SUPLEMENTO

REGISTRO OFICIAL
ÓRGANO DE LA REPÚBLICA DEL ECUADOR

SUMARIO:

Págs.

Año III - Nº 571 - 50 páginas
Quito, viernes 5 de noviembre de 2021

ACUERDO No. 018–CG–2021

EL CONTRALOR GENERAL DEL ESTADO

Considerando:

Que, el inciso tercero del artículo 204 de la Constitución de la República del Ecuador otorga a la Contraloría General del Estado personalidad jurídica y autonomía administrativa, financiera, presupuestaria y organizativa;

Que, el número 3 del artículo 212 de la Norma Suprema; y, el artículo 31, numeral 22 y artículo 95 de la Ley Orgánica de la Contraloría General del Estado, establecen que el organismo técnico de control expedirá la normativa necesaria para el cumplimiento de sus funciones;

Que, de conformidad con lo dispuesto en el número 2 del artículo 18 de la Carta Fundamental, todas las personas tienen derecho a acceder libremente a la información generada tanto en entidades públicas, como en privadas que manejen fondos del Estado o realicen funciones públicas, sin que exista reserva de información, excepto en los casos expresamente establecidos en la ley;

Que, el segundo inciso del artículo 1 de la Ley Orgánica de Transparencia y Acceso a la Información Pública, señala que toda la información que emane o esté en poder, entre otros, de las instituciones, organismos y entidades públicas, está sometida al principio de publicidad, salvo las excepciones establecidas en la citada Ley Orgánica;

Que, el crecimiento y fortalecimiento tecnológico e informático que ha experimentado la Contraloría General del Estado en el ejercicio de sus funciones, implementando servicios en línea para la ciudadanía a nivel nacional, han incrementado notablemente el volumen y la criticidad de la información que se genera, procesa y archiva en la infraestructura institucional;

Que, mediante Acuerdo N° 009-CG-2017, de 08 de mayo del 2017, publicado en el Registro Oficial N° 10, de 08 de junio del 2017, se expidió el Reglamento Sustitutivo de Seguridad de la Información, Buen Uso de Internet, Correo electrónico, Control de los Recursos Informáticos y de Telecomunicaciones de la Contraloría General del Estado; y,

Que, es necesario actualizar la normativa institucional vigente con el fin de precautelar la confidencialidad, integridad y disponibilidad de la información que se genera, procesa y almacena en la Contraloría General del Estado.

En ejercicio de las atribuciones conferidas por la Constitución de la República del Ecuador y la Ley Orgánica de la Contraloría General del Estado,

ACUERDA:

EXPEDIR EL REGLAMENTO DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN Y USO RESPONSABLE DE LOS RECURSOS DE TECNOLOGÍA DE LA INFORMACIÓN Y COMUNICACIÓN DE LA CONTRALORÍA GENERAL DEL ESTADO

Capítulo I
Normas Generales

Sección I
Objeto y ámbito de aplicación

Artículo 1.- Ámbito y alcance.- El cumplimiento de las disposiciones incluidas en el presente Reglamento es de carácter general y obligatorio para todos los servidores públicos, los proveedores y personas que desempeñen labores temporales o proporcionen algún tipo de servicio a la Contraloría General del Estado; y, toda persona externa que mantenga relación con la institución y que, como consecuencia de aquello, tenga acceso a la información determinada en el artículo 2 del presente Reglamento.

Artículo. 2.- Objeto.- El presente reglamento tiene por objeto determinar las políticas, acciones y medidas de gestión de seguridad que se requieren para proteger y precautelar la integridad, confidencialidad y disponibilidad de la información generada por cualquier medio en la Contraloría General del Estado dentro de los procesos de control y auditoría, de determinación de responsabilidades, estratégicos, operativos y de apoyo; la relacionada con la correspondencia remitida; la que se encuentra bajo su custodia en archivos digitales, temporales o permanentes; y, en bases de datos o almacenada en los recursos tecnológicos a nivel de usuario, incluyendo sistemas y aplicaciones, hardware de cómputo y red, paquetes de software, dispositivos móviles y sistemas de telecomunicaciones; y, aquella información en etapa de gestión dentro de procesos internos, los cuales constituyen un activo institucional y fundamental para el cumplimiento de las funciones de la entidad.

Artículo 3.- Usuarios involucrados y responsables.- Serán directamente responsables del cumplimiento de este Reglamento los directivos, servidores públicos y trabajadores de la Contraloría General del Estado, incluidos quienes se encuentren en comisión de servicio o con licencia; los auditores internos y servidores públicos que colaboren en las unidades de auditoría interna, así como aquellas personas que presten sus servicios temporales; el personal externo, los proveedores y contratistas que desempeñen labores o proporcionen algún tipo de bien o servicio y que, como consecuencia, tengan acceso a información institucional.

Sección II
Esquema Organizacional de Seguridad de la Información

Artículo 4.- Esquema organizacional.- Con el fin de definir roles y responsabilidades específicas, considerando las actividades necesarias para una correcta gestión de la seguridad de la información en la Contraloría General del Estado, se establece el esquema organizacional detallado en los siguientes artículos.

Artículo 5.- Contralor/a General del Estado.- Es la máxima autoridad de la institución que imparte directrices claras, procurando garantizar de forma permanente que los objetivos de seguridad de la información estén suficientemente identificados y cumplan con las necesidades institucionales, disponiendo la asignación de los recursos necesarios para estos efectos.

El Contralor/a General del Estado aprobará las políticas generales y específicas de seguridad de la información y demás normas y procedimientos relacionados, previniendo sobre su conocimiento y aplicación obligatoria tanto al personal institucional, como a los usuarios externos, asignando para estos propósitos las responsabilidades que sean del caso.

Artículo 6.- Comité de Seguridad de la Información.- El Comité de Seguridad de la Información tendrá las siguientes funciones y responsabilidades:

a) Asesorar a la institución en temas de seguridad de la información;
b) Desarrollar y poner a consideración de la Máxima Autoridad de la Contraloría General del Estado para su respectiva aprobación, las disposiciones inherentes a la gestión de la seguridad de la información que se acatarán dentro de la institución;
c) Responder ante los incidentes de seguridad que sucedieren y activar los procedimientos correspondientes cuando sea necesario;
d) Verificar el cumplimiento de las políticas de seguridad de la información;
e) Procesar los requerimientos institucionales y establecer, en función de la clasificación de la información, las necesidades de respaldo y restauración.

La conformación, miembros, otras funciones y demás procedimientos de este Comité se determinarán en el correspondiente Instructivo de funcionamiento que disponga, para estos efectos, la máxima autoridad o su delegado.

Artículo 7.- Encargado de Seguridad de la Información.- El titular de la Dirección Nacional de Tecnología de la Información y Comunicaciones o su delegado, será el Encargado de Seguridad de la Información y el principal responsable en el proceso de desarrollo y propuesta de los criterios de seguridad de la información, así como de coordinar acciones con el Comité de Seguridad de la Información y velar por la correcta implementación, aplicación y observancia de las políticas y lineamientos de seguridad de la información.

Tendrá las siguientes funciones y responsabilidades:

a) Liderar el proceso de desarrollo, propuesta, adopción y aplicación de políticas, normas y procedimientos de seguridad de la información, tomando en cuenta la evolución tecnológica de la institución;
b) Supervisar y asistir en la ejecución permanente del monitoreo de la seguridad de los sistemas de información de la institución;
c) Mantener medidas y mecanismos de seguridad apropiadas para la protección contra accesos no autorizados a información electrónicamente almacenada y transmitida.

Artículo 8.- Dirección Nacional de Tecnología de la Información y Comunicaciones.- De conformidad con lo previsto en el Estatuto Orgánico de Gestión Organizacional de Procesos de la Contraloría General del Estado, la Dirección Nacional

de Tecnología de la Información y Comunicaciones, entre sus funciones cuenta con la cobertura de los requerimientos para la operación y administración de los sistemas y recursos tecnológicos de la institución; la supervisión de las tareas de desarrollo y mantenimiento de sistemas, siguiendo una metodología de ciclo de vida apropiada; y, la implementación de medidas de seguridad en los sistemas, en todas las fases.

En este contexto, las responsabilidades de la Dirección Nacional de Tecnología de la Información y Comunicaciones, en lo que respecta al ámbito de políticas de seguridad de la información y uso responsable de recursos tecnológicos, incluirán las que a continuación se detallan:

1. Política de Control de Accesos:

a) Implementar y ejecutar los procedimientos para la activación y desactivación de derechos de acceso a redes, incluido el acceso remoto, así como para el resto de recursos de tecnologías de la información;
b) Analizar e implementar los métodos para el control de acceso a los diferentes recursos como redes, servidores, aplicaciones, bases de datos y demás servicios provistos por esta Dirección;
c) Evaluar el costo e impacto de implementación de una infraestructura que permita establecer controles y registros de acceso adecuados a los diferentes servicios y recursos de tecnologías de la información de la institución;
d) Implementar mecanismos de seguridad para el control de conexiones de red, incluidas las de acceso remoto, a nivel físico y lógico, así como para el control de flujo y enrutamiento de tráfico en las distintas subredes de la entidad;

2. Política de uso responsable de recursos de TIC´s:

a) Implementar y mantener un registro de eventos y actividades de los usuarios, en lo concerniente al acceso a los recursos de tecnologías de la información, así como informar sobre accesos indebidos y uso inadecuado de dichos recursos;
b) Entregar a cada usuario las herramientas tecnológicas que requiera acorde a sus funciones y responsabilidades, previa justificación y análisis;
c) Implementar mecanismos y ejecutar el control de la utilización de los recursos tecnológicos e informar, de ser necesario, a la Dirección Nacional de Talento Humano sobre usos indebidos de los mismos por parte de los usuarios para el inicio del régimen disciplinario de ser el caso;
d) Brindar soporte mediante la mesa de ayuda, en lo concerniente al acceso y uso de recursos de tecnología de la información y comunicación;
e) Difundir entre los usuarios y servidores públicos de la institución las políticas, normativa, manuales, guías, etc., para adoptar medidas de prevención y corrección en el uso de los recursos de TIC.

3. Política de Respaldos:

a) Determinar los procedimientos técnicos para el almacenamiento y resguardo de la información, de conformidad con los parámetros establecidos por el Comité de Seguridad de la Información;
b) Definir el procedimiento de etiquetado de las copias de respaldo, identificando su contenido, periodicidad y retención;
c) Determinar el tipo y la frecuencia de los respaldos, de acuerdo a los requisitos de la operación de la institución;
d) Establecer procedimientos regulares de verificación y restauración de los medios de respaldo, a efectos de garantizar que sean confiables para su uso cuando éste se requiera; y,

e) Eliminar de forma segura los medios que contienen información sensible, cuando sea necesario, registrando la eliminación para mantener pruebas de auditoría.

Artículo 9.- Servidores públicos y trabajadores de la Contraloría General del Estado.- Todos los servidores públicos y trabajadores de la institución tienen la responsabilidad de cumplir con las políticas, normas, procedimientos y estándares establecidos por este Organismo Técnico de Control, inherentes a la seguridad de la información.

Capítulo II
Política General de Seguridad de la Información

Artículo 10.- Descripción de la política.- La información institucional contenida en soportes digitales, así como los medios que permiten su gestión y custodia, constituyen activos fundamentales para la Contraloría General del Estado, que deben ser administrados y protegidos garantizando permanentemente su disponibilidad, confidencialidad e integridad, en cumplimiento de las disposiciones contenidas en el presente reglamento.

La Política General de Seguridad de la Información se encuentra soportada por políticas, normas, procedimientos y otros instrumentos específicos, que dirigen el manejo adecuado de la información de la entidad, y proporcionan lineamientos en aspectos como: control de acceso, buen uso de los recursos de tecnologías de la información, respaldos de información, continuidad de operaciones y recuperación ante desastres.

El mantenimiento de la presente política, de las políticas específicas y demás documentos asociados a la política general debe ser realizado por el Encargado de Seguridad de la Información. Las revisiones y cambios serán aprobados por el Comité de Seguridad de la Información y la Máxima Autoridad.

Artículo 11.- Objetivos de la política.- La Política General de Seguridad de la Información tendrá como objetivos los siguientes:

a) Proteger la información que se genera, procesa, transporta y almacena mediante el uso de recursos y servicios de tecnologías de la información.
b) Definir un marco normativo que regule la protección de la información institucional contra la pérdida de confidencialidad, integridad o disponibilidad, ya sea de forma intencional o accidental.
c) Establecer criterios y lineamientos de gestión de seguridad de la información aplicables a la Contraloría General del Estado, que sirvan como base para la adopción de las políticas, normas y procedimientos correspondientes.
d) Asegurar el cumplimiento de los lineamientos establecidos en el ámbito de seguridad de la información, determinando las obligaciones pertinentes y destacando la necesidad de generar estrategias de difusión y toma de conciencia.

Artículo 12.- Clasificación de la información.- Con el fin de garantizar la protección y custodia de la información contenida tanto en documentos digitales, como en correos electrónicos, bases de datos, medios de almacenamiento, archivos de audio y video; e, información verbal, se establece la siguiente clasificación, de acuerdo con su nivel de confidencialidad:

a) **Información reservada.-** Información y documentación clasificada con carácter de reservada, acorde a lo establecido en el artículo 2 del Reglamento de Clasificación de Información Reservada y Confidencial de la Contraloría General del Estado, aprobado mediante Acuerdo 005-CG-2017 de 04 de abril de 2017 y publicado en el Registro Oficial N° 992, de 26 de abril de 2017.

b) **Información de uso interno.-** Información con acceso de lectura para todos los servidores públicos de la institución y sujeta a modificación por personal autorizado.

c) **Información pública.-** Información que no ostente el carácter de reservada y a la que pueda acceder sin restricciones cualquier persona o entidad, así como aquella que no haya sido declarada como reservada por el Comité de Transparencia de la Contraloría General del Estado, de conformidad con lo establecido en el "Instructivo para la publicación de información en la Página WEB de la Contraloría General del Estado", aprobado mediante Acuerdo 006-CG-2019 de 01 de febrero de 2019, publicado en el Suplemento del Registro Oficial N° 427 de 13 de febrero de 2019 y su reforma.

Artículo 13.- Acuerdo de Confidencialidad.- Se suscribirán los siguientes acuerdos de confidencialidad:

- Las autoridades, asesores y demás servidores públicos de la Contraloría General del Estado; y, de ser el caso, las personas naturales y jurídicas externas que presten servicios a la institución y/o tengan acceso a la información en ella generada, suscribirán el "Acuerdo de confidencialidad para el uso de herramientas tecnológicas e información institucional para los servidores de la Contraloría General del Estado" **(*Anexo 1)***

- Los servidores públicos pertenecientes a la Dirección Nacional de Tecnología de la Información y Comunicaciones suscribirán el "Acuerdo de Confidencialidad de la Información para los servidores de la Dirección Nacional de Tecnología de la Información y Comunicaciones" **(*Anexo 2)***

- Los Operadores de Bases de Datos suscribirán el "Acuerdo de Confidencialidad y Responsabilidad de la Información para los Operadores de Bases de Datos" (***Anexo 3)***

- Los Administradores Funcionales de sistemas de las diferentes unidades administrativas suscribirán el "Acuerdo de Confidencialidad y Responsabilidad de la Información para los Administradores Funcionales de Sistemas" **(*Anexo 4*)**

- Los pasantes y/o practicantes suscribirán el "Acuerdo de Confidencialidad para el Uso de Herramientas Tecnológicas e Información Institucional para los Pasantes y/o Practicantes" **(*Anexo 5)***

- Los contratistas de la Contraloría General del Estado suscribirán el "Acuerdo de Confidencialidad de la información para las empresas contratistas" **(*Anexo 6)***. Dentro de los términos de referencia, especificaciones técnicas, pliegos y contrato, la unidad requirente incorporará el requisito de la suscripción del citado acuerdo de confidencialidad.

La Dirección Nacional de Talento Humano se encargará de asegurar que los servidores públicos conozcan su responsabilidad respecto del uso de los recursos informáticos y la información institucional; además, coordinará la suscripción del Acuerdo de

Confidencialidad para todos los servidores públicos, trabajadores y pasantes, con las unidades administrativas de las matriz y Direcciones Provinciales.

La Dirección Nacional de Tecnología de la Información y Comunicaciones se encargará de la suscripción del Acuerdo de Confidencialidad inherente a los servidores de esta unidad; a los operadores de bases de datos institucionales; y, a los administradores funcionales de los sistemas institucionales.

La Dirección Nacional Administrativa y Servicios será la encargada de coordinar la suscripción del Acuerdo de Confidencialidad con el representante legal de la empresa contratista, cuando el caso lo amerite.

Capítulo III
Política de Control de Acceso

Artículo 14.- Descripción de la política.- La Política de Control de Acceso tiene por objeto establecer los mecanismos de control de acceso a nivel de red, sistema operativo, aplicativos, sistemas de información, e implementar los procedimientos destinados a asignar los privilegios correspondientes al perfil de cada usuario que acceda a la información institucional y demás recursos y servicios de tecnología de la información.

Artículo 15.- Objetivos de la política.- La Política de Control de Acceso tendrá los siguientes objetivos:

a) Asegurar que la institución cuente con controles de seguridad adecuados para restringir el acceso a sus sistemas e información.

b) Establecer los lineamientos sobre el control de acceso a la información institucional, con la finalidad de asegurar su confidencialidad, integridad y disponibilidad, conforme lo requieran los sistemas y usuarios de la entidad.

Artículo 16.- Usuarios y privilegios de acceso.- El acceso a los recursos y servicios de tecnología de la información que ofrece la Contraloría General del Estado, se efectuará a través de una cuenta única de usuario con su respectiva contraseña.

La Dirección Nacional de Tecnología de la Información y Comunicaciones establecerá los procedimientos para controlar la asignación de privilegios y derechos de acceso, observando los siguientes principios:

a) **Mínimo conocimiento:** Los usuarios tendrán acceso únicamente a los sistemas e información institucional que sea estricta y efectivamente necesaria para el cumplimiento de sus funciones y responsabilidades.

b) **Menor privilegio:** Se otorgará el acceso con los privilegios mínimos e indispensables para que los usuarios y recursos cumplan con sus funciones y responsabilidades.

Artículo 17.- Gestión de usuarios.- La Dirección Nacional de Tecnología de la Información y Comunicaciones es la encargada de la administración y gestión de cuentas de usuarios de servicios de TI, junto con sus respectivos privilegios de acceso, los cuales se asignarán de acuerdo a lo siguiente:

a) **Usuarios administradores de sistemas e infraestructura:** los servidores públicos de la Dirección Nacional de Tecnología de la Información y

Comunicaciones, encargados de los procesos técnicos de gestión de las diferentes plataformas tecnológicas de software y hardware institucionales.

b) **Usuarios de soporte:** los servidores públicos de la Dirección Nacional de Tecnología de la Información y Comunicaciones que conforman la Gestión de Servicios y servidores públicos afines a nivel nacional, encargados de brindar soporte a los usuarios finales en temas relacionados con el uso de los recursos y servicios de tecnología de la información que ofrece la Contraloría General del Estado.

c) **Usuarios finales:** todos los servidores públicos que poseen acceso autorizado a determinados recursos de tecnología de la información para cumplir con sus funciones y responsabilidades.

Artículo 18.- Actualización de privilegios e información de usuarios.- La Dirección Nacional de Talento Humano, a través de los sistemas informáticos disponibles, proporcionará mensualmente, o cuando el caso lo amerite, a la Dirección Nacional de Tecnología de la Información y Comunicaciones, el detalle de las novedades que se hubieren presentado respecto al ingreso administrativo de los servidores públicos, cese de funciones o comisión de servicios, designación de autoridades y nivel directivo, así como personal contratado, pasantes; y/o, personas que mantengan alguna relación con la entidad, a efectos de habilitar o deshabilitar el acceso a los servicios de tecnología de la información correspondientes.

El servidor público que deje de pertenecer a la institución devolverá en un estado razonable de conservación todas las herramientas informáticas (equipos y dispositivos tecnológicos) que le hayan sido proporcionadas, incluyendo la información en ellas contenida. De esta entrega-recepción se dejará constancia en un acta que será suscrita por el ex servidor público, el custodio de bienes de la unidad administrativa correspondiente, el jefe inmediato superior; y, un delegado de la Dirección Nacional de Tecnología de la Información y Comunicaciones.

Artículo 19.- Uso de la contraseña.- La contraseña tiene por objeto garantizar que únicamente el servidor público a quien se le haya asignado, disponga de acceso a los sistemas y recursos de tecnologías de la información institucionales que estrictamente le correspondan, de acuerdo con su perfil de usuario, funciones y responsabilidades. La contraseña es de uso personal, exclusivo, reservado, confidencial e intransferible; en consecuencia:

a) Se prohíbe a los usuarios, aun cuando se encuentren temporal o definitivamente desvinculados de la Institución por cualquier motivo, dar a conocer su contraseña a terceras personas, así como registrarla en medio alguno o dejarla en sitios de fácil acceso, siendo legalmente responsables por todas y cada una de las actividades que se realicen utilizando su cuenta y contraseña;

b) En caso de que el usuario sospeche que su contraseña es de conocimiento de una tercera persona, gestionará de inmediato su cambio, o solicitará asistencia a la mesa de ayuda de la Administración de Gestión de Servicios de la Dirección Nacional de Tecnología de la Información y Comunicaciones;

c) En caso de que el usuario olvide o pierda su contraseña o su cuenta fuera bloqueada, deberá solicitar el restablecimiento de su contraseña a la mesa de ayuda mencionada en el literal precedente y proceder obligatoriamente con el cambio de la misma;

d) El sistema permitirá máximo cinco (5) intentos fallidos para acceder a una cuenta de usuario. En caso de exceder este número la cuenta será bloqueada

temporalmente por un lapso de treinta (30) minutos, transcurrido el cual se retirará de forma automática el bloqueo sobre la cuenta.

e) Las contraseñas deberán cambiarse de forma permanente cada noventa (90) días, debiendo la Dirección Nacional de Tecnología de la Información y Comunicaciones activar los mecanismos necesarios para notificar oportunamente a los usuarios sobre la obligación de cambiar sus contraseñas a través de las aplicaciones y servicios automáticos institucionales. Para estos efectos, la Administración de Gestión de Servicios de la Dirección Nacional de Tecnología de la Información y Comunicaciones llevará un registro del reseteo y/o cambio de contraseña, como constancia de los requerimientos de los usuarios solicitantes.

f) Los usuarios finales deberán utilizar contraseñas compuestas de por lo menos ocho (8) caracteres. Por su parte, los usuarios administradores de sistemas e infraestructura y los usuarios de soporte deberán utilizar contraseñas compuestas de por lo menos doce (12) caracteres. La Dirección Nacional de Tecnología de la Información y Comunicaciones definirá las características y condiciones que deberán observarse para estos efectos, además de que implementará los respectivos controles que aseguren el cumplimiento de las políticas de seguridad de la información.

g) Las contraseñas serán alfanuméricas y estarán compuestas de por lo menos tres (3) de los siguientes tipos de caracteres: letras mayúsculas (A - Z), letras minúsculas (a - z), dígitos (0 - 9) y/o caracteres no alfanuméricos (# $ @ % &)

h) Para el cambio de contraseñas no se podrá utilizar ninguna de las empleadas anteriormente. De igual modo, no se utilizarán variaciones o secuencias de contraseñas anteriores, así como nombres de usuario, nombres y apellidos propios o de familiares, nombres de mascotas, fechas de nacimiento, nombre de la institución, números de cédula, teléfonos, cuentas personales de correo electrónico, redes sociales, ni cualquier otro dato del usuario que sea fácilmente deducible.

i) Cuando se trate del desarrollo de nuevos sistemas y aplicativos institucionales, las contraseñas asociadas a los mismos deberán ser cambiadas y entregadas al responsable antes de su utilización.

El incumplimiento de lo establecido en este artículo, constituirá causal para la aplicación del régimen disciplinario previsto en el Capítulo XI del Reglamento Interno Sustitutivo de Administración de Talento Humano de la Contraloría General del Estado.

Artículo 20.- Control de acceso a servicios de red.- Con el propósito de garantizar a los usuarios el acceso a las redes y a los recursos y servicios de tecnologías de la información que ofrece la institución; y, con el objeto de precautelar la seguridad de la información, el mismo será controlado, a nivel interno y externo, mediante la segmentación de redes, implementación de firewalls y otros dispositivos de seguridad de red. Del mismo modo, se aplicarán los mecanismos de autenticación necesarios para detectar, prevenir e impedir accesos no autorizados. Para estos efectos se acatarán las siguientes directrices:

a) El acceso a cualquier servicio de red debe ser otorgado únicamente a usuarios, equipos y dispositivos debidamente autorizados;

b) Las conexiones desde distintas localidades deben ser autenticadas usando equipamiento para identificación automática;

c) Cualquier recurso de tecnología de la información que tenga una configuración de diagnóstico, o servicios de gestión vía remota, será evaluado con el propósito de verificar la necesidad de acceder remotamente;

d) Todas las dependencias de la Contraloría General del Estado deben adoptar el enfoque de segmentación de redes para separar de manera lógica los dominios de red;

e) Es obligatorio mantener habilitados únicamente los servicios y puertos lógicos que sean utilizados por los sistemas de información y software de la entidad. Todos los demás deben ser bloqueados; y,

f) Se controlará el acceso lógico a los servicios y recursos de tecnología de la información, tanto en su uso como en su administración, a través de reglas y políticas de seguridad en firewalls de la entidad.

Artículo 21.- Acceso a través de redes inalámbricas.- El acceso a redes inalámbricas se realizará mediante mecanismos apropiados de autenticación, autorización y contabilización. Se emplearán métodos como el estándar 802.1x, opciones de cifrado de al menos WPA-2 y mecanismos de autenticación de doble factor.

La Dirección Nacional de Tecnología de la Información y Comunicaciones se encargará de proveer los recursos e implementar los mecanismos de seguridad necesarios para el acceso a través de redes inalámbricas.

Artículo 22.- Control de acceso al sistema operativo.- La Dirección Nacional de Tecnología de la Información y Comunicaciones implementará los procedimientos y configuraciones necesarias para impedir accesos no autorizados a los sistemas operativos, a través de la aplicación de controles apropiados que permitan autenticar correctamente a los usuarios, proporcionarles el acceso que les corresponda según sus perfiles y funciones, registrar sus actividades y generar notificaciones en caso de incumplimientos.

Artículo 23.- Procedimientos seguros de inicio de sesión.- La Dirección Nacional de Tecnología de la Información y Comunicaciones adoptará procedimientos de inicio de sesión que minimicen al máximo la oportunidad de accesos no autorizados a los sistemas operativos.

Artículo 24.- Sistema de gestión de contraseñas.- Se implementará un sistema eficaz de gestión de contraseñas, cuyas políticas, directrices y procedimientos serán de acatamiento estricto y obligatorio.

Artículo 25.- Uso de programas utilitarios.- La Dirección Nacional de Tecnología de la Información y Comunicaciones controlará la utilización de programas utilitarios, empleando procedimientos adecuados y efectivos de identificación, autenticación y autorización. Únicamente los usuarios administradores podrán instalar y gestionar el acceso a los programas utilitarios que sean permitidos para la entidad.

Artículo 26.- Sesiones inactivas.- Con la finalidad de prevenir que terceras personas accedan a la información o a sistemas y aplicaciones de sesiones previamente iniciadas, todo usuario que se ausente o abandone momentáneamente su estación de trabajo bloqueará el acceso a su equipo mediante protectores de pantalla con contraseñas. Se establecerán mecanismos automáticos para el bloqueo de pantallas y cierre de sesiones en sistemas y aplicativos, en caso de que se detecte inactividad del usuario.

Artículo 27.- Registro de eventos.- Los servidores públicos de la Contraloría General del Estado, incluido el personal técnico de la Dirección Nacional de Tecnología de la Información y Comunicaciones, como operadores de infraestructura, administradores de red, gestores de servicios y calidad; y, programadores de sistemas y administradores de bases de datos, dispondrán de un único identificador de uso exclusivo, a efectos de que todas las actividades realizadas mediante recursos y servicios de tecnología de la información puedan ser registradas y tengan trazabilidad.

Artículo 28.- Acceso remoto.- El acceso o trabajo remoto de usuarios a la red institucional que sea requerido para el desarrollo de sus funciones, de acuerdo con sus roles y responsabilidades previamente establecidos, será otorgado observando los requisitos y procedimientos que para estos efectos determine la Dirección Nacional de Tecnología de la Información y Comunicaciones.

Para el caso de los usuarios externos, tales como proveedores, contratistas y demás entidades públicas o privadas que presten servicios a la Contraloría General del Estado y que, como consecuencia de la prestación de dichos servicios requieran acceso a la red institucional, los respectivos permisos y procedimientos de acceso serán otorgados por la Dirección Nacional de Tecnología de la Información y Comunicaciones, una vez que haya verificado las condiciones de seguridad pertinentes, de conformidad con los siguientes lineamientos:

a) Los accesos vía remota se realizarán exclusivamente mediante herramientas tecnológicas autorizadas y dispuestas por la Dirección Nacional de Tecnología de la Información y Comunicaciones.

b) Cualquier tipo de acceso remoto se realizará mediante conexiones seguras tipo VPN, SSL, IPSec, conexiones HTTPS, o conexiones cifradas.

c) La Dirección Nacional de Tecnología de la Información y Comunicaciones tendrá la potestad de monitorear en todo momento las acciones que se ejecuten mediante el uso del acceso remoto.

d) Los usuarios, sean servidores públicos de la Institución o terceras personas, que requieran utilizar una conexión remota para acceder a la red institucional, solicitarán autorización a la Dirección Nacional de Tecnología de la Información y Comunicaciones, a través de la entrega del "*Formulario para Solicitud de Acceso Remoto*" contenido en el ***Anexo 7*** del presente Reglamento. Para efectos de control, la citada Dirección Nacional mantendrá un registro de las solicitudes en cuestión.

e) Los accesos que se realicen vía remota se limitarán exclusivamente a aquellos recursos que se requieran para el desarrollo de las labores del usuario solicitante, de acuerdo con sus funciones, recursos que se detallarán específicamente en el formulario de solicitud.

f) Es responsabilidad permanente de los usuarios proteger y resguardar sus credenciales, así como los datos proporcionados y demás información inherente a la conexión de acceso remoto que les haya sido autorizada.

Artículo 29.- Dispositivos móviles.- Con el objeto de proteger tanto los recursos institucionales de tecnología de la información como los datos que contienen, frente a eventuales riesgos generados por el acceso proveniente de ambientes potencialmente desprotegidos, la Dirección Nacional de Tecnología de la Información y Comunicaciones implementará controles de acceso a nivel de computación móvil y telefonía celular, indicando previamente al usuario que debe reconocer y aceptar los lineamientos establecidos por la entidad para estos efectos.

Adicionalmente, se observará lo prescrito en el artículo 27 del Reglamento Interno Sustitutivo de Administración del Talento Humano de la Contraloría General del Estado, emitido mediante Acuerdo No. 014-CG-2020 de 08 de julio de 2020, publicado en la Edición especial del Registro Oficial No. 790 de 17 de julio de 2020, respecto de la prohibición de utilizar dispositivos electrónicos móviles de reproducción y grabación fotográfica, de audio y video, en los puestos de trabajo en las unidades administrativas que determine la Dirección Nacional de Gestión Institucional, durante la jornada de trabajo.

El acceso a través de redes institucionales de área local inalámbricas (WLAN) se realizará exclusivamente a través de los mecanismos aprobados y soportados por la Dirección Nacional de Tecnología de la Información y Comunicaciones.

Artículo 30.- Ingreso de equipos externos.- Las personas que no presten sus servicios en la institución y requieran ingresar a sus instalaciones con computadores portátiles y/o dispositivos móviles, cumplirán con el registro y los filtros de seguridad correspondientes, tanto a su entrada como a su salida, para lo cual se deberá completar la información correspondiente según lo contemplado en el documento de "*Registro de Ingreso y Salida de Computadores y/o Equipos Informáticos*", adjunto como ***Anexo 8***, y; de acuerdo a lo previsto para estos efectos en el Instructivo para el Control del Ingreso, Permanencia y Salida de los Visitantes a las Diferentes Dependencias de la Contraloría General del Estado, a nivel nacional, aprobado mediante Acuerdo N° 039-CG-2018, de 20 de junio del 2018, reformado mediante Acuerdo N° 055-CG-2018, de 02 de octubre del 2018. El citado control será realizado por el personal de seguridad contratado por la entidad.

La Dirección Nacional de Tecnología de la Información y Comunicaciones se encargará de controlar el acceso a redes tanto cableadas como inalámbricas de la entidad, que se efectúe empleando dichos equipos y dispositivos.

Artículo 31.- Dispositivos y medios de almacenamiento extraíbles.- A fin de garantizar la integridad y confidencialidad de la información, considerando las vulnerabilidades relacionadas con la facilidad de uso, alta movilidad y capacidad de almacenamiento de dispositivos y medios extraíbles, como lo son la divulgación no autorizada, el robo, el comprometimiento de la integridad de la información, entre otras, la Dirección Nacional de Tecnología de la Información y Comunicaciones, de forma programada y en atención a los requerimientos de las unidades administrativas, procederá a:

1. Restringir el acceso a los puertos USB que permiten la transmisión de información a dispositivos de almacenamiento masivo; y,
2. Aplicar excepciones para los usuarios que requieran el acceso de dispositivos de almacenamiento de información digital.

El servidor público que requiera acceso a estos dispositivos deberá solicitar la autorización pertinente al titular de la unidad administrativa a la que pertenezca. La Dirección Nacional de Tecnología de la Información y Comunicaciones llevará un registro de los usuarios autorizados.

Para estos efectos, cada unidad administrativa informará a la Dirección mencionada el nombre de los servidores públicos autorizados que dispondrán de acceso limitado a dichos dispositivos, quienes serán personal y directamente responsables por la información que almacenen y transmitan.

Artículo 32.- Ingreso al Centro de Datos y Espacios de Telecomunicaciones.- El ingreso de personas a los centros de procesamiento de datos de la institución se controlará mediante mecanismos adecuados para el efecto, como el sistema de acceso biométrico con por lo menos dos (2) factores de autenticación.

Se mantendrá un registro prolijo y permanente de todos los ingresos a dichas instalaciones, que incluirá la información captada por los sistemas de video vigilancia instalados en sus entradas, que contarán además con puertas de seguridad específicamente diseñadas.

El ingreso a estos centros y espacios será permitido exclusivamente a proveedores y personal previamente autorizado de la Dirección Nacional de Tecnología de la Información y Comunicaciones.

Capítulo IV
Política de Uso Responsable de los Recursos de Tecnología de Información y Comunicación

Artículo 33.- Descripción de la política.- Los recursos de tecnología de la información y comunicación, así como los datos e información que se maneja a través de los mismos, son propiedad de la Contraloría General del Estado y serán utilizados exclusivamente con propósitos institucionales; por lo tanto, se establecerán mecanismos de control y uso responsable para su procesamiento, utilización, transferencia y almacenamiento, considerando que constituyen un elemento esencial para el funcionamiento de la Entidad.

Artículo 34.- Objetivos de la política.- La política tiene los siguientes objetivos:

1. Establecer los lineamientos que sustenten el uso adecuado de las herramientas y medios tecnológicos que son puestos a disposición de los usuarios, para el desempeño de sus funciones; y,
2. Asegurar la conservación y buen uso de dichos recursos institucionales.

Sección I
Computadoras y Dispositivos Móviles

Artículo 35.- Computadoras de escritorio, portátiles y demás dispositivos móviles.- La información almacenada y los programas instalados en los equipos informáticos que la Contraloría General del Estado proporciona a sus servidores públicos, constituyen un activo de la entidad; por tanto, su utilización se destinará exclusivamente a funciones y actividades institucionales.

Las computadoras portátiles, de escritorio y demás dispositivos móviles son recursos informáticos de propiedad de la institución que están a cargo y responsabilidad de los servidores públicos, por lo que éstos se encuentran en la obligación de aplicar y mantener las medidas correspondientes para su debido cuidado, precaución, prolijidad y prudencia, a efectos de optimizar su rendimiento, considerando que:

a) Las computadoras de escritorio, portátiles y demás dispositivos móviles de la Contraloría General del Estado deben ser utilizados única y exclusivamente por el personal que se encuentre autorizado para ello y por el responsable de los mismos;

en caso de que el recurso informático vaya a ser empleado por persona diversa a la que fue asignado, esta última garantizará y velará por su buen uso;

b) La adquisición, disponibilidad, distribución, entrega, utilización, devolución y demás aspectos relacionados con los equipos en cuestión, estarán contemplados dentro de las políticas impartidas por la Dirección Nacional de Tecnología de la Información y Comunicaciones, que cuenten con la aprobación de la máxima autoridad;

c) El servidor público encargado mantendrá permanentemente la integridad de los equipos y recursos; y, por ende, de la información que contienen, incluso y particularmente en caso de que éstos se encuentren fuera de las instalaciones de la entidad;

d) Si fuere preciso instalar en los equipos algún programa o aplicación informática que no disponga la entidad, en atención a necesidades estrictamente institucionales, el interesado deberá contactar a la Dirección Nacional de Tecnología de la Información y Comunicaciones, para solicitar la autorización e instalación de la aplicación requerida, luego de haber obtenido la aprobación del titular de su unidad administrativa;

e) Cada usuario será responsable de coordinar, de acuerdo con las instrucciones que para el efecto emita la Dirección Nacional de Tecnología de la Información y Comunicaciones, las actividades relacionadas con el mantenimiento preventivo y correctivo de los equipos informáticos a su cargo, como lo son la instalación de software básico, parches o software de seguridad, aplicaciones, respaldos, entre otras;

f) Con el fin de proteger la información y los programas almacenados en el equipo asignado, los usuarios utilizarán constante y permanentemente el bloqueo de pantalla y acceso a red, para impedir el acceso de personas no autorizadas;

g) Cada usuario es responsable de la información almacenada en su computador por lo que, cuando lo estime pertinente y necesario, solicitará a la Dirección Nacional de Tecnología de la Información y Comunicaciones realizar respaldos de la misma, en función de la criticidad y de las vulnerabilidades de los datos almacenados;

h) En caso de falla o mal funcionamiento de los componentes de hardware o de software de un equipo informático, el servidor público a cargo del equipo reportará el particular a la Administración de Gestión de Servicios de la Dirección Nacional de Tecnología de la Información y Comunicaciones, unidad autorizada para revisar el equipo y corregir las fallas o remitirlo al proveedor en aplicación de la respectiva garantía, cuando ésta se encuentre vigente;

i) Los usuarios de equipos informáticos que deban conectar los mismos a redes diferentes a las de la institución, tomarán todas las precauciones correspondientes para evitar ataques de malware. En caso de duda, antes de volver a conectar el equipo en las redes institucionales, necesariamente acudirá a la Dirección Nacional de Tecnología de la Información y Comunicaciones, para su verificación;

j) Cada usuario precautelará la integridad tanto del computador como de la información y programas en él almacenados e instalados. En caso de pérdida o sustracción, reportará el incidente inmediatamente a su superior inmediato, a la Dirección Nacional Administrativa y Servicios y a la Dirección Nacional de Patrocinio, para que se realice la denuncia y se continúe con el trámite correspondiente, de conformidad con lo previsto en el Reglamento General Sustitutivo para la Administración, Utilización, Manejo y Control de los Bienes e Inventarios del Sector Público.

k) Los usuarios evitarán cualquier actividad que comprometa la seguridad de la información almacenada en sus computadoras y demás dispositivos electrónicos, particularmente en lo que respecta a la introducción de virus o programas que puedan

atentar contra el normal desarrollo de los sistemas. La Dirección Nacional de Tecnología de la Información y Comunicaciones mantendrá actualizado el programa de antivirus y los parches de actualización y seguridad;

l) Los medios electrónicos de almacenamiento de datos (dispositivos móviles) que se introduzcan en los computadores de escritorio y portátiles, deberán ser examinados y sometidos a un programa para detectar malware y evitar que el resto de equipos institucionales se contaminen. La Dirección Nacional de Tecnología de la Información y Comunicaciones realizará las configuraciones necesarias para que el análisis de malware sea automático. Sin perjuicio de ello, será obligación de los servidores públicos ejecutar esta operación en todos los casos, siendo responsables directos de los eventuales daños causados tanto a la información como al equipo;

m) El usuario verificará regularmente que su equipo informático disponga de software antivirus institucional actualizado. De no contar con dicha herramienta o en caso de duda, está obligado a solicitar a la Administración de Gestión de Servicios de la Dirección Nacional de Tecnología de la Información y Comunicaciones su instalación o actualización; y,

n) En caso de suponer o evidenciar la presencia de virus o similares en su equipo informático, el usuario notificará a la Administración de Gestión de Servicios de la Dirección Nacional de Tecnología de la información y Comunicaciones.

Artículo 36.- Prohibiciones en el uso de computadoras de escritorio, portátiles y demás dispositivos móviles.- En lo que a la utilización de equipos y recursos informáticos respecta, queda estrictamente prohibido:

a) Emplearlos para asuntos personales y/o ajenos a la actividad laboral, aún fuera del horario de trabajo y de las instalaciones de la institución;

b) Obtener por cualquier medio y sin consentimiento, información de los computadores o de la red informática de la Contraloría General del Estado, para utilizarla de forma personal o en favor de terceros;

c) Trasladar los equipos informáticos fuera de la institución sin contar con autorización expresa previa y por escrito del titular de la unidad administrativa correspondiente;

d) Manipular los equipos informáticos institucionales; esto es, entre otros similares: instalar, extraer, acoplar o cambiar dispositivos externos o internos, piezas de hardware, accesorios y elementos que no sean de propiedad de la Contraloría General del Estado, sin contar con el consentimiento previo y por escrito de la Dirección Nacional de Tecnología de la Información y Comunicaciones;

e) Instalar en los equipos informáticos institucionales programas de servidores de correo, web, archivos (FTP o TFTP), proxy y similares, ajenos a los proporcionados por la entidad, videojuegos; y, en general, cualquier tipo de software, sea de licencia libre, gratuita o propietaria, puesto que implican un evidente riesgo de daño a los sistemas y perjuicio a la institución. Por software ilegal se entiende cualquier aplicación informática, archivo, imagen, documento, salvapantallas o programa cuya licencia de uso no sea de titularidad de la Contraloría General del Estado. La Dirección Nacional de Tecnología de la Información y Comunicaciones evaluará y autorizará la instalación de software;

f) Instalar, enviar o utilizar aplicaciones informáticas, archivos, imágenes, documentos o programas con contenido ofensivo, inapropiado y/o discriminatorio; en particular, emplear protectores de pantalla, fotos, videos, animaciones o cualquier otro medio de reproducción o visualización con contenido que pueda ser considerado como material de acoso o intimidación en el trabajo;

g) Averiar, dañar o deteriorar intencionalmente las partes y piezas de los equipos informáticos, incluidos puertos USB, entradas y salidas de audio, video, datos y puntos de red;

h) Realizar análisis del flujo de información que pasa por la red (decodificación de paquetes o utilización de sniffers) así como detección de vulnerabilidades de la red y/o equipo de cómputo; y, en definitiva, cualquier forma de ataque o que pretenda acceder a información no autorizada;

i) Acceder, disponer o manipular, sin la correspondiente autorización, repositorios de archivos o bases de datos que contengan información confidencial o reservada;

j) Ausentarse del puesto de trabajo sin bloquear o apagar el computador asignado;

k) Borrar de los equipos y herramientas informáticas archivos, programas; y, en general, cualquier información que tenga relación con la entidad;

l) Operar equipos informáticos no asignados al servidor público para obtener archivos y cualquier otra información en ellos almacenada, o en la red informática de la institución, sin contar con la autorización por escrito del respectivo titular de la unidad administrativa, o por medio de los procedimientos establecidos por la Dirección Nacional de Tecnología de la Información y Comunicaciones para estos efectos;

m) Conectarse a la red con equipos que no sean de propiedad de la Contraloría General del Estado, sin la debida autorización conforme a los términos establecidos por la Dirección Nacional en cuestión;

n) Ejecutar cualquier actividad que afecte perjudicialmente el regular desempeño de las funciones y actividades del resto de servidores públicos y usuarios de red;

o) Utilizar los equipos informáticos institucionales para almacenar y/o manipular documentos ajenos a las funciones y actividades asignadas; y, especialmente, aquellos que contengan material considerado de distracción u ocio; y,

p) Almacenar en los equipos informáticos asignados cualquier archivo o documento de dudosa condición y/o calidad, que pueda ocasionar daños, tanto procedente de internet, como introducido al computador mediante dispositivos de almacenamiento externo (discos duros externos, memorias flash USB, entre otros) de los cuales no se tenga certeza de que están libres de malware.

El quebrantamiento de las prohibiciones establecidas en este artículo, constituirá causal para la aplicación del régimen disciplinario previsto en el Capítulo XI del Reglamento Interno Sustitutivo de Administración de Talento Humano de la Contraloría General del Estado.

Sección II
Internet

Artículo 37.- Internet.- El acceso a internet y demás servicios relacionados está autorizado tanto para las actividades de control y auditoría, determinación de responsabilidades, como para las labores de carácter técnico y administrativo de soporte. No obstante, a efectos de evitar eventuales riesgos ocasionados por su inadecuada utilización, se observarán las siguientes reglas:

a) El acceso a internet se efectuará única y exclusivamente para la investigación de asuntos concretos relacionados con las funciones que desempeñan los servidores públicos de la institución;

b) Durante la jornada de trabajo estará restringido el acceso y la utilización de sistemas públicos de correo electrónico, servicio que además estará sujeto a la política interna de la Dirección Nacional de Tecnología de la Información y Comunicaciones, aprobada por la máxima autoridad;

c) En caso de que un servidor público para el ejercicio de sus funciones requiera acceder a un sitio restringido, remitirá una solicitud a la Administración de Gestión de Servicios de la Dirección Nacional de Tecnología de la Información y Comunicaciones, para su habilitación, previa autorización del titular de su unidad administrativa.

Artículo 38.- Prohibiciones en el acceso a internet.- A fin de evitar eventuales riesgos ocasionados por la inadecuada utilización de esta herramienta informática que la entidad proporciona a sus servidores públicos, queda estrictamente prohibido:

a) Utilizarlo para establecer conexiones no autorizadas;

b) Emplear la cuenta de correo electrónico institucional para conectarse a foros de discusión, redes sociales u otras agrupaciones, salvo que se disponga de autorización previa y se lo haga para ejecutar tareas institucionales;

c) Navegar y/o visitar sitios con contenido ofensivo, inapropiado o discriminatorio; y, en general, sitios ajenos a las actividades institucionales; y,

d) La conexión mediante medios y canales diferentes a los dedicados para el efecto por la Dirección Nacional de Tecnología de la Información y Comunicaciones; es decir, a través de líneas telefónicas, inalámbricas, dispositivos móviles, teléfonos inteligentes o smartphones y otros medios no autorizados.

El quebrantamiento de las prohibiciones establecidas en este artículo, constituirá causal para la aplicación del régimen disciplinario previsto en el Capítulo XI del Reglamento Interno Sustitutivo de Administración de Talento Humano de la Contraloría General del Estado.

Sección III
Correo Electrónico Institucional

Artículo 39.- Correo electrónico institucional.- Constituye una herramienta autorizada tanto para las actividades de control y auditoría, determinación de responsabilidades, como para las labores de carácter técnico y administrativo de soporte. No obstante, a efectos de evitar eventuales riesgos ocasionados por su inadecuada utilización, se acatarán tanto las disposiciones pertinentes contenidas en la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos y su Reglamento, como se observarán las siguientes reglas:

a) A cada servidor público de la Contraloría General del Estado se le asignará una cuenta de correo electrónico institucional, provista por la Dirección Nacional de Tecnología de la Información y Comunicaciones, la misma que será individual y cuyo acceso se efectuará mediante autenticación del usuario y clave personal, siendo una herramienta de uso obligatorio para el desempeño de las actividades institucionales;

b) El uso que se dé a la cuenta institucional de correo electrónico será responsabilidad exclusiva y absoluta de su titular;

c) Cada uno de los usuarios del correo electrónico institucional será responsable del almacenamiento de mensajes y anexos válidos, siendo su obligación eliminar elementos innecesarios;

d) La entidad se reserva el derecho de establecer cuotas de espacio disponible para cada cuenta de correo, pudiendo restringirse de forma automática el envío o recepción de mensajes. En caso de superarse el límite establecido, el usuario solicitará asistencia a la mesa de ayuda a la Administración de Gestión de Servicios de la Dirección Nacional de Tecnología de la Información y Comunicaciones, para descargar los correos electrónicos hacia un espacio adecuado de almacenamiento; y,

e) Las opiniones que los servidores públicos formulen a través de su cuenta de correo electrónico son de carácter personal y en ningún modo implican pronunciamiento ni compromiso institucional alguno, salvo que lo contrario haya sido dispuesto por la autoridad competente.

Artículo 40.- Prohibiciones en el uso del correo electrónico institucional.- Con el propósito de evitar eventuales riesgos ocasionados por la inadecuada utilización de esta herramienta informática que la entidad proporciona a sus servidores públicos, queda estrictamente prohibido:

a) Enviar información de carácter personal y/o relacionada con asuntos ajenos a las funciones y actividades institucionalmente asignadas, así como información reservada o sujeta a sigilo, a menos que se cuente con la disposición o aprobación previa de la máxima autoridad;

b) Interceptar o utilizar el correo electrónico de otros usuarios, alterar o falsificar el contenido de mensajes y ocultar la identidad del remitente. En caso de inobservancia se estará a lo establecido en la Ley Orgánica de la Contraloría General del Estado, previa la ejecución de la auditoría informática correspondiente;

c) Enviar o reenviar, desde y hacia las cuentas institucionales, correos masivos de índole personal, correos no deseados (spam), cadenas y/o mensajes ajenos a las funciones y actividades asignadas;

d) Enviar información institucional mediante correos electrónicos no institucionales;

e) Abrir o reenviar mensajes que no provengan de fuentes conocidas, confiables y seguras, así como descargar anexos de correos que puedan ser fuente de virus o similares, o cuya procedencia y características desconozca.

El quebrantamiento de las prohibiciones establecidas en este artículo, constituirá causal para la aplicación del régimen disciplinario previsto en el Capítulo XI del Reglamento Interno Sustitutivo de Administración de Talento Humano de la Contraloría General del Estado.

Sección IV
Impresoras, Copiadoras y Escáneres

Artículo 41.- Impresoras, copiadoras y escáneres.- Las impresoras, copiadoras y escáneres son recursos informáticos que se encuentran a cargo de una o varias unidades administrativas estando, en tal virtud, a disposición de pluralidad de usuarios, motivo por el cual serán empleados con el debido cuidado, precaución, prolijidad y prudencia, considerando en todo momento que:

a) A cada unidad administrativa o usuario se le asignarán los equipos necesarios para el adecuado desempeño de sus funciones. De ser el caso, los equipos se activarán a través de claves;

b) La Dirección Nacional de Tecnología de la Información y Comunicaciones implementará los respectivos mecanismos que permitan monitorear el mantenimiento y uso adecuado de recursos tecnológicos, impresoras, tóner y demás implementos informáticos, para lo cual se procederá según la necesidad de cada unidad administrativa. Los servidores públicos serán personalmente responsables por la información que impriman;

c) Los equipos estarán ubicados en sitios de fácil acceso, evitando su exposición al sol, al polvo o en zonas que generen electricidad estática;

d) La Dirección Nacional de Tecnología de la Información y Comunicaciones, de ser necesario y en función de optimizar recursos, podrá reubicar los equipos de impresión, copiadoras y escáneres, en coordinación con los respectivos titulares de las unidades administrativas; y,

e) La Dirección Nacional de Tecnología de la Información y Comunicaciones se encargará de diseñar y proponer soluciones integrales de tal manera que, en los espacios asignados a una o más unidades administrativas, se cuente con al menos una impresora multifunción de alto volumen y empresarial.

Artículo 42.- Prohibiciones en el uso de impresoras, copiadoras y escáneres.- A efectos de precautelar el óptimo estado de los equipos y asegurar el uso adecuado de las herramientas informáticas, queda estrictamente prohibido:

a) Emplearlas en asuntos ajenos al desempeño de funciones institucionales;

b) Que sean manipuladas por personal diferente a los técnicos de la Dirección Nacional de Tecnología de la Información y Comunicaciones autorizados para el efecto; y,

c) Trasladar los equipos, escáneres, impresoras, copiadoras y demás dispositivos, fuera del sitio asignado, sin autorización previa de la Dirección Nacional de Tecnología de la Información y Comunicaciones y sin conocimiento del servidor público que esté a cargo del bien y/o del guardalmacén.

El quebrantamiento de las prohibiciones establecidas en este artículo, constituirá causal para la aplicación del régimen disciplinario previsto en el Capítulo XI del Reglamento Interno Sustitutivo de Administración de Talento Humano de la Contraloría General del Estado.

Sección V
Dispositivos de Telefonía

Artículo 43.- Dispositivos de telefonía.- Los teléfonos institucionales constituyen parte integral del servicio de red conocido como telefonía IP y serán asignados a los servidores públicos dependiendo de los requerimientos de la unidad administrativa a la que pertenezcan, para lo cual se observarán las siguientes reglas:

a) La asignación de un teléfono institucional se efectuará mediante la suscripción del documento de acta de entrega-recepción correspondiente;

b) Su utilización se efectuará exclusivamente en actividades institucionales;

c) Para llamadas locales, nacionales, internacionales y celulares, la Dirección Nacional de Tecnología de la Información y Comunicaciones asignará un código de seguridad a cada servidor público;

d) Para llamadas internas entre oficinas de la Contraloría General del Estado a nivel nacional, la conexión se realizará mediante la marcación directa del número de extensión asignada al usuario;

e) Para llamadas locales, nacionales, internacionales y celulares, el tiempo máximo será de veinte (20) minutos por llamada, con las debidas justificaciones de las áreas que requieran el servicio; y,

f) Los servidores públicos reportarán de forma inmediata a la mesa de servicios de la Dirección Nacional de Tecnología de la Información y Comunicaciones sobre cualquier anomalía, desperfecto, mal funcionamiento o incidente que verifiquen en el teléfono asignado.

Artículo 44.- Prohibiciones en el uso de dispositivos de telefonía.- Con el objeto de precautelar el óptimo estado de estas herramientas, queda estrictamente prohibido:

a) Que su configuración sea manipulada o modificada por personal ajeno a la mesa de servicios de la Dirección Nacional de Tecnología de la Información y Comunicaciones; y,

b) Escuchar de forma no autorizada e indebida y/o grabar conversaciones telefónicas realizadas mediante dispositivos pertenecientes a la institución.

Sección VI
Mecanismos de Control de Recursos Informáticos y de Telecomunicaciones

Artículo 45.- Control de recursos informáticos y de telecomunicaciones.- Todos los equipos, herramientas informáticas, tecnológicas y de telecomunicaciones de propiedad de la Contraloría General del Estado, puestas a disposición de los servidores públicos, serán utilizados con fines exclusivamente institucionales y relacionados con las funciones que desempeñan. La institución se reserva el derecho de comprobar, cuando lo estime conveniente, si su utilización se ajusta a dicha finalidad y a lo previsto en este reglamento.

Artículo 46.- Tipos de control.- Con el objeto de implementar mecanismos de control efectivos destinados a verificar la adecuada utilización de los recursos informáticos y de telecomunicaciones, se establecen las siguientes clases o categorías de control:

a) **Control concurrente.-** De manera permanente, solo los servidores públicos autorizados por la Dirección Nacional de Tecnología de la Información y Comunicaciones, monitorearán y brindarán soporte y seguridad, revisarán y verificarán, a través de la red interna institucional, los programas instalados y los servicios puestos a disposición de los servidores públicos de la Institución, precautelando la privacidad, integridad y confidencialidad de la información y enmarcándose dentro de las actividades propias que son de competencia de la Dirección Nacional de Tecnología de la Información y Comunicaciones;

b) **Control a través del acceso físico a los equipos informáticos.-** El control podrá ser realizado a través del acceso físico a los equipos informáticos de los servidores públicos, ante indicios de eventuales usos indebidos de los equipos asignados. En caso de que dicho control deba efectuarse mediante una auditoría de tecnología informática, se observará lo establecido en el procedimiento correspondiente para estos efectos, considerando las normas y técnicas de auditoría previstas en la ley. En todos y cada uno de los casos, el procedimiento de control que se aplique garantizará permanentemente la legalidad, legitimidad, privacidad y confidencialidad de la información contenida en el equipo, de conformidad con lo prescrito a continuación:

1. Se hará en presencia del servidor público al que esté asignado el equipo informático que vaya a ser objeto de control, dentro de la jornada de trabajo. Si el servidor se niega a estar presente durante el control y revisión de su equipo, se hará constar esta circunstancia en el acta que se levante para el efecto.
2. Para realizar la acción de control, en ciertos casos, se podrá trasladar el equipo informático que vaya a ser revisado, a una sala donde se pueda garantizar la privacidad.
3. La revisión del equipo informático será realizada por un profesional en materia informática que designe el Contralor General del Estado. Durante la acción de control, la institución estará representada por un servidor público designado por el titular de la unidad administrativa en la que se realizará dicha acción. Además, la entidad podrá contar con el apoyo y asesoramiento de uno o dos profesionales en materia informática, así como de un abogado de la institución. De ser pertinente, podrá requerirse la presencia de dos servidores públicos, que actuarán en calidad de testigos.
4. El servidor público usuario del equipo informático proporcionará todas las claves de acceso. Si se negare a facilitarlas, se hará constar el particular en el acta correspondiente y se podrán adoptar las medidas técnico-informáticas que permitan el acceso al equipo y a los diferentes programas.
5. La revisión de los equipos podrá abarcar inclusive los archivos que contenga el equipo, a fin de verificar si su utilización ha sido o no correcta. Si alguno de los archivos que estén siendo objeto de revisión contiene información de carácter personal o privado, se hará constar en el acta de entrega-recepción.
6. A efectos de obtener pruebas, archivos, documentos y demás evidencias de la incorrecta utilización del equipo informático, se realizarán copias de seguridad de su contenido, pudiéndose además imprimir la información que fuere del caso.
7. Los documentos que se impriman serán firmados por los presentes y quedarán bajo la custodia del titular de la unidad administrativa que realizó el control y revisión de las copias de seguridad, debiendo permanecer bajo la custodia de la Dirección Nacional de Tecnología de la Información y Comunicaciones.
8. Sobre este procedimiento se levantará un acta, en la que se hará constar el número de documentos impresos y el servidor público responsable de su custodia. Cuando uno de los presentes se negare a firmar alguno de los documentos que se impriman, las razones del hecho se indicarán en dicha acta, misma que contendrá, entre otros puntos, lo siguiente:
   a) Nombres y apellidos completos, número de cédula de ciudadanía de las personas que actúan en la diligencia y la calidad en la que comparecen en el proceso de revisión.
   b) Motivo de la acción de control y descripción de las actuaciones de comprobación que se realicen.
   c) Detalle de cualquier incidente producido durante el proceso de revisión y de los comentarios y opiniones que los asistentes crean oportuno referenciar; y,
   d) En el acta se hará constar que los intervinientes guardarán absoluta reserva sobre el procedimiento realizado. De comprobarse su inobservancia, serán objeto de las correspondientes sanciones disciplinarias.

Artículo 47.- Procedimiento a seguir por cambio, traslado administrativo y/o salida del servidor público.- En todos los casos de cambio, traslado administrativo y salida de servidores públicos de la Institución, se procederá conforme a lo prescrito a continuación:

a) La Dirección Nacional de Talento Humano notificará con antelación al titular de la unidad administrativa correspondiente respecto al cambio, traslado administrativo y/o la salida de la entidad del servidor público; y, éste, a su vez, deberá pedir el apoyo correspondiente a la Dirección Nacional de Tecnología de la Información y Comunicaciones, para que se designe un representante de la misma quien se encargará del proceso de revisión y recepción de la herramienta tecnológica que le fue asignada al servidor público;

b) Se validará la información constante en la herramienta tecnológica, diferenciándose entre información personal y oficial;

c) Se levantará un acta en la que constará toda la información oficial que manejaba el servidor público, la misma que deberá ser entregada a la unidad administrativa mediante medios magnéticos o dispositivos electrónicos. El acta será suscrita por el titular de la unidad administrativa o su delegado, el representante de la Dirección Nacional de Tecnología de la Información y Comunicaciones; y, el servidor público usuario de la herramienta tecnológica;

d) Se remitirá un acta a la Dirección Nacional de Talento Humano, para que ésta continúe con el proceso correspondiente de cambio, traslado administrativo y/o salida de la entidad del servidor público.

Artículo 48.- Reglas especiales en cuanto a la revisión del correo electrónico.- El servicio de correo electrónico que la Contraloría General del Estado brinda a los servidores públicos será utilizado exclusivamente para propósitos institucionales y no deberá comprometer la imagen de la entidad. La Contraloría General del Estado, a través de la Dirección Nacional de Tecnología de la Información y Comunicaciones, establecerá los mecanismos necesarios para que los servidores públicos realicen un buen uso y manejo de las direcciones electrónicas que la entidad dispone para la comunicación interna y externa.

Únicamente las unidades administrativas o personal autorizado por la Dirección Nacional de Tecnología de la Información y Comunicaciones, podrán realizar envíos de correos masivos, sea dentro o fuera de la institución.

Capítulo V
Política de Respaldos

Artículo 49.- Información considerada para respaldos.- La información a ser respaldada es la que se encuentra alojada en bases de datos institucionales consideradas críticas y de alta importancia, incluyendo las de servidores de almacenamiento y compartición de archivos (file servers), así como las de correo electrónico. En este contexto, el acceso a la información almacenada en discos duros locales de los equipos de cómputo estará limitado a determinados servidores públicos, considerando la complejidad y delicadeza de sus funciones. Los procesos de respaldos de información se aplicarán a:

- Base de datos AplicativosCore,
- Base de datos PlanAdquisiciones,
- Base de datos PortalWeb,
- Base de datos de SharePoint (WSS_Content_Intranet),
- Base de datos Históricos de SharePoint (WSS_Content_Historicos),
- Base de datos de Correo Electrónico (Exchange),
- Base de datos BI,
- Logs de auditoría sobre las bases,
- Bases de datos de sistema Autoaudit (SISCONWEB),

- Bases de datos de lectores biométricos de control de acceso,
- Información en servidores de almacenamiento y compartición de archivos,
- Información almacenada en equipos personales de determinados servidores públicos;
- Información de logs de seguridad de equipos perimetrales.

Adicionalmente y para los efectos pertinentes, se tendrán en cuenta las siguientes excepciones:

- No se considerará para propósitos de respaldo la información guardada en dispositivos de usuarios como computadores de escritorio, portátiles, estaciones de trabajo, ni la registrada en las cámaras de video vigilancia, salvo que se trate de dispositivos administrados por la Dirección Nacional de Tecnología de la Información y Comunicaciones, así como de información de bases de datos de telefonía y tarifación.
- Existirán consideraciones especiales para aquellos servidores públicos que, considerando la complejidad y delicadeza de sus funciones, manejen información crítica para la institución, en cuyo caso se utilizarán herramientas para el respaldo de la información.

Artículo 50.- Tipos de respaldo.- Se clasifican en las categorías detalladas a continuación:

- **Total o Completo (Full Backup):** que consiste en la realización de una copia igual a la fuente de información, al día y hora en la que se ejecute el proceso de copia de seguridad mediante herramientas de respaldos.
- **Incremental:** respaldo de la información que ha sido modificada luego de haberse efectuado un respaldo total. Las copias de seguridad posteriores contienen únicamente los cambios registrados desde la realización del respaldo o copia total inicial. En caso de que se requiera una restauración de información es necesario restablecer primero aquella contenida en el respaldo total inicial y luego la contenida en el último respaldo incremental.
- **Diferencial:** De manera similar a los respaldos incrementales, solamente se copia la información que ha sido modificada. Sin embargo, los respaldos diferenciales son acumulativos.
- **Imagen total (Full Image):** es la copia total de servidores virtuales. Se usará únicamente en casos específicos y bajo requerimientos por escrito.

Será responsabilidad de la Dirección Nacional de Tecnología de la Información y Comunicaciones aplicar los métodos de respaldo más adecuados a las necesidades institucionales y al tipo y naturaleza de la información a ser respaldada.

Artículo 51.- Medios para respaldo.- Para respaldos recientes, de hasta dos (2) años de antigüedad, cuya información sea de fácil y rápido acceso, se contemplará el uso de respaldos locales en discos.

En el caso de información cuya antigüedad supere los dos (2) años, deberá contemplarse el uso de dispositivos como cintas magnéticas, que se almacenarán en un sitio externo, con las respectivas precauciones de seguridad.

Artículo 52.- Esquema y frecuencia de procesos de respaldo.- Los procesos de respaldo se ejecutarán en horarios durante los cuales exista el menor riesgo de

afectación posible a los servicios asociados con la información a ser respaldada, considerando la criticidad del servicio.

Para el establecimiento de tareas (Jobs) destinadas a la generación de respaldos, se tomará en cuenta el volumen de la data o información a ser respaldada.

La Dirección Nacional de Tecnología de la Información y Comunicaciones determinará la periodicidad para la generación de respaldos, considerando tanto la frecuencia con que se modifica, elimina y crea la información, como las necesidades institucionales establecidas por el Comité de Seguridad de la Información.

Artículo 53.- Almacenamiento en computadoras.- La información almacenada en discos duros locales de computadoras de escritorio y portátiles asignadas a los servidores públicos, no es objeto de procesos de respaldo; por lo tanto, es responsabilidad de cada uno de los usuarios asegurar que dicha información sea respaldada en servidores de archivos (file servers) u otros medios autorizados, para lo cual solicitará el apoyo del personal de la Dirección Nacional de Tecnología de la Información y Comunicaciones.

Se exceptúan los equipos y dispositivos que alojen información crítica o estén a cargo de determinados servidores públicos, considerando la complejidad y delicadeza de sus funciones, en cuyo caso la Dirección Nacional de Tecnología de la Información y Comunicaciones proporcionará las herramientas pertinentes para el respaldo de la información.

Artículo 54.- Protección de medios de respaldo.- Los medios de respaldo se almacenarán en gabinetes o baúles estructurados con material resistente o retardante de fuego, que cuenten con las respectivas seguridades para restringir su acceso físico, como combinaciones de seguridad. Las locaciones de resguardo de los medios de respaldo proporcionarán condiciones apropiadas de protección física y ambiental.

Para estos efectos se dispondrá de un espacio externo ubicado a una distancia prudencial y suficiente del centro de almacenamiento principal, con el objeto de evitar eventuales daños en caso de que ocurra algún desastre, espacio externo que estará dotado de las condiciones de dimensión y protección ambiental suficientes. Para la Contraloría General del Estado el sitio de almacenamiento externo se ubicará en las instalaciones de la Dirección Provincial del Azuay.

Los medios de respaldo que contengan información de hasta dos (2) años de antigüedad deberán almacenarse en la locación principal. Aquellos medios de respaldo que guarden información cuya antigüedad supere los dos (2) años deberán trasladarse y almacenarse en el sitio externo.

Se realizará permanentemente una limpieza de los drives de lectura y escritura de la plataforma de respaldos con una periodicidad de seis (6) meses.

Artículo 55.- Restauración de información.- En caso de ser necesaria la restauración de información, se remitirá un requerimiento escrito a la Dirección Nacional de Tecnología de la Información y Comunicaciones, en el que conste el nombre especifico del archivo, su fecha de creación, información sobre su última modificación; y, fecha y hora en la que fue destruido o eliminado, siempre que sea posible.

La restauración se realizará en un servidor administrado por el personal de la Administración de Gestión de Infraestructura de la Dirección Nacional en cuestión, dependiendo de la naturaleza, tipo y volumen de la información a ser restaurada y

debiendo considerarse, para estos efectos, los siguientes parámetros y tiempos promedio:

a) Para información de bases de datos con respaldos locales en el sitio principal (on-site), se manejará un término de entre uno (1) y dos (2) días laborables.

b) Para información de file servers con respaldos locales se manejará un término de entre cuatro (4) y ocho (8) horas.

c) Para máquinas virtuales completas con respaldos locales, se manejará un término de entre ocho (8) y doce (12) horas.

d) Para información almacenada en el sitio externo (off-site), se considerará un incremento de dos (2) días laborables, teniendo en cuenta el traslado de los medios de almacenamiento.

Capítulo VI
Régimen Sancionatorio

Artículo 56.- Sanciones.- El incumplimiento de las disposiciones contenidas en el presente Reglamento acarreará la determinación de las responsabilidades administrativas, civiles y/o penales a las que hubiere lugar, de conformidad con lo establecido en la Ley Orgánica del Servicio Público, el Código Orgánico Integral Penal, la Ley Orgánica de la Contraloría General del Estado, la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos; y, demás normativa vigente y aplicable.

La Dirección Nacional de Tecnología de la Información y Comunicaciones, dentro de su respectivo ámbito de competencia, velará permanentemente por el resguardo de los intereses institucionales y el cumplimiento de las Políticas de Seguridad de la Información contenidas en el presente instrumento.

DISPOSICIONES GENERALES

Primera.- El presente instrumento será actualizado, previa autorización del Contralor General del Estado, en atención a las necesidades y requerimientos institucionales, de conformidad con las atribuciones estatutarias asignadas a la Dirección Nacional Jurídica – Gestión de Normativa Técnica, en coordinación y considerando los aportes, recomendaciones e insumos proporcionados por la Dirección Nacional de Tecnología de la Información y Comunicaciones.

Segunda.- Encárguese de la ejecución e implementación del presente Acuerdo a la Dirección Nacional de Tecnología de la Información y Comunicaciones y al Comité de Seguridad de la Información.

DISPOSICIÓN DEROGATORIA

Se deroga el Acuerdo N° 009-CG-2017 de 08 de mayo del 2017 y publicado en el Registro Oficial N° 10 de 08 de junio del 2017 mediante el cual se emitió el "*Reglamento Sustitutivo de Seguridad de la Información, Buen Uso de Internet, Correo electrónico, Control de los Recursos Informáticos y de Telecomunicaciones de la Contraloría General del Estado*".

DISPOSICIÓN FINAL

El presente Acuerdo entrará en vigencia a partir de su publicación en el Registro Oficial.

Dado en el Despacho del Contralor General del Estado, Subrogante, en la ciudad de San Francisco de Quito, Distrito Metropolitano, a los catorce días del mes de octubre de dos mil veintiuno.

Comuníquese.-

Firmado electrónicamente por:
CARLOS ALBERTO RIOFRIO GONZALEZ

Ing. Carlos Alberto Riofrio González
CONTRALOR GENERAL DEL ESTADO, SUBROGANTE

CONTRALORÍA GENERAL DEL ESTADO. – SECRETARÍA GENERAL. - Dictó y firmó electrónicamente el Acuerdo que antecede el ingeniero Carlos Riofrio González, Contralor General del Estado, Subrogante, en la ciudad de San Francisco de Quito, Distrito Metropolitano, a los 14 días del mes de octubre de dos mil veintiuno. - LO CERTIFICO.

Firmado electrónicamente por:
MARCELO FERNANDO MANCHENO MANTILLA

Dr. Marcelo Mancheno Mantilla
Secretario General

ANEXO 1

ACUERDO DE CONFIDENCIALIDAD PARA EL USO DE HERRAMIENTAS TECNOLÓGICAS E INFORMACIÓN INSTITUCIONAL PARA LOS SERVIDORES DE LA CONTRALORÍA GENERAL DEL ESTADO

ANTECEDENTES:

Suscriben el presente Acuerdo de Confidencialidad los servidores/as de la Contraloría General del Estado (bajo cualquier modalidad de prestación de servicios), y tiene como finalidad establecer expresamente la responsabilidad del servidor/a respecto del uso de los recursos informáticos de los que la institución dispone; y, que entrega a cada uno de sus servidores/as para el cumplimiento de sus funciones. En consecuencia, quienes forman parte de esta entidad, al suscribirlo, aceptan las limitaciones y restricciones de acceso a la información y divulgación de la misma.

El acceso a la información que los servidores/as de la Contraloría tienen para cumplir con las funciones a ellos encomendadas es libre de acuerdo al nivel de competencia que desempeñen; por tanto, es preciso proteger la información constituida en patrimonio institucional. El uso indebido o ilegal de la información acarrearía consecuencias negativas en contra de los intereses institucionales y nacionales por lo que, a partir de la suscripción de este Acuerdo de Confidencialidad, el servidor/a que haga mal uso de dicha información o de los medios que la contienen, se someterá a las sanciones que las disposiciones legales y reglamentarias establecen para el efecto.

COMPROMISO:

Considerando lo manifestado, yo, (nombres y apellidos completos); de nacionalidad_____; mayor de edad; portador de cédula de identidad o ciudadanía o pasaporte No._____; código _____; en mi calidad de (nombre del cargo), (con nombramiento provisional, nombramiento definitivo, a contrato) de la Contraloría General del Estado, a quien en lo posterior se denominará servidor/a, a través del presente documento acepto y me comprometo a guardar la confidencialidad en el tratamiento de la información respecto al ejercicio de las funciones inherentes a mi cargo, de conformidad con las siguientes cláusulas:

PRIMERA.- La Contraloría General del Estado posee una plataforma y sistemas informáticos debidamente registrados que conforman el patrimonio tecnológico de la entidad, constituidos por la plataforma informática, red de comunicación, dispositivos informáticos (hardware y software) y todos los demás recursos integrados con la tecnología de la información, que permiten el desarrollo diario de sus actividades, los cuales están a disposición limitada de todos los servidores/as, conforme sus funciones y las necesidades institucionales.

La Contraloría General del Estado, en el cumplimiento de su misión y de las disposiciones constitucionales y legales que regulan su actividad, crea información a través de sus diferentes procesos generadores de valor y habilitantes, información que es de su propiedad y, el servidor/a acepta y reconoce tal calidad sin objeción alguna, por lo que, el acceso a ésta es limitado, y los servidores/as podrán acceder a la misma, conforme las

necesidades de cada función y con las restricciones que al respecto señalan las normas legales, en especial la Ley Orgánica de Transparencia y Acceso a la Información Pública.

Se considera información de propiedad de la institución y de prohibida publicación y/o divulgación, toda clase de documentos, archivos e información que se encuentren en soportes físicos o electrónicos, así como registros, diagramas, flujogramas, dibujos, fotografías, disposiciones internas, memorándums, programas para computadora desarrollados al interior de la entidad, creaciones en multimedia o equipos digitales, logotipos, ideas, proyectos y en general toda clase de datos que se generen en la entidad, como parte de sus labores.

Conforme lo expuesto, el/la servidor/a (nombres y apellidos completos), reconoce y acepta que toda la información es de propiedad de la entidad, salvo aquella que por su naturaleza es pública y se encuentra a disposición de la sociedad por intermedio del portal institucional.

El/la servidor/a reconoce y acepta además que todos los recursos informáticos que se encuentran definidos bajo el dominio “contraloria.gob.ec” son de propiedad exclusiva de la Contraloría General del Estado.

El/la servidor/a reconoce y acepta que el uso del correo electrónico de la Contraloría General del Estado y el acceso al servicio de Internet a través de la red interna, constituyen una herramienta que la entidad le otorga a fin de que pueda realizar sus labores, por lo que su uso, a más de estar limitado al ejercicio de las funciones de cada servidor/a, podrá ser restringido total o parcialmente, sin previo consentimiento de aquel.

De ser dispuesta la medida de restricción total o parcial para los servicios de correo electrónico o de internet o ambos a la vez, se comunicará al servidor/a para que pueda adoptar medidas de comunicación diferentes, a fin de cumplir con sus funciones.

Por ser el acceso a correo externo ilimitado, toda clase de información, documentos, comunicación o mensaje de datos enviado por esta vía, deben de guardar cuidado con la imagen institucional, por lo que la Contraloría General del Estado adoptará las medidas necesarias para evitar daños en su imagen y fugas de información, sin que por ello se pueda alegar violación de privacidad.

El/la servidor/a acepta y reconoce que la información de la Contraloría General del Estado constituye un bien intangible invalorable, por lo que los riesgos por mal uso y/o divulgación indebida de la misma comportan que la entidad deba tomar medidas respecto de la integridad documental e informática.

El/la servidor/a se obliga a mantener y guardar confidencialidad y reserva respecto de la información relevante que le sea entregada para cumplir con sus labores, quedando prohibido divulgar por cualquier medio, distribuir, reproducir, traducir, utilizar, disponer, y/o publicar la información que le haya sido proporcionada, que haya obtenido o que llegue a conocer por cualquier canal de comunicación institucional.

En el soporte informático que la institución proporcione a cada servidor/a, siempre que así se requiera para cumplir con sus funciones, éste/a podrá almacenar y mantener información personal, si la información no causa problemas a los sistemas de la entidad y si no supera el tamaño de almacenamiento que impida el normal funcionamiento del equipo.

Cada servidor/a será responsable de la asignación, uso y cuidado de sus claves de acceso a los sistemas informáticos, las cuales son personales e intransferibles, sin que se pueda alegar necesidades personales o institucionales, para divulgarlas por cualquier medio, permitiendo que otros servidores/as accedan a los sistemas con claves ajenas.

El/la servidor/a que ingrese información a las herramientas tecnológicas y de información que la Contraloría General del Estado le ha proveído para el desempeño y desarrollo de

su trabajo, deberá asumir la responsabilidad de los datos ingresados procurando que los mismos sean veraces, coherentes y oportunos.

SEGUNDA. – El/la servidor/a se compromete a utilizar tanto la información documental como digital y los recursos tecnológicos de la Contraloría General del Estado con ética, reserva y profesionalismo conforme las normas y reglamentos vigentes.

El/la servidor/a acepta que la Contraloría General del Estado puede ejercer control y seguimiento de la información institucional que esté bajo su custodia, así como de los recursos tecnológicos a él/ella proporcionados, con la finalidad de garantizar el uso correcto de la información y los sistemas informáticos, cuando lo estime pertinente y sin necesidad de notificación previa.

TERCERA. - La Contraloría General del Estado, previa autorización judicial y con la obligación de guardar en secreto la información para cuando sea necesario, podrá abrir, retener y examinar la correspondencia electrónica contenida en la cuenta individual de correo electrónico de el/la servidor/a de la institución, que esté bajo el dominio "contraloría.gob.ec", así como la información electrónica que esté contenida en los recursos tecnológicos asignados

CUARTA. – La Contraloría General del Estado se reserva la atribución de aplicar el régimen disciplinario previsto en el Reglamento Interno Sustitutivo de Administración de Talento Humano de la Contraloría General del Estado, ante el incumplimiento del presente Acuerdo.

QUINTA.- El uso inadecuado, inapropiado y no autorizado de las herramientas informáticas y de la información de la Contraloría General del Estado conforme las disposiciones del "Reglamento de políticas de seguridad de la información y uso responsable de los recursos de tecnología de la información y comunicación de la Contraloría General del Estado" y el incumplimiento de los términos señalados en este instrumento, facultará a esta entidad el inicio de acciones administrativas, civiles y/o penales en contra de los servidores que incumplieren lo descrito en esta cláusula.

El/la servidor/a público acepta y declara de forma expresa que se somete a las responsabilidades y sanciones que le sean imputables, sin perjuicio del establecimiento de responsabilidades administrativas, civiles y/o penales.

El presente Acuerdo de Confidencialidad tendrá vigencia durante el tiempo que el/la servidor/a preste sus servicios a la institución; y, por ética profesional, posteriormente a su salida, sin perjuicio de la adopción de nuevas medidas de seguridad, las cuales serán automáticamente incorporadas y constituirán parte de este instrumento.

En virtud de lo expuesto, acepto de manera voluntaria las cláusulas contenidas en el presente Acuerdo de Confidencialidad, a fin de ejercer mis funciones de manera idónea y proba.

Atentamente,

_____

(nombres y apellidos completos)
Servidor/a de la (nombre de la Unidad Administrativa a la que pertenece)
Cargo:
Cédula y/o pasaporte:

Recibo una copia del presente documento

ANEXO 2

ACUERDO DE CONFIDENCIALIDAD DE LA INFORMACIÓN PARA LOS SERVIDORES DE LA DIRECCIÓN NACIONAL DE TECNOLOGÍA DE LA INFORMACIÓN Y COMUNICACIONES

El/la señor/a, (nombres y apellidos completos) de nacionalidad (señalar nacionalidad), mayor de edad, portador de cédula de identidad o pasaporte No. (XXXXXXXXXX); con el cargo de (indicar el cargo) de la Dirección Nacional de Tecnología de la Información y Comunicaciones (DNTIyC), que en adelante para los efectos del presente instrumento se denominará "servidor/a", de manera libre, voluntaria y en pleno uso de sus capacidades, suscribe el presente Acuerdo de Confidencialidad al tenor de las siguientes cláusulas:

PRIMERA.- OBJETO

Mediante el presente instrumento el/la servidor/a acepta y se obliga a guardar sigilo, confidencialidad y reserva, sobre toda la información de la Contraloría General del Estado a la cual pueda tener acceso, incluyendo, pero no limitándose a: bases de datos; sistemas informáticos; sistemas gestión de infraestructura tecnológica; y, credenciales de acceso que le sean otorgadas para el manejo de diferentes recursos.

Además, el/la servidor/a se compromete a hacer uso de la información exclusivamente para la realización de actividades relacionadas con las funciones que desempeña, conforme a las obligaciones y prohibiciones legales pertinentes.

SEGUNDA.- CREDENCIALES DE ACCESO

El/la servidor/a acepta que la o las credenciales que le sean otorgadas para acceso a sistemas en todos los ambientes de desarrollo, control de calidad o producción, bases de datos, e infraestructura tecnológica, según corresponda; son de uso personal e intransferible, cuya utilización es de su exclusiva responsabilidad.

El/la servidor/a se compromete a no divulgar ni a revelar las credenciales de acceso que le sean otorgadas, incluso después de que haya terminado la relación laboral con la Contraloría General del Estado.

En caso de pérdida, olvido, sustracción o destrucción de la o las credenciales de acceso que le sean otorgadas, el/la servidor/a deberá comunicar el hecho al Director Nacional de Tecnología de la Información y Comunicaciones de manera inmediata.

TERCERA.- MANEJO DE INFORMACIÓN INSTITUCIONAL

Las bases de datos, sistemas informáticos y la información contenida en todos los elementos de hardware y software de la infraestructura tecnológica y centro de datos, se considera como información confidencial. El/la servidor/a debe guardar absoluta reserva de la misma.

El/la servidor/a se compromete a no divulgar, no revelar, ni alterar la información de las bases de datos y sistemas informáticos de la Contraloría General del Estado. De igual forma, se compromete a no divulgar ni alterar información relacionada a procedimientos, configuraciones y demás aspectos técnicos y administrativos que se generen, incluso después de que haya terminado la relación laboral.

El/la servidor/a también se compromete a no divulgar, reproducir o utilizar el código fuente de sistemas informáticos desarrollados en la institución o adquiridos, ni la información relacionada, a la cual, por motivos del desarrollo de sus actividades laborales pudiera tener acceso.

CUARTA.- SANCIONES

La Contraloría General del Estado se reserva la atribución de aplicar el régimen disciplinario previsto en el Reglamento Interno Sustitutivo de Administración de Talento Humano de la Contraloría General del Estado, ante el incumplimiento del presente Acuerdo.

El uso inadecuado, inapropiado y no autorizado de las herramientas informáticas y de la información de la Contraloría General del Estado conforme las disposiciones del "Reglamento de políticas de seguridad de la información y uso responsable de los recursos de tecnología de la información y comunicación de la Contraloría General del Estado" y el incumplimiento de los términos señalados en este instrumento, facultará a esta entidad el inicio de acciones administrativas, civiles y/o penales en contra de los servidores que incumplieren lo descrito en esta cláusula.

El/la servidor/a público acepta y declara de forma expresa que se somete a las responsabilidades y sanciones que le sean imputables, sin perjuicio del establecimiento de responsabilidades administrativas, civiles y/o penales.

QUINTA.- VIGENCIA

El presente Acuerdo de Confidencialidad tendrá vigencia durante el tiempo que el/la servidor/a preste sus servicios a la Institución; y, por ética profesional, posteriormente a su salida, sin perjuicio de la adopción de nuevas medidas de seguridad, las cuales serán automáticamente incorporadas y constituirán parte de este instrumento.

SEXTA.- ACEPTACIÓN

El/la servidor/a conoce y acepta el contenido de todas y cada una de las cláusulas del presente Acuerdo de Confidencialidad y en consecuencia, de manera voluntaria se compromete a cumplirlas en toda su extensión. Para constancia y fines legales pertinentes, se firman dos ejemplares del presente documento, con el mismo tenor y efecto, en la ciudad de (ciudad), el día (día del mes) del mes de (especificar mes) del año (año).

Atentamente,

_____

(nombres y apellidos completos)
Servidor/a de la (nombre de la Unidad Administrativa a la que pertenece)
Cargo:
Cédula y/o pasaporte:

Recibo una copia del presente documento

ANEXO 3

ACUERDO DE CONFIDENCIALIDAD Y RESPONSABILIDAD DE LA INFORMACIÓN PARA LOS OPERADORES DE BASES DE DATOS

El/la señor/a, (nombres y apellidos completos) de nacionalidad (señalar nacionalidad), mayor de edad, portador de cédula de identidad o pasaporte No. (XXXXXXXXXX); como especialista encardado de la operación de las bases de datos institucionales, dentro de la Dirección Nacional de Tecnología de la Información y Comunicaciones (DNTIyC), y que, en adelante y para los efectos del presente instrumento se denominará "DBA", de manera libre y voluntaria, y en el uso de sus capacidades, suscribe el presente Acuerdo de Confidencialidad y Responsabilidad al tenor de las siguientes cláusulas:

PRIMERA. - OBJETO

Mediante el presente instrumento el/la DBA, acepta y se obliga a guardar absoluta confidencialidad y reserva sobre todos los datos e información de la Contraloría General del Estado, que se encuentre dentro de cualquier tipo de base de datos, y que, por motivo de sus funciones y responsabilidades, llegare a conocer, tener acceso, y hacer uso o manejo.

SEGUNDA. – CONFIDENCIALIDAD Y RESPONSABILIDAD

El/la DBA acepta y entiende que, es responsable de la administración de las bases de datos institucionales, que contienen información de propiedad de la Contraloría General del Estado, por lo que se compromete a:

- Custodiar y proteger diligentemente toda la información a la que tenga acceso, conocimiento o que se encuentre en su poder, y, guardar confidencialidad de la información contenida en las bases de datos institucionales, junto con el manejo de las herramientas de gestión de bases de datos.
- No alterar la información contenida en las bases de datos de la Contraloría General del Estado, ni la información relacionada a procedimientos, configuraciones, y demás aspectos técnicos y administrativos que se generen, excepto cuando existan controles de cambios regularizados o autorizaciones explícitas para el efecto.
- Conceder y permitir el acceso a la información dentro de las bases de datos, únicamente a aquellos/as funcionarios/as autorizados/as, con la aprobación del Director Nacional de Tecnología de la Información y Comunicaciones; de forma limitada, exclusivamente a lo que fuere necesario, y, adicionalmente, llevar un registro actualizado de los permisos concedidos.
- Responder en caso de que se hayan concedido accesos no autorizados a bases de datos y a la información contenida en ellas, o en caso de que funcionarios/as para los que se concedió acceso legítimo infringieren las obligaciones de confidencialidad establecidas por la institución.

- Abstenerse de realizar copias o reproducciones de la información, exceptuando las copias estrictamente necesarias que se encuentren programadas en planes de respaldos, o cuando se requieran copias para otros ambientes como control de calidad y desarrollo, con la respectiva aprobación del Director Nacional de Tecnología de la Información y Comunicaciones.
- No pretender titularidad o autoría de ningún tipo, ni solicitar privilegios de propiedad intelectual sobre la información contenida en cualquier base de datos de la Contraloría General del Estado.
- Informar de forma inmediata y por escrito al Director Nacional de Tecnología de la Información y Comunicaciones, en caso de que se detecten accesos no autorizados, posibles fugas de información, niveles o roles de permisos alterados, sobre las bases de datos que administra.

Adicionalmente, el/la DBA acepta que la o las credenciales que le sean otorgadas, para acceso a los sistemas de gestión de bases de datos institucionales; son de uso personal e intransferible, cuya utilización es de su exclusiva responsabilidad. El/la DBA se compromete a no divulgar dichas credenciales, incluso después de que haya terminado la relación laboral con la Contraloría General del Estado.

En caso de pérdida, olvido, sustracción, o destrucción de la o las credenciales de acceso que le sean otorgadas, el/la servidor/a deberá comunicar el hecho al Director Nacional de Tecnología de la Información y Comunicaciones de manera inmediata.

TERCERA. – SANCIONES

La Contraloría General del Estado se reserva la atribución de aplicar el régimen disciplinario previsto en el Reglamento Interno Sustitutivo de Administración de Talento Humano de la Contraloría General del Estado, ante el incumplimiento del presente Acuerdo.

El uso inadecuado, inapropiado y no autorizado de las herramientas informáticas y de la información de la Contraloría General del Estado conforme las disposiciones del "Reglamento de políticas de seguridad de la información y uso responsable de los recursos de tecnología de la información y comunicación de la Contraloría General del Estado" y el incumplimiento de los términos señalados en este instrumento, facultará a esta entidad el inicio de acciones administrativas, civiles y/o penales en contra de el/la DBA que incumpliere lo descrito en esta cláusula.

El/la DBA acepta y declara de forma expresa que se somete a las responsabilidades y sanciones que le sean imputables, sin perjuicio del establecimiento de responsabilidades administrativas, civiles y/o penales.

CUARTA. – VIGENCIA

El presente Acuerdo de Confidencialidad tendrá vigencia durante el tiempo que el/la servidor/a preste sus servicios a la Institución; y, por ética profesional, posteriormente a su salida, sin perjuicio de la adopción de nuevas medidas de seguridad, las cuales serán automáticamente incorporadas y constituirán parte de este instrumento.

QUINTA. – ACEPTACIÓN

El/la DBA conoce y acepta el contenido de todas y cada una de las cláusulas del presente acuerdo, y, en consecuencia, de manera voluntaria se compromete a cumplirlas en toda su extensión. Para constancia y fines legales pertinentes, se firman dos ejemplares del

presente documento, con el mismo tenor y efecto, en la ciudad de (ciudad), el día (día del mes) del mes de (especificar mes) del año (año).

_____
(nombres y apellidos completos)
Cédula/pasaporte: XXXXXXXXXX

ANEXO 4

ACUERDO DE CONFIDENCIALIDAD Y RESPONSABILIDAD DE LA INFORMACIÓN PARA LOS ADMINISTRADORES FUNCIONALES DE SISTEMAS

El/la señor/a, (nombres y apellidos completos) de nacionalidad (señalar nacionalidad), mayor de edad, portador de cédula de identidad o pasaporte No. (XXXXXXXXXX); como encargado/a de la administración funcional del sistema (nombre del sistema) de la Contraloría General del Estado, que en adelante y para los efectos del presente instrumento se denominará "administrador/a funcional", de manera libre y voluntaria, y en el uso de sus capacidades, suscribe el presente Acuerdo de Confidencialidad y Responsabilidad al tenor de las siguientes cláusulas:

PRIMERA. - OBJETO

A través del presente instrumento el/la administrador/a funcional, acepta y se obliga a guardar absoluta confidencialidad y reserva sobre toda la información de la Contraloría General del Estado, que se encuentre dentro del sistema o forme parte del mismo, y que, por motivo de sus funciones y responsabilidades, llegare a conocer, tener acceso, y hacer uso o manejo.

SEGUNDA. – CONFIDENCIALIDAD Y RESPONSABILIDAD

El/la administrador/a funcional acepta y entiende que, es responsable del manejo integral del funcionamiento del sistema y de los procesos automatizados en el mismo; y de toda la información ingresada, procesada u obtenida de dicho sistema, que constituye información de propiedad de la Contraloría General del Estado. Por ello se compromete a:

- Custodiar y proteger diligentemente toda la información a la que tenga acceso, conocimiento o que se encuentre en su poder, y, guardar confidencialidad de la información contenida en el sistema.
- Mantener la integridad de la información contenida en el sistema, y no alterar la misma a menos que se tenga un requerimiento específico, o cuando existan solicitudes regularizadas y autorizaciones explícitas para el efecto.
- Solicitar la asignación o eliminación oportuna de permisos de acceso al sistema, con los perfiles de usuario adecuados, únicamente a aquellos/as funcionarios/as autorizados/as; exclusivamente a lo que fuere necesario, y, adicionalmente, llevar un registro actualizado de los perfiles y permisos concedidos.
- Capacitar a los usuarios finales sobre los procesos automatizados del sistema, el funcionamiento del mismo, su buen uso y verificar periódicamente la calidad de la información ingresada, procesada y generada.
- Abstenerse de realizar copias o reproducciones de la información del sistema, exceptuando las copias estrictamente necesarias y que tengan la autorización respectiva.

- Informar de forma inmediata y por escrito al Director Nacional de Tecnología de la Información y Comunicaciones, en caso de detectar irregularidades en la información, funcionamiento, y perfiles de usuario o permisos de acceso, en el sistema bajo su administración funcional.

Adicionalmente, el/la administrador/a funcional acepta que la o las credenciales que le sean otorgadas para acceso al sistema, son de uso personal e intransferible, cuya utilización es de su exclusiva responsabilidad. El/la administrador/a funcional se compromete a no divulgar dichas credenciales, incluso después de que haya terminado la relación laboral con la Contraloría General del Estado.

En caso de pérdida, olvido o sustracción de la o las credenciales de acceso que le sean otorgadas, deberá comunicar el hecho al Director Nacional de Tecnología de la Información y Comunicaciones de manera inmediata.

TERCERA. – SANCIONES

La Contraloría General del Estado se reserva la atribución de aplicar el régimen disciplinario previsto en el Reglamento Interno Sustitutivo de Administración de Talento Humano de la Contraloría General del Estado, ante el incumplimiento del presente Acuerdo.

El uso inadecuado, inapropiado y no autorizado de las herramientas informáticas y de la información de la Contraloría General del Estado conforme las disposiciones del "Reglamento de políticas de seguridad de la información y uso responsable de los recursos de tecnología de la información y comunicación de la Contraloría General del Estado" y el incumplimiento de los términos señalados en este instrumento, facultará a esta entidad el inicio de acciones administrativas, civiles y/o penales en contra del administrador funcional que incumpliere lo descrito en esta cláusula.

El/la administrador/a funcional acepta y declara de forma expresa que se somete a las responsabilidades y sanciones que le sean imputables, sin perjuicio del establecimiento de responsabilidades administrativas, civiles y/o penales.

CUARTA. – VIGENCIA

El presente Acuerdo de Confidencialidad tendrá vigencia durante el tiempo que el funcionario/a se mantenga como administrador/a funcional del sistema, y, por ética profesional, posteriormente a este tiempo incluso después de su salida de la Institución; sin perjuicio de la adopción de nuevas medidas de seguridad, las cuales serán automáticamente incorporadas y constituirán parte de este instrumento.

QUINTA. – ACEPTACIÓN

El/la administrador/a funcional conoce y acepta el contenido de todas y cada una de las cláusulas del presente acuerdo, y, en consecuencia, de manera voluntaria se compromete a cumplirlas en toda su extensión. Para constancia y fines legales pertinentes, se firman dos ejemplares del presente documento, con el mismo tenor y efecto, en la ciudad de (ciudad), el día (día del mes) del mes de (especificar mes) del año (año).

_____

(nombres y apellidos completos) **Cédula/pasaporte:** XXXXXXXXXX

ANEXO 5

ACUERDO DE CONFIDENCIALIDAD PARA EL USO DE HERRAMIENTAS TECNOLÓGICAS E INFORMACIÓN INSTITUCIONAL PARA LOS PASANTES Y/O PRACTICANTES EN LA CONTRALORÍA GENERAL DEL ESTADO

ANTECEDENTES:

Suscriben el presente Acuerdo de Confidencialidad los pasantes y/o practicantes de la Contraloría General del Estado (bajo cualquier modalidad), con el fin de establecer expresamente la responsabilidad del pasante y/o practicante, respecto del uso de los recursos informáticos de los que la institución dispone y que entrega a cada uno de sus pasantes y/o practicantes para el cumplimiento de sus funciones. En consecuencia, quienes forman parte de esta entidad al suscribirlo aceptan las limitaciones y restricciones de acceso a la información y divulgación de la misma.

El acceso a la información que los pasantes y/o practicantes de la Contraloría tienen para cumplir sus funciones es libre de acuerdo al nivel de competencia que desempeñen, por tanto, es preciso proteger la información constituida en patrimonio institucional. El uso indebido o ilegal de la información acarrearía consecuencias negativas en contra de los intereses institucionales y nacionales, por tanto, a partir de la firma de este Acuerdo de Confidencialidad, los pasantes y/o practicantes que haga mal uso de la misma o de los medios que la contienen, se someterán a las sanciones que las disposiciones legales y reglamentarias establecen para el efecto.

COMPROMISO

Considerando lo manifestado yo, (nombres y apellidos completos), de nacionalidad _____, mayor de edad, portador de cédula de identidad o ciudadanía, o pasaporte No. _____; en mi calidad de (pasante y/o practicante) de la Contraloría General del Estado, a través del presente documento acepto y me comprometo a guardar la confidencialidad en el tratamiento de la información respecto al ejercicio mis funciones, de conformidad con las siguientes cláusulas:

PRIMERA.- La Contraloría General del Estado posee una plataforma y sistemas informáticos debidamente registrados que conforman el patrimonio tecnológico de la entidad, constituidos por la plataforma informática, red de comunicación, dispositivos informáticos (hardware y software) y todos los demás recursos integrados con la tecnología de la información, que permiten el desarrollo diario de sus actividades, los cuales están a disposición limitada de todos los pasantes y/o practicantes, conforme sus funciones y las necesidades institucionales.

La Contraloría General del Estado, en el cumplimiento de su misión y de las disposiciones constitucionales y legales que regulan su actividad, crea información a través de sus diferentes procesos generadores de valor y habilitantes, información que es de su propiedad y el pasante y/o practicante acepta y reconoce tal calidad sin objeción alguna, por lo que el acceso a ésta es limitado y los pasantes y/o practicantes podrán acceder a la misma conforme a las necesidades de cada función y con las restricciones que al respecto señalan las normas legales, en especial la Ley Orgánica de Transparencia y Acceso a la Información Pública.

Se considera información de propiedad de la institución y de prohibida publicación y/o divulgación, toda clase de documentos, archivos e información que se encuentren en soportes físicos o electrónicos, así como registros, diagramas, flujogramas, dibujos, fotografías, disposiciones internas, memorándums, programas para computadora desarrollados al interior de la entidad, creaciones en multimedia o equipos digitales, logotipos, ideas, proyectos y en general toda clase de datos que se generen en la entidad, como parte de sus labores.

Conforme lo expuesto, el/la pasante y/o practicante _____, reconoce y acepta que toda la información es de propiedad de la entidad, salvo aquella que por su naturaleza es pública y se encuentra a disposición de la sociedad por intermedio del portal institucional.

El/la pasante y/o practicante reconoce y acepta además que todos los recursos informáticos que se encuentran definidos bajo el dominio “contraloria.gob.ec” son de propiedad exclusiva de la Contraloría General del Estado.

El/la pasante y/o practicante reconoce y acepta que el uso del correo electrónico de la Contraloría General del Estado y el acceso al servicio de Internet a través de la red interna, constituyen una herramienta que la entidad le otorga a fin de que pueda realizar sus labores, por lo que su uso, a más de estar limitado al ejercicio de las funciones de cada servidor/a, podrá ser restringido total o parcialmente sin previo consentimiento de aquel.

De ser dispuesta la medida de restricción total o parcial para los servicios de correo electrónico o de internet, o ambos a la vez, se comunicará al pasante y/o practicante para que pueda adoptar medidas de comunicación diferentes, a fin de cumplir con sus funciones.

Por ser el acceso a correo externo ilimitado, toda clase de información, documentos, comunicación o mensaje de datos enviado por esta vía, deben guardar cuidado con la imagen institucional, por lo que la Contraloría General del Estado adoptará las medidas necesarias para evitar daños en su imagen y fugas de información, sin que por ello se pueda alegar violación de privacidad.

El/la pasante y/o practicante acepta y reconoce que la información de la Contraloría General del Estado constituye un bien intangible invalorable, por lo que los riesgos por mal uso y/o divulgación indebida de la misma comportan que la entidad deba tomar medidas respecto de la integridad documental e informática.

El pasante y/o practicante se obliga a mantener y guardar confidencialidad y reserva respecto de la información relevante que le sea entregada para cumplir con sus labores, quedando prohibido divulgar por cualquier medio, distribuir, reproducir, traducir, utilizar, disponer y/o publicar la información que le haya sido proporcionada, que haya obtenido o que llegue a conocer por cualquier canal de comunicación institucional.

En el soporte informático que la institución proporcione a cada pasante y/o practicante, siempre que así se requiera para cumplir con sus funciones, éste/a podrá almacenar y mantener información personal, si la información no causa problemas a los sistemas de la entidad y si no supera el tamaño de almacenamiento que impida el normal funcionamiento del equipo.

Cada pasante y/o practicante será responsable de la asignación, uso y cuidado de sus claves de acceso a los sistemas informáticos, las cuales son personales e intransferibles, sin que se pueda alegar necesidades personales o institucionales, para divulgarlas por cualquier medio, permitiendo que otros servidores/as accedan a los sistemas con claves ajenas.

El/la pasante y/o practicante que ingrese información a las herramientas tecnológicas y de información que la Contraloría General del Estado le ha proveído para el desempeño y desarrollo de su trabajo, deberá asumir la responsabilidad de los datos ingresados procurando que los mismos sean veraces, coherentes y oportunos.

SEGUNDA.- El pasante y/o practicante se compromete a utilizar tanto la información documental como digital y los recursos tecnológicos de la Contraloría General del Estado, con ética, reserva y profesionalismo conforme las normas y reglamentos vigentes.

El/la pasante y/o practicante acepta que la Contraloría General del Estado puede ejercer control y seguimiento de la información institucional que esté bajo su custodia, así como de los recursos tecnológicos a él proporcionados, con la finalidad de garantizar el uso correcto de la información y los sistemas informáticos cuando lo estime pertinente y sin necesidad de notificación previa.

TERCERA.- La Contraloría General del Estado, previa autorización judicial y con la obligación de guardar en secreto la información para cuando sea necesario, podrá abrir, retener y examinar la correspondencia electrónica contenida en la cuenta individual de correo electrónico del pasante y/o practicante de la institución, que esté bajo el dominio “contraloría.gob.ec”, así como, la información electrónica que esté contenida en los recursos tecnológicos asignados.

CUARTA.- El uso inadecuado, inapropiado y no autorizado de las herramientas informáticas y de la información de la Contraloría General del Estado conforme las disposiciones del “Reglamento de políticas de seguridad de la información y uso responsable de los recursos de tecnología de la información y comunicación de la Contraloría General del Estado” y el incumplimiento de los términos señalados en este instrumento, facultará a esta entidad el inicio de acciones administrativas, civiles y/o penales en contra del pasante y/o practicante que incumpliere lo descrito en esta cláusula; y, será considerado como causal para la terminación unilateral del contrato o convenio de pasantía.

El/la pasante y/o practicante acepta y declara de forma expresa que se somete a las responsabilidades y sanciones que le sean imputables, sin perjuicio del establecimiento de responsabilidades administrativas, civiles y/o penales.

QUINTA.- El presente Acuerdo de Confidencialidad tendrá vigencia durante el tiempo que el/la pasante y/o practicante preste sus servicios a la Contraloría General del Estado; y, por ética profesional, posteriormente a su salida de la institución, sin perjuicio de la adopción de nuevas medidas de seguridad, las cuales serán automáticamente incorporadas y constituirán parte de este instrumento.

SEXTA. – El/la pasante y/o practicante conoce y acepta el contenido de todas y cada una de las cláusulas del presente acuerdo, y, en consecuencia, de manera voluntaria se compromete a cumplirlas en toda su extensión. Para constancia y fines legales pertinentes, se firman dos ejemplares del presente documento, con el mismo tenor y efecto, en la ciudad de (ciudad), el día (día del mes) del mes de (especificar mes) del año (año).

Atentamente,

_____

(nombres y apellidos completos)
Servidor/a de la (nombre de la Unidad Administrativa a la que pertenece)
Cargo:
Cédula y/o pasaporte:
Recibo una copia del presente documento

ANEXO 6

ACUERDO DE CONFIDENCIALIDAD DE LA INFORMACIÓN PARA LAS EMPRESAS CONTRATISTAS

El/la señor/a, (nombres y apellidos completos), de nacionalidad (nacionalidad), mayor de edad, portador de cédula de identidad o pasaporte No. (XXXXXXXXXX); en calidad de representante legal de la compañía/empresa (nombre de la empresa), que en adelante y para los efectos del presente instrumento se denominará "la contratista"; en virtud de la ejecución del contrato No. (número de contrato), cuyo objeto es (indicar objeto del contrato), suscrito el (indicar la fecha, día, mes y año de suscripción del contrato), de manera libre y voluntaria, suscribe el presente Acuerdo de Confidencialidad al tenor de las siguientes cláusulas:

PRIMERA. - OBJETO

La Contraloría General del Estado, en el cumplimiento de su misión y de las disposiciones constitucionales y legales que regulan su actividad, crea información a través de sus diferentes procesos generadores de valor y habilitantes, información que es de su propiedad y, la contratista acepta y reconoce tal calidad sin objeción alguna, por lo que, el acceso a ésta es limitado, y podrá acceder a la misma, conforme a las necesidades de ejecución del contrato correspondiente y con las restricciones que al respecto señalan las normas legales, en especial la Ley Orgánica de Transparencia y Acceso a la Información Pública.

Mediante el presente instrumento la contratista acepta y se obliga a guardar la debida confidencialidad, sobre toda la información que obtenga de la Contraloría General del Estado, incluyendo, pero no limitándose a: documentos, archivos, registros, diagramas, flujogramas, dibujos, fotografías, disposiciones internas, memorándums, programas para computadora desarrollados al interior de la entidad, creaciones en multimedia o equipos digitales, logotipos, proyectos, bases de datos, códigos fuente, credenciales de acceso, elementos sobre los cuales la Contraloría General del Estado sea titular de los derechos de autor, y, en general, toda clase de datos que se generen en la Contraloría General del Estado, como parte de sus labores. Esto engloba a información verbal, escrita, en medio físico o en medio digital, puesta a disposición de la contratista, y/o sus empleados, que estén directa o indirectamente relacionados con la ejecución del contrato.

Además, la contratista se compromete a hacer uso de la información recibida exclusivamente para la realización de actividades relacionadas a la ejecución del contrato, conforme a las obligaciones y prohibiciones legales pertinentes.

SEGUNDA. - CONTRASEÑAS DE ACCESO

La contratista acepta que las contraseñas o credenciales (nombre de usuario y contraseña) que le sean otorgadas, para acceso a sistemas en todos los ambientes de desarrollo, control de calidad o producción, bases de datos, y elementos de infraestructura tecnológica, según corresponda, son intransferibles y la utilización de las mismas es de su exclusiva responsabilidad.

La contratista se compromete a no divulgar, no revelar, las credenciales de acceso que le sean otorgadas, incluso después de que haya terminado la relación contractual con la Contraloría General del Estado.

TERCERA. – MANEJO DE INFORMACIÓN DE LA CONTRALORÍA GENERAL DEL ESTADO

La contratista se compromete expresamente a no revelar y/o proporcionar información de la Contraloría General del Estado a ningún tercero ajeno al contrato que ejecuta, por tanto, solo podrá transmitir dicha información a sus colaboradores directos, cuyos nombres deberán ser comunicados a la Contraloría General del Estado, y serán debidamente informados acerca de la naturaleza los términos confidenciales de la referida información y de los términos y condiciones del presente compromiso.

La información a la que pueda tener acceso la Contratista no podrá ser copiada o revelada a terceros por ningún medio, salvo que la Contraloría General del Estado así lo autorice expresamente por escrito. La Contratista tendrá la responsabilidad de informar a la Contraloría General del Estado si algún tipo de información se ha divulgado.

La Contratista no podrá tomar fotografías o grabar videos, a menos que tenga la autorización explícita para el efecto, proporcionada por la Contraloría General del Estado.

La Contraloría General del Estado podrá requerir a la contratista el retorno o devolución de la información confidencial en cualquier momento, mediante notificación escrita. En ese caso la Contratista devolverá toda la información confidencial original y destruirá todas las copias y reproducciones (ya sean escritas o electrónicas) que se encuentren en su poder.

CUARTA. – SANCIONES

El uso inadecuado, inapropiado y no autorizado de las herramientas informáticas y de la información de la Contraloría General del Estado conforme las disposiciones del “Reglamento de políticas de seguridad de la información y uso responsable de los recursos de tecnología de la información y comunicación de la Contraloría General del Estado” y el incumplimiento de los términos señalados en este instrumento, facultará a esta entidad el inicio de acciones administrativas, civiles y/o penales en contra del contratista que incumpliere lo descrito en esta cláusula.

El/la contratista acepta y declara de forma expresa que se somete a las responsabilidades y sanciones que le sean imputables, sin perjuicio del establecimiento de responsabilidades administrativas, civiles y/o penales.

QUINTA. – VIGENCIA

El presente Acuerdo de Confidencialidad y todos los términos establecidos en el mismo, se mantendrá vigente de manera indefinida a partir de la fecha de su suscripción, incluso después de que la contratista termine sus obligaciones contractuales con la Contraloría General del Estado.

SEXTA. – ACEPTACIÓN

La contratista conoce y acepta el contenido de todas y cada una de las cláusulas del presente Acuerdo de Confidencialidad y, en consecuencia, de manera voluntaria se compromete a cumplirlas en toda su extensión. Para constancia y fines legales pertinentes, se firman dos ejemplares del presente documento, con el mismo tenor y efecto, en la ciudad de (ciudad), el día (día del mes) del mes de (especificar mes) del año (año).

(nombres y apellidos completos)
Cédula/pasaporte: XXXXXXXXXX
Cargo:
Empresa:

ANEXO 7

FORMULARIO PARA SOLICITUD DE ACCESO REMOTO

SOLICITANTE			
Fecha de solicitud (DD/MM/AAAA)		**Lugar**	
Nombres y apellidos			
Cédula			
Unidad			
Entidad o empresa (Externos a CGE)			
Cargo			
Teléfono		**Correo electrónico**	
RECURSOS A LOS QUE SOLICITA EL ACCESO *(Detallar todos los requeridos)*			
Fechas desde		**Fechas hasta** (indicar si es indefinido)	
JUSTIFICACIÓN *(Detallar razones que justifiquen los permisos de acceso)*			
ACEPTACIÓN DE CONDICIONES			
• El acceso vía remota es exclusivamente para fines laborales, del ámbito de las funciones de el/la solicitante, y en beneficio de la Contraloría General del Estado. • Las credenciales y documentación relacionada que se otorgue para el acceso remoto es personal e intransferible. Todas las acciones que se realicen usando dichas credenciales son responsabilidad de el/la solicitante. • Las conexiones remotas hacia la red de la Contraloría General del Estado se realizarán mediante un equipo que cuente con un software de antivirus actualizado. • El acceso remoto que sea otorgado está sujeto a procedimientos de monitoreo y verificación de uso por parte de la DNTIyC. • En caso de detectarse actividades no autorizadas o en perjuicio de la Contraloría General del Estado, se aplicarán las medidas y sanciones pertinentes.			
FIRMAS DE RESPONSABILIDAD			
Solicitado por:		*Responsable de la Unidad:*	
Nombre: Cargo:		Nombre: Cargo:	

ANEXO 8

CONTRALORÍA GENERAL DEL ESTADO REGISTRO DE INGRESO Y SALIDA DE COMPUTADORES Y/O EQUIPOS INFORMÁTICOS									
N°	**FECHA**	**NOMBRES**	**APELLIDOS**	**INSTITUCIÓN**	**OCUPACIÓN**	**DETALLE DEL EQUIPO** (Laptop, Tablet, Número de Serie, etc.)	**UNIDAD ADMINISTRATIVA A LA QUE SE DIRIGE**	**HORA DE ENTRADA**	**HORA DE SALIDA**

ANEXO 9

GLOSARIO

Para efectos de aplicación del presente Reglamento se entenderán por:

- **Activo de información:** Cualquier elemento que contiene información ya sea esta física o digital y que tiene valor para la institución. Esto incluye todos los componentes relevantes en la generación, transmisión, procesamiento, almacenamiento, visualización, comunicación y recuperación de la información.
- **Confidencialidad:** Propiedad que garantiza que la información sea accesible solo para aquellas personas autorizadas a tener acceso a la misma.
- **Disponibilidad:** Propiedad que garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, cuando sea requerido.
- **Información:** un activo fundamental de las instituciones, en las formas que se manifieste sean estas: textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales y en cualquier medio sea, magnético, papel, electrónico, computadoras, audiovisual y otros.
- **Integridad:** Propiedad que salvaguarda la exactitud y totalidad de la información, en su procesamiento, transmisión y almacenamiento.
- **Seguridad de la información:** Mantenimiento de la confidencialidad, integridad y disponibilidad de la información institucional.
- **Sistema de información:** Conjunto de elementos de la organización que interactúan entre sí, y que sirven como soporte para el proceso de captación, transformación y comunicación de la información. Comprenden a las aplicaciones, servicios, activos de tecnología u otros componentes que permiten el manejo de la información.
- **Tecnologías de la información (TI):** término que engloba cuestiones propias de la informática, electrónica y las telecomunicaciones. Se relaciona al uso de equipos de telecomunicaciones y equipos de computación, para la transmisión, procesamiento y almacenamiento de datos.
- **Acceso remoto:** Característica que permite la conexión a recursos de TI a través de redes WAN privadas, o redes públicas como internet.
- **VPN:** Siglas de Virtual Private Network, o red privada virtual. Es un túnel seguro entre dos o más recursos. Las VPN se usan para proteger el tráfico privado que se transporta por Internet, brindando confidencialidad e integridad.
- **Autenticación:** Procedimiento informático que permite comprobar que alguien o algo, es realmente quien dice ser.
- **LDAP:** Siglas de Lightweight Directory Access Protocol o protocolo ligero de acceso a directorios. Constituye un conjunto de protocolos usados para acceder información guardada centralmente, organizada en una estructura jerárquica y categorizada, dentro de un directorio.

- **Credenciales:** Conjunto de nombre de usuario y contraseña, que constituye una identidad digital y es una forma de evidencia la certificación para el acceso a determinados elementos y la realización de actividades específicas.
- **Custodio administrativo:** Servidor/a delegado para la administración y control de activos fijos en cada unidad.
- **Usuario:** Cualquier persona que hace uso de los recursos y servicios de TI de la CGE, mediante una identidad en los sistemas de información.
- **Equipo informático:** Dispositivo electrónico que procesa información de forma automática. Incluye computadoras o cualquier tipo de dispositivo electrónico, que consiste en procesadores, memoria, medios de almacenamiento, etc.
- **Malware:** Expresión, que engloba a todo tipo de programa o código informático malicioso cuya función es dañar un sistema, causar un mal funcionamiento, o robar información; dentro de este conjunto se encuentran términos como: virus, troyanos, gusanos, keyloggers, botnets, ransomwares, entre otros.
- **Recurso informático:** Cualquier aplicación, herramienta, componente o dispositivo que se puede agregar a una computadora o sistema; por lo tanto, puede ser un recurso de hardware (dispositivos) o de software (programas)
- **Sniffer:** Software o aplicación de propósito específico para redes de datos, que permite como tal capturar los paquetes que viajan por una red.
- **Tecnologías de la información y Comunicación (TIC):** son el conjunto de medios y las aplicaciones que permiten la captura, procesamiento, almacenamiento, transmisión y presentación de la información.
- **Log:** Registro de actividad de un sistema que generalmente se guarda en un fichero de texto, al que se le van añadiendo líneas a medida que se realizan acciones sobre dicho sistema.
- **Respaldo (Backup):** Término en el ámbito de la tecnología y de la información, que define una copia de seguridad o el proceso de copia de seguridad. Backup se refiere a la copia y archivado de datos, de modo que pueda utilizarse para restaurar la información original en caso de que sea requerido.
- **Restauración (Restore):** Proceso de copiar datos de un respaldo o backup desde el almacenamiento secundario y restituirlos a su ubicación original o, a una nueva ubicación. Se realiza una restauración para devolver los datos perdidos, robados o dañados a su estado original o para mover los datos a una nueva ubicación.
- **Servidor de archivos (File server):** Recurso responsable del almacenamiento y administración centralizada de archivos e información, para que otros usuarios y equipos de la red autorizados puedan acceder a ella.

Oficio Nro. GMCM-ALC-2021-1084-OF

Macas, 14 de octubre de 2021

Asunto: FE DE ERRATAS ORDENANZA DE CREACIÓN DEL "BARRIO LA CORTE" DE LA PARROQUIA GENERAL PROAÑO",

Ingeniero
Hugo del Pozo B.
Director
REGISTRO OFICIAL
En su Despacho

De mi consideración:

Con el debido comedimiento solicito se sirva disponer la Publicación en el Registro Oficial, la **FE DE ERRATAS** de la "**ORDENANZA DE CREACIÓN DEL "BARRIO LA CORTE" DE LA PARROQUIA GENERAL PROAÑO**", aprobada por el Concejo Municipal del Cantón Morona, en sesiones ordinarias de fecha 15 de septiembre 2021 y 22 de septiembre de 2021 , y publicado en el Registro Oficial - Segundo Suplemento Nº 556, de fecha Martes 12 de octubre de 2021, en vista de que se ha cometido un error de redacción **FE DE ERRATAS**, en la parte de certificación dice: "(...Proveyó y firmó la ordenanza que antecede el Ing. Franklin Galarza Guzmán, Alcalde del Cantón Morona (…), debe decir: Proveyó y firmó la ordenanza que antecede la Sra. Nadia Sensú Tunki, Alcaldesa del Cantón Morona(S).

Con sentimientos de distinguida consideración.

Atentamente,

Firmado electrónicamente por:
RUTH ELIZABETH CABRERA SALAS

Abg. Ruth Elizabeth Cabrera Salas
SECRETARIA GENERAL DE CONCEJO

Ing. Hugo Del Pozo Barrezueta
DIRECTOR

Quito:
Calle Mañosca 201 y Av. 10 de Agosto
Telf.: 3941-800
Exts.: 3131 - 3134

www.registroficial.gob.ec

El Pleno de la Corte Constitucional mediante Resolución Administrativa No. 010-AD-CC-2019, resolvió la gratuidad de la publicación virtual del Registro Oficial y sus productos, así como la eliminación de su publicación en sustrato papel, como un derecho de acceso gratuito de la información a la ciudadanía ecuatoriana.

"Al servicio del país desde el 1º de julio de 1895"