización de esa autorización estará a cargo de la Oficina de Administración de Personal o de la Oficina de Imagen Institucional.
- 7.8. Déjese sin efecto la Directiva N° 002-2005 aprobada mediante Resolución Administrativa N° 016-2005-P/TC.