CONTRALORÍA GENERAL

Resolución de Contraloría No. 121-2016-CG

Lima, 03 MAYO 2016

VISTO, la Hoja Informativa N° 00011-2016-CG/PROCAL del Departamento de Gestión de Procesos y Calidad;

CONSIDERANDO:

Que, el artículo 16° de la Ley N° 27785, Ley Orgánica del Sistema Nacional de Control y de la Contraloría General de la República, señala que la Contraloría General de la República es el ente técnico rector del Sistema Nacional de Control, dotado de autonomía administrativa, funcional, económica y financiera;

Que, mediante Resolución Jefatural N° 088-2003-INEI se aprobó la Directiva N° 005-2003-INEI/DTNP "Normas para el uso del servicio de correo electrónico en las entidades de la Administración Pública", que tiene por objetivo dar lineamientos para el uso correcto del servicio de correo electrónico oficial;

Que, mediante Resolución de Contraloría N° 235-2012-CG se aprobó la Directiva N° 005-2012-CG/GAF "Normas para el uso de las computadoras, internet y correo electrónico", con el objetivo de establecer las disposiciones que regulen la utilización y salvaguarda de las computadoras, internet y correo electrónico, así como de sus recursos periféricos, por los usuarios de los servicios de la red de la Contraloría General de la República;

Que, mediante el documento de visto, el Departamento de Gestión de Procesos y Calidad, propone la aprobación del proyecto de Directiva "Asignación, acceso, uso y revocación de los recursos informáticos de la Contraloría General de la República", señalando que resulta necesario emitir un documento normativo que establezca las disposiciones que regulen la asignación, acceso, uso y revocación de los equipos de cómputo, red institucional, servicio de correo electrónico institucional y servicio de Internet de la Contraloría General de la República, indicando que el citado proyecto se ajusta a las disposiciones establecidas en la Directiva N° 014-2013-CG/REG "Organización y Emisión de Documentos Normativos";

En uso de las facultades previstas en el artículo 32° de la Ley N° 27785, Ley Orgánica del Sistema Nacional de Control y de la Contraloría General de la República;

SE RESUELVE:

Artículo Primero.- Aprobar la Directiva N° 007 -2016-CG/PROCAL "Asignación, acceso, uso y revocación de los recursos informáticos de la Contraloría General de la República", cuyo texto forma parte integrante de la presente Resolución.

Artículo Segundo.- Dejar sin efecto la Resolución de Contraloría N° 235-2012-CG, que aprobó la Directiva N° 005-2012-CG/GAF "Normas para el uso de las computadoras, internet y correo electrónico".

Artículo Tercero.- La Directiva "Asignación, acceso, uso y revocación de los recursos informáticos de la Contraloría General de la República", entrará en vigencia a partir del día siguiente hábil de su aprobación.

Artículo Cuarto.- Encargar al Departamento de Tecnologías de la Información la publicación de la presente Resolución y la Directiva aprobada en la Intranet de la Contraloría General de la República.

Regístrese y comuníquese

FUAD KHOURY ZARZAR
Contralor General de la República

LA CONTRALORÍA
GENERAL DE LA REPÚBLICA

DIRECTIVA N° 007-2016-CG/PROCAL

"ASIGNACIÓN, ACCESO, USO Y REVOCACIÓN DE LOS RECURSOS INFORMÁTICOS DE LA CONTRALORÍA GENERAL DE LA REPÚBLICA"

RESOLUCIÓN DE CONTRALORÍA
N° 121-2016-CG

DIRECTIVA Nº 007-2016-CG/PROCAL

ASIGNACIÓN, ACCESO, USO Y REVOCACIÓN DE LOS RECURSOS INFORMÁTICOS DE LA CONTRALORÍA GENERAL DE LA REPÚBLICA

ÍNDICE

1. FINALIDAD

Regular la asignación, acceso, uso y revocación de los recursos informáticos de la Contraloría General de la República, a fin que los usuarios cuenten con las herramientas necesarias para el desarrollo eficiente y eficaz de sus actividades.

2. OBJETIVO

Establecer las disposiciones que regulen la asignación, acceso, uso y revocación de los equipos de cómputo, red institucional, servicio de correo electrónico institucional y servicio de Internet de la Contraloría General de la República.

3. ALCANCE

Las disposiciones de la presente Directiva son aplicables a:

a) Los colaboradores de la Contraloría General de la República, independientemente de su régimen laboral, modalidad contractual o convenio (CAP, CAS y practicantes).
b) Las personas distintas a las señaladas en el literal a) del presente numeral, que prestan servicios en la Contraloría General de la República y que para el desarrollo de sus actividades, según corresponda, se les asignen recursos informáticos de la CGR.
c) Los jefes y el personal de los Órganos de Control Institucional.

Las personas descritas en el presente numeral serán consideradas usuarios para efectos de la presente Directiva.

4. SIGLAS

CD : Disco Compacto (Compact Disc, por sus siglas en inglés).
CGR : Contraloría General de la República.
CPU : Unidad Central de Procesamiento (Central Processing Unit, por sus siglas en inglés).
DVD : Disco Versátil Digital (Digital Versatile Disc, por sus siglas en inglés).
OCI : Órgano de Control Institucional.
SCG : Sistema de Control Gubernamental.
SNC : Sistema Nacional de Control.
USB : Bus Universal en Serie (Universal Serial Bus, por sus siglas en inglés).
WAP : Protocolo de Aplicaciones Inalámbricas (Wireless Application Protocol, por sus siglas en inglés).

5. BASE LEGAL

- Ley N° 27785, Ley Orgánica del Sistema Nacional de Control y de la Contraloría General de la República, y sus modificatorias.
- Ley N° 28493, Ley que regula el uso del correo electrónico comercial no solicitado (SPAM), y su modificatoria.
- Ley N° 29733, Ley de protección de datos personales.
- Decreto Supremo Nº 031-2005-MTC, que aprueba el Reglamento de la Ley N° 28493, Ley que regula el envío de correo electrónico comercial no solicitado (SPAM).

- Decreto Supremo N° 003-2013-JUS, que aprueba el Reglamento de la Ley N° 29733, Ley de protección de datos personales.
- Resolución Ministerial N° 246-2007-PCM, que aprueba el uso obligatorio de la Norma Técnica Peruana "NTP-ISO/IEC 17799:2007 EDI. Tecnología de la Información. Código de buenas prácticas para la gestión de la seguridad de la Información. 2ª. Edición" en todas las entidades integrantes del Sistema Nacional de Informática.
- Resolución de Contraloría N° 178-2010-CG, que aprueba el Reglamento de Seguridad de la Contraloría General de la República.
- Resolución de Gerencia General N° 033-2011-CG/GG, que aprueba la Directiva N° 001-2011-CG/GG-LO-PATRIM "Procedimiento para el Requerimiento de Movimiento de Bienes Patrimoniales por Comisión de Servicio" de la CGR.
- Resolución de Contraloría N° 350-2013-CG, que aprueba el Manual de Políticas de Recursos Humanos de la Contraloría General de la República.
- Resolución de Contraloría N° 173-2015-CG, que aprueba el Reglamento Interno de Trabajo de la Contraloría General de la República.
- Resolución de Contraloría N° 249-2015-CG, que aprueba el Manual de Identidad Corporativa de la Contraloría General de la República.
- Resolución de Contraloría N° 353-2015-CG, que aprueba la versión actualizada de la Directiva N° 007-2015-CG/PROCAL "Directiva de los Órganos de Control Institucional".
- Resolución Jefatural N° 088-2003-INEI, que aprueba la Directiva N° 005-2003-INEI/DTNP "Normas para el uso del servicio de correo electrónico en las entidades de la Administración Pública".
- Reglamento de Organización y Funciones de la Contraloría General de la República vigente.

6. DISPOSICIONES GENERALES

6.1 Asignación y revocación de los recursos informáticos

La CGR puede asignar o revocar a los usuarios los siguientes recursos informáticos:

- Equipos de cómputo.
- Red institucional, la cual comprende los aplicativos informáticos de la CGR.
- Servicio de correo electrónico institucional.
- Servicio de Internet.

La unidad orgánica en la que el usuario desarrolla sus actividades o el Departamento de Gestión de OCI, para el caso de los jefes y el personal de los OCI, cuando corresponda, solicitan la asignación o revocación de los recursos informáticos a las unidades orgánicas que los administran, de acuerdo a lo señalado en las disposiciones específicas desarrolladas en el numeral 7 de la presente Directiva.

La asignación de recursos informáticos a los usuarios establecidos en el literal b) y al personal que no es de la CGR en el caso del literal c) del numeral 3 de la presente Directiva, no genera vínculo laboral o contractual con éstos.

6.2 Cuentas y contraseñas para el acceso y uso de los recursos informáticos

Para el acceso y uso de los recursos informáticos se deberá asignar cuentas y contraseñas al usuario, las cuales son de carácter personal, confidencial e intransferible, bajo su responsabilidad.

Los usuarios señalados en los literales a) y b) del numeral 3 de la presente Directiva, podrán acceder a sus equipos de cómputo y a los aplicativos informáticos de la CGR desde instalaciones fuera de las sedes de la CGR, a través de una contraseña virtual (token virtual) solicitada al Departamento de Tecnologías de la Información, siempre que cuenten con autorización del gerente o jefe de la unidad orgánica en la que desarrollan sus actividades.

El usuario no debe utilizar las cuentas y contraseñas de otro usuario, ni intentar apoderarse de éstas, ni vulnerar los sistemas de seguridad bajo ningún motivo, el incumplimiento de esta disposición conlleva a la aplicación, en lo que corresponda, del Reglamento Interno de Trabajo.

Aquel usuario que advierta una incorrecta utilización de sus cuentas y contraseñas, debe informar de inmediato al gerente o jefe de la unidad orgánica en la que desarrolla sus actividades, y este a su vez informar al Departamento de Seguridad Integral, al Departamento de Tecnologías de la Información y a las unidades orgánicas responsables de los aplicativos informáticos de la CGR que correspondan, a fin que adopten las medidas correspondientes.

Las buenas prácticas para la selección y uso de las contraseñas se encuentran recogidas en el **Anexo N° 03** de la presente Directiva.

6.3 Supervisión de accesos y uso de los recursos informáticos

La supervisión de los accesos y uso de los recursos informáticos asignados a los usuarios se encuentra a cargo del jefe o gerente de la unidad orgánica en la que aquellos desarrollan sus actividades.

Para el caso del personal de OCI, la supervisión de los accesos y uso de los recursos informáticos está a cargo del jefe de OCI; y para el caso del jefe de OCI, la supervisión está a cargo de la unidad orgánica bajo cuyo ámbito se encuentra el OCI.

Cualquier usuario que identifique algún acceso no autorizado o mal uso de un recurso informático, deberá comunicarlo al Departamento de Tecnologías de la Información a fin que revoque dicho acceso y se tomen las medidas correctivas que correspondan.

7. DISPOSICIONES ESPECÍFICAS

Estas disposiciones comprenden las obligaciones, prohibiciones y recomendaciones para la asignación, acceso, uso y revocación de los siguientes recursos informáticos:

- De los equipos de cómputo.
- De la red institucional, la cual comprende los aplicativos informáticos de la CGR.
- Del servicio de correo electrónico institucional.
- Del servicio de Internet.

7.1 De los equipos de cómputo

Los equipos de cómputo están constituidos por las computadoras de escritorio o portátiles, cuya asignación o revocación de asignación se realiza de la forma siguiente:

a) **Asignación:** La unidad orgánica en la que los usuarios señalados en los literales a) y b) del numeral 3 de la presente Directiva desarrollan sus actividades, solicita al Departamento de Tecnologías de la Información la asignación de equipos de cómputo, en atención al inicio de la relación laboral, contractual o por convenio de dichos usuarios.

   Excepcionalmente, el Departamento de Gestión de OCI puede solicitar al Departamento de Tecnologías de la Información la asignación de equipos de cómputo de la CGR para los jefes y el personal del OCI que mantengan vínculo laboral o contractual con la CGR.

b) **Revocación de asignación:** La unidad orgánica en la que los usuarios señalados en los literales a) y b) del numeral 3 de la presente Directiva desarrollan sus actividades, revoca la asignación de equipos de cómputo a dichos usuarios, al término de la relación laboral, contractual o por convenio; para tal efecto, realiza la devolución de los equipos de cómputo al Departamento de Logística.

   El Departamento de Gestión de OCI revoca la asignación de equipos de cómputo a los jefes de OCI o su personal, al término de la relación laboral o contractual de dichos usuarios; para tal efecto, realiza la devolución de los equipos de cómputo al Departamento de Logística.

El Departamento de Tecnologías de la Información realiza las coordinaciones necesarias con control patrimonial del Departamento de Logística, quien es responsable del registro y movimiento de los equipos de cómputo.

El Departamento de Tecnologías de la Información es la única unidad orgánica autorizada a instalar y actualizar el *software* en cada equipo de cómputo de la CGR; así como configurar los accesos para los dispositivos periféricos en los equipos de cómputo en tanto se encuentren en la red de la CGR.

Los usuarios cuyos equipos de cómputo se encuentren permanente o temporalmente fuera de la red de la CGR, y que tengan rol de administrador, son responsables de cualquier instalación no autorizada o indebida de *software* en los equipos de cómputo.

7.1.1 Puertos periféricos del equipo de cómputo

El jefe o gerente de la unidad orgánica en la que el usuario desarrolla sus actividades solicita al Departamento de Tecnologías de la información la asignación o revocación de acceso a los puertos periféricos para el uso de dispositivos periféricos tales como memorias USB, discos duros externos, unidades de CD, DVD, entre otros, de acuerdo a las actividades que desarrolla el usuario.

Los tipos de accesos a los puertos periféricos son los siguientes:

- **Sin acceso:** bloquea el uso de todos los puertos periféricos.
- **Solo lectura:** permite el uso solo para lectura de los dispositivos periféricos. Esta será la configuración por defecto.
- **Total:** permite la lectura y escritura en los dispositivos periféricos.

7.1.2 Obligaciones sobre el uso de los equipos de cómputo

El usuario a fin de dar un uso adecuado a los equipos de cómputo debe cumplir las siguientes obligaciones:

a) Manipular de manera segura los equipos de cómputo.
b) Bloquear los equipos de cómputo (Ctrl + Alt + Supr) en caso el usuario se ausente del lugar donde desarrolla sus actividades.
c) En caso de infección de virus en el equipo de cómputo, reportar inmediatamente al Departamento de Tecnologías de la Información.

Adicionalmente, en el caso de computadoras portátiles, el usuario debe cumplir las siguientes obligaciones:

a) En caso el usuario se ausente del lugar donde desarrolla sus actividades, cerrar la computadora portátil.
b) En caso el usuario se retire del lugar donde desarrolla sus actividades, guardar la computadora portátil en un compartimento con llave; así como conservarla en una oficina, sala o ambiente que tenga llave.
c) En caso el usuario tenga que salir de comisión, mantener la computadora portátil consigo sin perderla de vista.
d) Transportar la computadora portátil en su maletín.
e) En caso de pérdida, sustracción o robo, comunicar de manera inmediata al jefe o gerente de la unidad orgánica en la que desarrolla sus actividades, al Departamento de Logística, al Departamento de Seguridad Integral y al Departamento de Tecnologías de la Información, a fin que adopten las medidas correspondientes.
f) En caso el usuario se encuentre de comisión, generar regularmente una copia de respaldo (Backup) de la información en un dispositivo USB o en un CD, para lo cual se debe haber solicitado previamente la autorización para utilizar estos dispositivos periféricos. El usuario es el único responsable por la integridad de la información contenida en los equipos de cómputo.

7.1.3 Prohibiciones en el uso de los equipos de cómputo

El usuario se encuentra prohibido de:

a) Colocar adhesivos en el equipo de cómputo.
b) Ingerir alimentos, colocar, rociar o manipular líquidos sobre el equipo de cómputo, o cerca de él.
c) Descargar, copiar y guardar información no autorizada en el equipo de cómputo, tales como música, vídeos musicales o de entretenimiento, material pornográfico, entre otros.
d) Colocar o apilar documentos y otros objetos sobre el equipo de cómputo.
e) Colocar el equipo de cómputo en ubicaciones que obstruyan o impidan su adecuada ventilación y uso.
f) Colocar el CPU en una posición distinta a su diseño original, horizontal o vertical.
g) Conectar artefactos eléctricos sobre la línea eléctrica estabilizada de uso exclusivo para los equipos de cómputo, o sobre los estabilizadores de corriente.
h) Cambiar el fondo de pantalla institucional del equipo de cómputo.
i) Instalar en el equipo de cómputo programas informáticos sin autorización del Departamento de Tecnologías de la Información.

j) Instalar o modificar los parámetros, configuración o componentes del hardware o software del equipo de cómputo, sin autorización del Departamento de Tecnologías de la Información.
k) Abrir los equipos de cómputo, así como extraer o cambiar sus componentes, a menos que se cuente con la autorización del Departamento de Tecnologías de la Información.
l) Dejar prendido o desbloqueado el equipo de cómputo cuando se retire o suspenda sus actividades, a menos que usuarios pertenecientes al Departamento de Tecnologías de la Información requieran dejar prendidos sus equipos de cómputo para poder acceder en forma remota en caso de emergencias fuera del horario de trabajo.
m) Establecer conexiones remotas entre el equipo de cómputo y cualquier otro equipo de cómputo ajeno a la institución, sin autorización del jefe o gerente de unidad orgánica en la que desarrolla sus actividades y del gerente del Departamento de Tecnologías de la Información.
n) Ingresar y usar equipos de cómputo ajenos a la institución, sin la autorización del jefe o gerente de la unidad orgánica en la que desarrolla sus actividades.
o) Encriptar carpetas y archivos sin la autorización del jefe o gerente de la unidad orgánica en la que desarrolla sus actividades, y sin el apoyo técnico del Departamento de Tecnologías de la Información.
p) Transferir o intercambiar total o parcialmente bancos de datos personales cuya titularidad corresponda a la CGR a cualquier destino dentro o fuera de la institución, a través de dispositivos periféricos sin la autorización del responsable del banco de datos personales de la CGR.
q) Trasladar computadoras de escritorio a otras instalaciones de la CGR, sin la autorización del jefe o gerente de la unidad orgánica en la que desarrolla sus actividades y del Departamento de Logística.
r) Guardar en el maletín de la computadora portátil algún documento que contenga claves o contraseñas relacionadas a los recursos informáticos de la CGR.

7.1.4 Recomendaciones para el uso de los equipos de cómputo

Se recomienda a los usuarios lo siguiente:

a) Generar regularmente una copia de respaldo (Backup) de la información relevante en la carpeta individual o compartida del servidor a la que tenga acceso, o en un dispositivo USB o CD, siempre que cuente con la autorización para utilizar dispositivos periféricos. El usuario es el único responsable por la integridad de la información contenida en los equipos de cómputo.
b) Transportar en un USB u otro dispositivo periférico la información a trabajar en algún ambiente distinto al que desarrolla sus actividades, siempre que cuente con la autorización para utilizar dispositivos periféricos.
c) En caso el usuario se encuentre de comisión, evitar usar la computadora portátil en lugares públicos.
d) En caso el jefe o gerente de una unidad orgánica solicite el uso de encriptación de carpetas o archivos, o autorice esta, deberá guardar la clave de encriptación de manera diligente y confidencial.

7.1.5 Traslado de equipos de cómputo

El Departamento de Logística es el encargado de registrar en el Sistema de Bienes Patrimoniales o el que haga sus veces, la asignación y los traslados de los equipos de cómputo.

Asimismo, el movimiento de equipos de cómputo por comisión de servicios, deberá sujetarse a lo dispuesto en la Directiva "Procedimiento para el requerimiento de movimiento de bienes patrimoniales por comisión de servicio" de la CGR.

7.2 De la red institucional

La red institucional es el sistema de comunicación que interconecta los equipos de cómputo de los usuarios, permitiendo el intercambio de información, acceso a los servicios de impresión, correo electrónico, Internet y aplicativos informáticos.

Los usuarios pueden acceder a los aplicativos informáticos de la CGR a través de la red institucional cuando se encuentren en las instalaciones de la CGR o mediante la web cuando estén fuera de éstas.

Los usuarios que se encuentran dentro de las instalaciones de la CGR, se encuentran prohibidos de conectar sus equipos a una red de datos diferente a la de la CGR.

7.2.1 Asignación y revocación de accesos a la red institucional, a los aplicativos informáticos de la CGR y al Sistema de Control Gubernamental

a) Red institucional:

El Departamento de Tecnologías de la Información asigna o revoca el acceso a la red institucional, de la forma siguiente:

- La unidad orgánica en la que los usuarios señalados en los literales a) y b) del numeral 3 de la presente Directiva desarrollan sus actividades, debe informar al Departamento de Tecnologías de la Información el inicio o fin de la relación laboral, contractual o por convenio de dichos usuarios, a fin que realice la asignación o revocación de acceso a la red institucional, según corresponda.

- Los jefes y el personal del OCI que tengan cuentas de correo electrónico institucional creadas de acuerdo al numeral 7.3.1 de la presente Directiva, tienen, por defecto, acceso a la red institucional (vía Extranet) asignado por el Departamento de Tecnologías de la Información. Al eliminarse la cuenta de correo electrónico institucional, se revoca también el acceso a la red institucional.

b) Aplicativos informáticos:

La unidad orgánica en la que el usuario desarrolla sus actividades solicita la asignación o revocación de los accesos a los aplicativos informáticos a:

- La unidad orgánica responsable del aplicativo informático que tenga a su cargo la administración de usuarios del aplicativo.

- La unidad orgánica responsable del aplicativo informático quien debe autorizar al Departamento de Tecnologías de la Información para su ejecución, cuando dicha unidad orgánica no tenga a su cargo la administración de usuarios.

Para el caso de los jefes y el personal del OCI, de corresponder, la unidad orgánica bajo cuyo ámbito se encuentra el OCI, solicita la asignación o revocación de los accesos a los aplicativos informáticos de las formas señaladas en el presente literal; a excepción de la solicitud de asignación o de la revocación de acceso al SCG, para tal caso, se aplica el literal c) del presente numeral.

Las funciones de las unidades orgánicas responsables de los aplicativos informáticos se encuentran recogidas en las disposiciones que sobre la materia emita la CGR.

c) Sistema de Control Gubernamental para los jefes y el personal del OCI:

El Departamento de Tecnologías de la Información asigna o revoca el acceso al aplicativo informático SCG o el que haga sus veces, de la forma siguiente:

- **Asignación de acceso al SCG**

  Para los jefes de OCI: el Departamento de Gestión de OCI debe informar al Departamento de Tecnologías de la Información, la designación o encargo de los jefes de OCI, con copia al Departamento de Control de Gestión, a fin que se les asigne el acceso correspondiente al SCG.

  Para el personal del OCI: el jefe de OCI solicita, bajo su responsabilidad, a la unidad orgánica bajo cuyo ámbito se encuentra, el acceso correspondiente al SCG para el personal a su cargo que designe con fines del desempeño de sus funciones; dicha unidad orgánica traslada, a su vez, la solicitud al Departamento de Control de Gestión, a fin que este autorice el acceso respectivo e informe al Departamento de Tecnologías de la Información para que asigne el acceso. El personal del OCI que no mantenga vínculo laboral (CAP o CAS) con la entidad, no podrá tener acceso al SCG.

  El jefe de OCI debe mantener actualizado el registro del personal a su cargo en el SCG en atención al inicio o fin del vínculo laboral (CAP o CAS); de no encontrarse el personal debidamente registrado, el Departamento de Control de Gestión no autorizará los accesos solicitados.

  La omisión del registro, el registro de información incorrecta, incompleta o falsa respecto del personal del OCI en el SCG por parte del jefe de OCI, son consideradas faltas disciplinarias, de acuerdo al literal d) del artículo 60° del Reglamento Interno de Trabajo, aplicándose las disposiciones sobre régimen disciplinario señaladas en los artículos 53° y siguientes del citado Reglamento. Tratándose de jefes de OCI de la entidad, se comunicará dichas situaciones al titular de la misma.

- **Revocación de acceso al SCG:**

  Para los jefes de OCI: el Departamento de Gestión de OCI debe informar al Departamento de Tecnologías de la Información, el término de la designación o el encargo de los jefes de OCI, con copia al Departamento de Control de Gestión, a fin que se revoque el acceso al SCG.

  Para el personal del OCI: la revocación del acceso se realiza de manera automática en atención al fin del vínculo laboral (CAP o CAS) del personal, que el jefe de OCI haya registrado en el SCG.

En caso de vacaciones, licencia, comisión de servicio debidamente autorizado, entre otras circunstancias de ausencia física del Jefe de OCI en la entidad, el Departamento de Gestión de OCI comunica al Departamento de Tecnologías de la Información que el acceso a los aplicativos informáticos será responsabilidad de la persona que haya asumido el encargo de funciones de la jefatura del OCI, de acuerdo al numeral 7.2.6 de la Directiva N° 007-2015-CG/PROCAL "Directiva de los Órganos de Control Institucional".

7.2.2 Carpetas compartidas

Las carpetas compartidas contienen archivos de interés institucional, y son utilizadas por varios usuarios o grupos de usuarios específicos. El uso de carpetas compartidas será de responsabilidad del usuario y para fines estrictamente relacionados con las actividades que desarrolla.

El Departamento de Tecnologías de la Información adoptará las medidas necesarias de respaldo y restauración de la información de las carpetas compartidas, para asegurar la disponibilidad de la misma en caso de pérdida.

Las carpetas compartidas son creadas a solicitud del jefe o gerente de la unidad orgánica, quien autoriza a los usuarios que tendrán acceso; la solicitud debe estar dirigida al Departamento de Tecnologías de la Información.

7.3 Del servicio de correo electrónico institucional

El servicio de correo electrónico institucional de la CGR es de uso exclusivo para comunicaciones relacionadas a los fines institucionales. Es obligación del usuario cautelar y asegurar, en el ámbito de su competencia, que su uso responda a dichos fines.

Los tipos de correos electrónicos institucionales son:

- **Correo tipo 1:** desde el cual se puede enviar o recibir mensajes con archivos adjuntos dentro del dominio de la CGR (contraloría.gob.pe); además puede recibir mensajes con archivos adjuntos desde correos externos. No permite el envío de mensajes hacia correos externos. Los usuarios que tienen este tipo de correo se encuentran señalados en el **Anexo N° 02** de la presente Directiva.

- **Correo tipo 2:** desde el cual se puede enviar o recibir mensajes con archivos adjuntos, tanto dentro como fuera del dominio de la CGR (contraloría.gob.pe). Los usuarios que tienen este tipo de correo se encuentran señalados en el **Anexo N° 02** de la presente Directiva.

Las modalidades de acceso al correo electrónico institucional son mediante:

- **Aplicativo de correo electrónico local:** cuando los usuarios se encuentran en las sedes de la CGR. Todos los usuarios tienen esta modalidad de acceso por defecto.

- **Aplicativo de correo web institucional:** cuando los usuarios se encuentran fuera de las sedes de la CGR. Todos los usuarios tienen la posibilidad de uso de esta modalidad de acceso, para lo cual deben solicitar el usuario y contraseña respectivos al Departamento de Tecnologías de la Información, a excepción de los practicantes.

- **Wap:** cuando los usuarios cuenten con dispositivos móviles inteligentes (Smartphone, Tablet, entre otros) asignados por la CGR. Esta modalidad de acceso debe ser solicitada por el jefe o gerente de la unidad orgánica en la que el usuario desarrolla sus actividades, al Departamento de Tecnologías de la Información para su habilitación. Los usuarios que pueden tener esta modalidad de acceso se encuentran señalados en el **Anexo N° 02** de la presente Directiva.

El cambio del tipo de correo o modalidad de acceso a uno distinto al señalado en el **Anexo N° 02** de la presente Directiva, será solicitado y sustentado formalmente por el jefe o gerente de la unidad orgánica en la que el usuario desarrolla sus actividades o por el jefe de OCI, cuando corresponda, al Departamento de Tecnologías de la Información.

7.3.1 Creación y eliminación de cuentas de correo electrónico institucional

La creación y eliminación de cuentas de correo electrónico institucional está a cargo del Departamento de Tecnologías de la Información y se realiza de la forma siguiente:

- La unidad orgánica en la que los usuarios señalados en los literales a) y b) del numeral 3 de la presente Directiva desarrollan sus actividades o, la unidad orgánica bajo cuyo ámbito se encuentren, debe informar al Departamento de Tecnologías de la Información el inicio o fin de la relación laboral, contractual o por convenio de dichos usuarios, a fin que se realice la creación o eliminación de cuentas de correo respectivas.

- El Departamento de Gestión de OCI, para el caso de los jefes de OCI, debe informar al Departamento de Tecnologías de la Información la designación, el término de esta designación o el encargo de jefes de OCI, a fin que se realice la creación o eliminación de cuentas de correo respectivas.

  En el caso de los jefes de OCI que mantienen vínculo laboral o contractual con la entidad, adicionalmente a lo señalado en el párrafo precedente; deben suscribir previamente a la creación de la cuenta de correo electrónico institucional el Acta de Compromiso que se detalla en el **Anexo N° 04** de la presente Directiva; siendo el Departamento de Gestión de OCI el responsable de su gestión.

Los tipos de correo electrónico institucional que les corresponde a los diferentes usuarios se encuentran detallados en el **Anexo N° 02** de la presente Directiva.

7.3.2 Obligaciones sobre el uso del correo electrónico institucional

El usuario del correo electrónico institucional se encuentra obligado a:

a) Mantener en línea el correo electrónico institucional, y activada la opción de avisar cuando llegue un nuevo mensaje.
b) Leer los mensajes recibidos de manera frecuente.
c) Depurar permanentemente aquellos mensajes innecesarios, a fin que se cuente con espacio disponible.
d) Realizar el archivamiento de los correos electrónicos que desee o sea necesario conservar, de acuerdo al procedimiento que emita el Departamento de Tecnologías de la Información. Se encuentran exceptuados de esta obligación los jefes y el personal de los OCI.
e) Utilizar siempre el campo "asunto" para conocer de qué trata el contenido del mensaje.

f) Expresar las ideas completas, con las palabras y signos de puntuación adecuados en el texto del mensaje.
g) Revisar el texto del mensaje y los destinatarios antes de enviarlo, con el fin de corregir posibles errores de ortografía, forma o fondo.
h) Al enviar un mensaje a un grupo de correos, verificar que el mensaje sea enviado al grupo correcto.
i) Incluir la firma automática en todos los mensajes a ser enviados de acuerdo al Manual de Identidad Corporativa de la CGR.
j) Si recibe un mensaje que se considere no deseado u ofensivo a su persona o a cualquier otra persona, debe comunicar este hecho al correo electrónico admin@contraloria.gob.pe, con el fin que se adopten las acciones respectivas. No debe retransmitirlo a otros usuarios o a terceras personas.
k) En caso se ausente de la institución por vacaciones, licencias, permisos u otros motivos, debe habilitar la opción de respuesta automática *"ausente de oficina"*; y consignar, la fecha de retorno y el funcionario de contacto, para que el remitente pueda derivar su comunicación a quien corresponda.
l) Cerrar la sesión de su correo electrónico en caso se retire o suspenda sus actividades, para evitar que otras personas usen su correo.

7.3.3 Prohibiciones en el uso del correo electrónico institucional

El usuario del correo electrónico institucional se encuentran prohibido de:

a) Utilizar el correo electrónico institucional para fines ajenos a la institución.
b) Inscribirse en listas de correos electrónicos no relacionadas directamente con las actividades que desarrolla.
c) Utilizar una cuenta de correo electrónico institucional diferente a la asignada.
d) Facilitar u ofrecer la contraseña del correo electrónico institucional a otros usuarios o a terceras personas.
e) Facilitar la recolección de correos electrónicos institucionales o la comercialización de bases de datos de correos electrónicos institucionales.
f) Falsificar cuentas de correo electrónico institucional.
g) Realizar manipulaciones técnicas sobre el campo "Asunto", a fin de evitar los sistemas y programas de bloqueo o filtro.
h) Enviar o reenviar cadenas de mensajes o similares.
i) Enviar mensajes con contenidos impropios o lesivos a la moral, o que afecten la imagen de terceros, de la institución u otras entidades públicas o privadas.
j) Enviar mensajes de correo electrónico a otros usuarios o a terceras personas en los que se divulgue, comente o exprese hechos, opiniones o cualquier tipo de información relacionada a controversias, problemas, funcionamiento, políticas, personas o cualquier otra situación o asunto interno de la CGR y del SNC; que puedan poner en entredicho la reputación o imagen institucional, aun cuando la información divulgada no sea de naturaleza reservada, secreta o confidencial.
k) Transferir o intercambiar total o parcialmente bancos de datos personales cuya titularidad corresponda a la CGR a cualquier destino dentro o fuera de la institución, sin la autorización del responsable del banco de datos personales de la CGR.
l) Propiciar o incurrir en actos o ataques con el objeto de imposibilitar o dificultar el servicio de correo electrónico, mediante "mail bombing" o envío desproporcionado de archivos con el propósito de saturar el buzón del correo del destinatario.
m) Enviar de forma masiva publicidad o cualquier otro tipo de correo no solicitado "spam".

n) Abrir correos electrónicos sospechosos o de dudosa procedencia, aún si conociera al remitente, teniendo especial cuidado con los mensajes recibidos en otros idiomas.

7.3.4 Recomendaciones para el uso del servicio de correo electrónico institucional

Se recomienda a los usuarios lo siguiente:

a) Evitar usar la opción "Acuse de recibo", a menos que sea absolutamente necesario en relación a la importancia del mensaje.
b) Evitar el envío de mensajes y archivos adjuntos a grupos de correos, a menos que sea un asunto institucional.
c) En caso de reenvío de un mensaje, incluir el mensaje original, para que el destinatario conozca el contexto en que se está dando el mensaje que recibe.
d) Los correos electrónicos que adjunten documentos que no son propios del remitente, deberán citar siempre la fuente de origen o a los autores, a fin de respetar los derechos de propiedad intelectual.
e) Evitar el uso generalizado de letras mayúsculas.
f) Considerar las buenas prácticas para la selección y uso de las contraseñas, señaladas en el **Anexo N° 03** de la presente Directiva.

7.3.5 Capacidad de almacenamiento del correo electrónico institucional

El Departamento de Tecnologías de la Información fija la capacidad de almacenamiento del correo electrónico institucional del usuario, estableciendo una capacidad básica, que aumentará solo en los siguientes casos:

- Usuarios que son jefes o gerentes de unidad orgánica.
- Usuarios que son jefes de OCI.
- Otros usuarios que cuenten con autorización del jefe o gerente de la unidad orgánica en la que desarrollan sus actividades.

Con la finalidad de mantener disponible la capacidad básica asignada, los usuarios deben realizar el archivamiento de los correos electrónicos de acuerdo al procedimiento que emita el Departamento de Tecnologías de la Información.

7.3.6 Grupos de correos electrónicos institucionales

Los grupos de correos electrónicos institucionales tienen por finalidad facilitar la comunicación masiva de información. Dentro de un grupo existen usuarios que tienen el privilegio de envío de las comunicaciones masivas, y otros de solo lectura. Los grupos solo pueden ser usados dentro del dominio de la CGR (contraloría.gob.pe).

Los tipos de grupos de correos electrónicos institucionales son:

- **Grupos esenciales:** son aquellos grupos cuya naturaleza está relacionada a la existencia de una unidad orgánica de la CGR o a una necesidad institucional de carácter permanente.

  El jefe o gerente de la unidad orgánica o, el responsable designado de los grupos de correos creados por necesidad institucional de carácter permanente, según corresponda, es el responsable de solicitar la actualización de los usuarios integrantes de estos grupos de correos y los privilegios para sus integrantes, al

Departamento de Tecnologías de la Información, quien está a cargo de su implementación.

En caso de modificación de la estructura orgánica de la CGR, cambio de denominación, fusión o absorción de una o más unidades orgánicas, la actualización de la denominación de estos grupos de correos es responsabilidad del Departamento de Tecnologías de la Información, sin que se requiera solicitud alguna.

El Departamento de Tecnologías de la Información comunica quiénes son los responsables de los grupos de correos esenciales.

- **Grupos temporales:** son aquellos grupos creados con fines institucionales específicos o en atención a un tema en particular, son de naturaleza temporal.

  El jefe o gerente de la unidad orgánica es el responsable de solicitar de manera sustentada la creación de estos grupos de correos, indicando el periodo de vigencia y los privilegios para sus integrantes; así como su eliminación y la actualización de los usuarios que los integran, al Departamento de Tecnologías de la Información, quien está a cargo de su implementación.

- **Grupos compuestos:** son aquellos grupos que pueden estar conformados por uno o más grupos esenciales o temporales.

  En caso de modificación de la estructura orgánica de la CGR, cambio de denominación, fusión o absorción de una o más unidades orgánicas, la actualización de la denominación o de la conformación de estos grupos de correos es responsabilidad del Departamento de Tecnologías de la Información, sin que se requiera solicitud alguna.

  En caso contrario, el jefe o gerente de la unidad orgánica o el responsable de algunos de los grupos esenciales que lo conforman, solicita su actualización al Departamento de Tecnologías de la Información, quien está a cargo de su implementación.

7.3.7 Cuentas de correo temático o genérico

Las cuentas de correo temático o genérico son cuentas que se crean para la realización de congresos, eventos, proyectos de diversa índole, entre otros, cuyos propósitos de comunicación tengan fines específicos.

La creación o eliminación de cuentas de correos temáticos o genéricos se realiza a solicitud debidamente sustentada del jefe o gerente de la unidad orgánica, y debe estar dirigida al Departamento de Tecnologías de la Información, quien está a cargo de su implementación.

La solicitud debe señalar quién o quiénes serán los responsables de la administración de las cuentas de correos, e indicar el carácter indefinido o temporal de las mismas, y de ser temporales debe señalarse el periodo de vigencia.

En caso se desactive o fusione la unidad orgánica que solicitó la creación de las cuentas de correos temáticos o genéricos, la unidad orgánica que asuma las funciones de aquella deberá comunicar al Departamento de Tecnologías de la

Información si se mantienen o eliminan las cuentas de correos temáticos o genéricos.

7.3.8 Correos electrónicos de comunicados institucionales

Los correos electrónicos que contengan comunicados institucionales internos podrán ser trasmitidos por los colaboradores, debidamente autorizados por su gerencia central o la unidad orgánica que haga sus veces, quienes serán responsables de su contenido.

7.3.9 Chat interno

El chat interno es un sistema de mensajería instantánea que permite la comunicación entre usuarios de manera inmediata. Por defecto, todos los usuarios tienen acceso al chat interno, a excepción de los jefes y personal de los OCI.

El uso del chat interno es de exclusiva responsabilidad del usuario y para ser utilizado única y exclusivamente para comunicaciones relacionadas con los fines institucionales, el incumplimiento de esta disposición conlleva a la aplicación del Reglamento Interno de Trabajo.

El jefe o gerente de la unidad orgánica en la que el usuario desarrolla sus actividades puede solicitar la revocación del chat interno para dicho usuario.

7.4 Del servicio de Internet

El servicio de Internet complementa la información requerida por el usuario para el desarrollo de sus actividades y es de uso exclusivo para los fines institucionales. Por defecto, todos los usuarios tienen acceso al servicio de Internet básico.

Para el caso de los jefes y el personal del OCI se debe tomar en cuenta las disposiciones sobre implementación del OCI que regula la Directiva de los Órganos de Control Institucional, la cual señala que la entidad provee la infraestructura y capacidad logística requerida por el jefe de OCI.

Los tipos de accesos al servicio de Internet son los siguientes:

- **Internet básico:** acceso a páginas de Internet con temas relacionados a negocios, interés general, traducción web y correo web institucional. Los usuarios que tienen este tipo de acceso por defecto, se encuentran señalados en el **Anexo N° 02** de la presente Directiva.

- **Internet intermedio:** acceso a Internet con los mismos temas del tipo "Internet básico" y adicionalmente con temas relacionados a correo electrónico basado en web (diferente al correo electrónico institucional), grupos de noticias y foros de mensajes.

- **Internet avanzado:** acceso a Internet con los mismos temas del tipo "Internet intermedio" y adicionalmente temas relacionados a mensajería instantánea (web), intercambio de archivos, radio y televisión por Internet, telefonía sobre Internet y redes sociales. Los usuarios que tienen este tipo de acceso por defecto, se encuentran señalados en el **Anexo N° 02** de la presente Directiva, a excepción de aquellos que por razones técnicas tengan restricciones de conexión.

El cambio de tipo de acceso al servicio de Internet por uno distinto al asignado en el **Anexo N° 02** de la presente Directiva, será solicitado y sustentado formalmente por el jefe o gerente de la unidad orgánica en la que el usuario desarrolla sus actividades, al Departamento de Tecnologías de la Información.

El jefe o gerente de la unidad orgánica en la que el usuario desarrolla sus actividades puede solicitar la revocación del servicio de Internet para dicho usuario.

En caso los usuarios sean trasladados de unidad orgánica, se les asignará el acceso al servicio de Internet establecido por defecto en el **Anexo N° 02** de la presente Directiva.

Para el acceso a los tipos de servicio de Internet se tendrá en cuenta las restricciones de conexión que existieran por razones técnicas.

Está prohibido usar en las instalaciones de la CGR dispositivos de comunicación de Internet móvil que no sean de la CGR en los equipos de cómputo asignados por ésta, excepto cuando se trate de usuarios que se encuentren en comisión de servicio.

El Departamento de Tecnologías de la Información restringirá o suspenderá el acceso al servicio de Internet cuando la red institucional de la CGR se encuentre en riesgo o la seguridad de la misma esté comprometida.

8. DISPOSICIONES COMPLEMENTARIAS FINALES

Primera.- Vigencia

La Directiva entrará en vigencia a partir del día hábil siguiente de la aprobación de la Resolución de Contraloría.

Segunda.- Responsabilidades de los jefes y gerentes de las unidades orgánicas

Los jefes y gerentes de las unidades orgánicas son responsables de los recursos informáticos que solicitan, los cuales deberán ser compatibles con las actividades que desarrolla el usuario.

Tercera.- Responsabilidad del usuario

Cada usuario es responsable de las acciones efectuadas en relación con los equipos de cómputo, la red institucional, el servicio de correo electrónico institucional y el servicio de Internet; comprendiendo las consecuencias y responsabilidades administrativas, civiles o penales que se deriven de las mismas.

Cuarta.- Seguridad de la información

Los usuarios se encuentran sujetos a la normativa vigente sobre seguridad de la información y a la que emita la CGR sobre la materia.

Quinta.- Denominación de unidades orgánicas

Cuando en la presente Directiva se hace referencia al Departamento de Tecnologías de la Información, al Departamento de Seguridad Integral, al Departamento de Logística, al Departamento de Gestión de OCI o al Departamento de Control de Gestión, deberá entenderse que se refiere a las unidades orgánicas antes señaladas o las unidades orgánicas que hagan sus veces.

Sexta.- Deterioro, pérdida, sustracción o hurto

En caso de deterioro, pérdida, sustracción o hurto de equipos de cómputo, se aplicará lo dispuesto en el Reglamento de Seguridad de la CGR.

Sétima.- Incumplimiento de la Directiva

El incumplimiento de lo establecido en la presente Directiva, constituye una falta disciplinaria de acuerdo a lo establecido en el literal a) del artículo 60° del Reglamento Interno de Trabajo, aplicándose las disposiciones sobre régimen disciplinario señaladas en los artículos 53° y siguientes del citado Reglamento.

Tratándose de usuarios CAS, practicantes y los señalados en el literal b) del numeral 3 de la presente Directiva, el incumplimiento de ésta se sujeta a lo establecido en los contratos o convenios respectivos.

Octava.- Documentos en el marco del Sistema de Gestión de la Calidad

En caso se requiera regular el desarrollo del contenido de la presente Directiva, se puede elaborar y aprobar documentos tales como manuales, procedimientos, instructivos, guías y directrices, entre otros, en el marco del Sistema de Gestión de la Calidad; los mismos que serán publicados en la Intranet de la CGR, a partir de lo cual serán de obligatorio cumplimiento para las unidades orgánicas, según corresponda.

9. ANEXOS

Anexo N° 01.- Glosario de términos.
Anexo N° 02.- Tipo de correo electrónico institucional y tipo de Internet.
Anexo N° 03.- Buenas prácticas para la selección y uso de las contraseñas.
Anexo N° 04.- Acta de compromiso del jefe del Órgano de Control Institucional.

ANEXOS

Anexo N° 01
Glosario de términos

- **Acceso a los recursos informáticos:** permiso para que un usuario haga uso de los equipos de cómputo, red institucional, servicio de correo electrónico institucional y servicio de Internet.

- **Aplicativo informático:** tipo de programa informático diseñado como herramienta para permitir a un usuario realizar uno o diversos tipos de trabajos.

- **Banco de datos personales:** Conjunto organizado de datos personales, automatizado o no, independientemente del soporte, sea éste físico, magnético, digital, óptico u otros que se creen; cualquiera fuere la forma o modalidad de su creación, formación, almacenamiento, organización y acceso.

- **Computadora portátil:** equipo de cómputo móvil o transportable, no necesita estar conectada físicamente ni a la electricidad ni a una red para ser usada, pueden ser: laptop, notebook, tablet, entre otras.

- **Copia de respaldo (Backup):** copia de datos originales que se realiza con el fin de disponer de un medio para recuperarlos en caso de su pérdida. Esta copia de seguridad debe ser guardada en algún otro sistema de almacenamiento masivo.

- **Correo electrónico (E-mail):** es un servicio de red que permite a los usuarios enviar y recibir mensajes mediante sistemas de comunicación electrónica.

- **Datos personales:** Toda información sobre una persona natural que la identifica o la hace identificable a través de medios que pueden ser razonablemente utilizados.

- **Dispositivos periféricos:** equipos o aparatos auxiliares e independientes conectados a la unidad central de procesamiento de una computadora. Son unidades o dispositivos de hardware a través de los cuales la computadora se comunica con el exterior, y también con los sistemas que almacenan o archivan información, sirviendo de memoria auxiliar de la principal, tales como USB, Disco Duro Externo, CD, DVD, entre otros.

- **Equipos de cómputo:** equipos electrónicos que reciben y procesan datos para convertirlos en información y pueden ejecutar tareas diversas con suma rapidez; poseen una unidad central de procesamiento, memoria principal y algún dispositivo periférico. Los equipos de cómputo pueden ser de escritorio o portátiles. Para efectos de la presente Directiva, abarca también a los dispositivos periféricos.

Hardware (parte física de un equipo informático): conjunto de elementos físicos o materiales que constituyen un equipo de cómputo o sistema informático.

Internet: conjunto descentralizado de redes de comunicación interconectadas que utiliza un protocolo especial de comunicación.

- **Listas de correos electrónicos:** listado que permite la distribución de mensajes entre múltiples usuarios de forma simultánea, y con contenido ajeno a los fines de la institución.

- **Mail bombing (bombardeo de correo electrónico):** envío indiscriminado y masivo de un mensaje a través del correo electrónico, el cual puede generar su saturación.

- **Red (Network):** es el sistema de comunicación de datos que conecta entre sí sistemas informáticos situados en diferentes lugares, que permite la transferencia de datos con la finalidad de compartir información, recursos y ofrecer servicios.

- **Recursos informáticos:** todo equipo informático (servidores, computadoras portátiles, equipos de cómputo de escritorio, dispositivos periféricos), infraestructura de comunicaciones (módems, routers, hubs, entre otros), software, aplicativo informático y servicios (correo electrónico, páginas web, entre otros).

- **Redes sociales:** permiten al usuario construir un perfil público o semi - público dentro de un sistema limitado; articular una lista de otros usuarios con los que comparte una conexión; visualizar y rastrear su lista de contactos y las elaboradas por otros usuarios dentro del sistema.

- **Seguridad de la información:** es la preservación de la confidencialidad, integridad y disponibilidad de la información.

- **Software:** conjunto de programas de cómputo, procedimientos, reglas, documentación y datos asociados, que forman parte de las operaciones de un sistema de computación.

- **Token virtual (contraseña virtual):** es una solución de seguridad de autenticación, permite almacenar claves criptográficas, así como firmas digitales o datos biométricos como huellas digitales. Esta solución de seguridad puede ser física o virtual. Para el caso de la presente Directiva, se encuentra basado en un software, el cual proporciona acceso remoto seguro a los aplicativos por web de la CGR.

- **USB:** dispositivo para el almacenamiento de información digital que utiliza generalmente memorias flash; permite el transporte personal de datos.

- **WEB:** interface simple y consistente para acceder a los recursos de Internet, la información se ofrece en forma de páginas electrónicas.

- **WAP:** protocolo para aplicaciones que utilizan las comunicaciones inalámbricas, por ejemplo: acceso a servicios de Internet desde un teléfono móvil.

Anexo N° 02
Tipo de correo electrónico institucional y tipo de Internet

Usuario	Tipo de correo y modalidad de acceso Wap	Tipo de Internet
• Contralor General de la República • Vice Contralor • Secretaria General • Gerentes Centrales y de Gerencias • Gerentes de Departamentos	• Tipo 2 • Wap	Avanzado
• Gerentes de Oficinas de Coordinación Regional • Jefes de Oficinas Regionales de Control	• Tipo 2 • Wap	Básico(*)
• Encargado temporal de Unidad Orgánica • Jefe de Área	• Tipo 2 • Wap	Básico
• Asesor de Despacho • Asistente de Gerencia del Despacho	• Tipo 2 • Wap	Avanzado
• Jefe de OCI personal CGR	• Tipo 2	No aplica
• Jefe de OCI con vínculo laboral o contractual con la entidad	• Tipo 1	No aplica
• Asistente de Gerencia	• Tipo 2	Básico
• Colaboradores CAP – CAS	• Tipo 1	Básico
• Colaboradores CAP – CAS en Comisión	• Tipo 2	No aplica
• Practicantes	• Tipo 1	Básico
• Personas que prestan servicios en la CGR	• De acuerdo a la cláusula del contrato	Básico

(*) De acuerdo a las condiciones técnicas los Jefes de ORC o Gerentes de las OCR podrán tener acceso al tipo de Internet Avanzado.

Anexo N° 03

Buenas prácticas para la selección y uso de las contraseñas

Selección de contraseñas

Es responsabilidad del usuario seguir las siguientes recomendaciones al momento de seleccionar sus contraseñas:

1. Crear contraseñas de al menos 8 caracteres.
2. Usar contraseñas alfanuméricas, acrónimos, mezcle letras mayúsculas y minúsculas, letras y números, incluya caracteres no alfanuméricos (caracteres especiales tales como &, @, $, y >), acrónimos con número, acrónimos como frase.

   Ejemplos:

   M1cr0$0ft
   7Mf@qp@7@
   ¡Ngc13aeE! (¡Nuestro gato cumplió 13 años en enero!)
   Mgeg&cc17@ (Mi gato está gordo y contento con 17 años)

3. No usar contraseñas que sean palabras (aunque sean extranjeras), o nombres (el del usuario, personajes de ficción, miembros de la familia, mascotas, marcas, ciudades, lugares u otro relacionado).
4. No usar contraseñas completamente numéricas con algún significado (teléfono, D.N.I., fecha de nacimiento, patente del automóvil, etc.) o estén carentes de caracteres consecutivos repetidos o que sean todos numéricos o todas letras.
5. No usar contraseñas que consistan en palabras incluidas en diccionarios.

Uso de contraseñas

Es responsabilidad del usuario cumplir con lo siguiente al momento de hacer uso de sus contraseñas:

1. Cambiar las contraseñas temporales asignadas para inicio, la primera vez que se ingrese al sistema.
2. Cambiar sus contraseñas cada tres meses.
3. Colocar su contraseña sin la presencia de alguien mirando.
4. Evitar enviar la contraseña por correo electrónico o mencionarla en una conversación.
5. No incluir contraseñas en ningún procedimiento automático de conexión que las deje almacenadas permanentemente.
6. No utilizar la misma contraseña para propósitos personales o de negocio.
7. Evitar guardar registros (papel, archivos de *software* o dispositivos) de las contraseñas, salvo si existe una forma segura de hacerlo y el método de almacenamiento ha sido aprobado.
8. Cambiar las contraseñas si se tiene algún indicio de su vulnerabilidad del sistema.
9. En caso de olvido de la contraseña, el usuario deberá gestionar el cambio de la misma a través de la Mesa de Ayuda.

Anexo N° 04
Acta de compromiso del jefe del Órgano de Control Institucional

El presente documento constituye un compromiso del jefe del Órgano de Control Institucional (OCI) encargado de .....[*nombre de la Entidad*] para cumplir las disposiciones relacionadas con el acceso y uso del correo electrónico institucional de la Contraloría General de la República (CGR).

La suscripción del presente compromiso, así como el acceso y uso del correo electrónico institucional de la CGR por parte de los jefes de OCI no genera vínculo laboral o contractual con este Órgano Superior de Control.

I. ALCANCE

El presente compromiso es de aplicación obligatoria para los jefes de OCI que mantienen vínculo laboral o contractual con las entidades señaladas en el artículo 3° de la Ley N° 27785, Ley Orgánica del Sistema Nacional de Control y de la Contraloría General de la República (Jefes de OCI - entidad).

II. OBLIGACIONES

Los jefes de OCI - entidad se encuentran obligados a:

2.1 Mantener en línea el correo electrónico institucional de la CGR.
2.2 Leer los mensajes recibidos de manera frecuente.
2.3 Depurar permanentemente los mensajes innecesarios, a fin que se cuente con espacio disponible.
2.4 Utilizar siempre el campo "asunto" para conocer de qué trata el contenido del mensaje.
2.5 Expresar las ideas completas, con las palabras y signos de puntuación adecuados en el texto del mensaje.
2.6 Revisar el texto del mensaje y los destinatarios antes de enviarlo, con el fin de corregir posibles errores de ortografía, forma o fondo.
2.7 Al enviar un mensaje a un grupo de correos, verificar que el mensaje sea enviado al grupo correcto.
2.8 Incluir la firma en todos los mensajes a ser enviados.
2.9 Si recibe un mensaje que se considere no deseado u ofensivo a su persona o a cualquier otra persona, debe comunicar este hecho al correo electrónico admin@contraloria.gob.pe, a fin que se adopten las acciones respectivas. No debe retransmitirlo a otros usuarios o a terceras personas.
2.10 En caso se ausente de la entidad por vacaciones, licencias, permisos u otros motivos, debe habilitar la opción de respuesta automática "ausente de oficina"; y consignar, la fecha de retorno y el funcionario de contacto, para que el remitente pueda derivar su comunicación a quien corresponda.
2.11 Cerrar la sesión de su correo electrónico en caso se retire o suspenda sus actividades, para evitar que otras personas usen su correo.

PROHIBICIONES

Los jefes de OCI - entidad se encuentran prohibidos de:

3.1 Utilizar el correo electrónico institucional de la CGR para fines ajenos al ejercicio de sus funciones.
3.2 Inscribirse en listas de correos electrónicos no relacionadas directamente con el ejercicio de sus funciones.
3.3 Utilizar una cuenta de correo electrónico institucional de la CGR diferente a la asignada.
3.4 Facilitar u ofrecer la contraseña del correo electrónico institucional de la CGR a otros usuarios o a terceras personas.
3.5 Facilitar la recolección de correos electrónicos institucionales de la CGR o la comercialización de bases de datos de correos electrónicos institucionales de la CGR.
3.6 Falsificar cuentas de correo electrónico institucional de la CGR.
3.7 Realizar manipulaciones técnicas sobre el campo "Asunto", a fin de evitar los sistemas y programas de bloqueo o filtro.
3.8 Enviar o reenviar cadenas de mensajes o similares.
3.9 Enviar mensajes con contenidos impropios o lesivos a la moral, o que afecten la imagen de terceros, de la CGR u otras entidades públicas o privadas.
3.10 Enviar mensajes a otros usuarios o a terceras personas en los que se divulgue, comente o exprese hechos, opiniones o cualquier tipo de información relacionada a controversias, problemas, funcionamiento, políticas, personas o cualquier otra situación o asunto interno de la CGR y del SNC; que puedan poner en entredicho la reputación o imagen institucional, aun cuando la información divulgada no sea de naturaleza reservada, secreta o confidencial.
3.11 Transferir o intercambiar total o parcialmente bancos de datos personales cuya titularidad corresponde a la CGR a cualquier destino, sin la autorización del responsable del banco de datos personales de la CGR.
3.12 Propiciar o incurrir en actos o ataques con el objeto de imposibilitar o dificultar el servicio de correo electrónico de la CGR, mediante "mail bombing" o envío desproporcionado de archivos con el propósito de saturar el buzón del correo del destinatario.
3.13 Enviar de forma masiva publicidad o cualquier otro tipo de correo no solicitado "spam".

3.14 Abrir correos electrónicos sospechosos o de dudosa procedencia, aún si conociera al remitente, teniendo especial cuidado con los mensajes recibidos en otros idiomas.

IV. RECOMENDACIONES

Se recomienda a los jefes de OCI - entidad, lo siguiente:

4.1 Evitar usar la opción "Acuse de recibo", a menos qué sea absolutamente necesario en relación a la importancia del mensaje.
4.2 Evitar el envío de mensajes y archivos adjuntos a grupos de correos, a menos que estén relacionados con el ejercicio de sus funciones.
4.3 En caso de reenvío de un mensaje, incluir el mensaje original, para que el destinatario conozca el contexto en que se está dando el mensaje que recibe.
4.4 Los correos electrónicos que adjunten archivos que no son propios del remitente, deberán citar siempre la fuente de origen o a los autores, a fin de respetar los derechos de propiedad intelectual.
4.5 Evitar el uso generalizado de letras mayúsculas.
4.6 Considerar el **Anexo N° 03** "Buenas prácticas para la selección y uso de las contraseñas" de la Directiva "Asignación, acceso, uso y revocación de los Recursos Informáticos de la CGR".

V. RESPONSABILIDAD

Cada jefe de OCI - entidad es responsable de las acciones efectuadas en relación al acceso y uso del correo electrónico institucional de la CGR, comprendiendo las consecuencias y responsabilidades civiles o penales que se deriven de las mismas.

VI. VIGENCIA

El presente compromiso tendrá vigencia en tanto el jefe del OCI - entidad, mantenga dicho puesto.

El jefe del OCI - entidad que suscribe, expresa su conformidad con la presente Acta de Compromiso, procediendo a firmarla en dos (02) ejemplares de igual contenido, en la ciudad de _____ a los _____ días del mes de _____ del año _____.

Huella Digital

Nombres y Apellidos: .....
DNI N°: .....
Jefe del OCI de: .....
Correo electrónico personal o el otorgado por la entidad a la cual pertenece el OCI (*):

(*) Se le enviará la cuenta y contraseña a este correo.