Secretaría Nacional de Planificación y Desarrollo

ACUERDO No. SNPD-039-2013

PABEL MUÑOZ LÓPEZ
SECRETARIO NACIONAL DE PLANIFICACIÓN Y DESARROLLO (S)

Considerando:

Que, el artículo 227 de la Constitución de la República, dispone que: "La Administración Pública constituye un servicio a la colectividad que se rige por los principios de eficacia, eficiencia, calidad, jerarquía, desconcentración, descentralización, coordinación, participación, planificación, transparencia y evaluación.";

Que, el Reglamento General Sustitutivo para el Manejo y Administración de Bienes del Sector Público, expedido en el Registro Oficial No. 378 de 17 de octubre del 2006, norma entre otros aspectos, el manejo y utilización de los bienes de propiedad de los organismos y entidades del sector público;

Que, el Art. 3 del referido Reglamento General, señala que es obligación de la máxima autoridad de cada entidad u organismo, el orientar y dirigir la correcta conservación y cuidado de los bienes públicos que han sido adquiridos o asignados para uso y que se hallen en poder de la entidad a cualquier título: depósito, custodia, préstamo de uso u otros semejantes, de acuerdo con dicho Reglamento y las demás disposiciones que dicte la Contraloría General y el propio organismo o entidad;

Que, mediante Acuerdo No. 039-CG, publicado en el Suplemento del Registro Oficial No. 87 de 14 de diciembre de 2009, la Contraloría General del Estado, expidió las Normas de Control Interno para las Entidades, Organismos del Sector Público y Personas Jurídicas de derecho privado que dispongan de recursos públicos, atribuyendo a la Unidad de Tecnología de Información la definición, documentación y difusión de las políticas, estándares y procedimientos que regulen las actividades relacionadas con tecnología de información y comunicaciones en la organización;

Que, mediante Acuerdo No. 392-2010, publicado en el Suplemento del Registro Oficial No. 95 de 02 de diciembre de 2010, se expide el Estatuto Orgánico de Gestión Organizacional por Procesos de la Secretaría Nacional de Planificación y Desarrollo - SENPLADES, cuyo numeral 6.7.1.5.2 señala entre las atribuciones y responsabilidades de la Dirección de Información, Seguimiento y Evaluación Institucional de la Coordinación General de Planificación Institucional: "Diseñar, administrar y perfeccionar las políticas, procedimientos, planes y programas, relacionados a herramientas tecnológicas de gestión y de seguridad de la información, desprendidas de la planeación estratégica, para su coherente implementación institucional";

Que, mediante Acuerdo No. 639-2012 de 15 de octubre de 2012, se expiden las reformas al Estatuto Orgánico de Gestión Organizacional por Procesos de la SENPLADES, incorporando a los procesos habilitantes de asesoría, a la Coordinación General de Gestión Estratégica, conformada entre otras, por la Dirección de Tecnologías de Información y Comunicación, cuya misión es: "Planear y ejecutar proyectos y procesos de Tecnologías de la Información (TI) para la aplicación de políticas públicas y mejora de la gestión institucional y de los servicios a la ciudadanía, así como garantizar la operación de los sistemas y servicios informáticos, gestionar la seguridad informática, brindar soporte técnico en herramientas, aplicaciones, sistemas y servicios informáticos de la institución, e implementar la interoperabilidad con otras entidades.";

Que, la Disposición General Primera del Acuerdo No. 639-2012, señala que: "Todas las atribuciones, funciones y productos relacionados a la gestión de tecnologías de información y comunicación y de soporte tecnológico para la gestión institucional interna que conforme el Estatuto Orgánico de Gestión Organizacional por Procesos de la SENPLADES, se hallen asignadas a la Dirección de

Secretaría Nacional de Planificación y Desarrollo

Innovación Tecnológica de Sistemas de Información y de la Dirección de Servicios Administrativos y Soporte Tecnológico, y que se enmarquen en la misión determinada en el presente Acuerdo para la Coordinación General de Gestión Estratégica, serán cumplidas por la citada Coordinación General y sus respectivas Direcciones";

Que, es necesario determinar las políticas y normas que regulen la designación, uso y control de los bienes y servicios tecnológicos y de comunicación que dispone la Secretaría Nacional de Planificación y Desarrollo, de manera que se garantice su oportuna disponibilidad, optimización y calidad, así como la confidencialidad, integridad y disponibilidad de la información que manejen los servidores y usuarios externos de la Institución; y, en general para la prestación de servicios de tecnología para la participación y control institucional y ciudadano en las actividades de planificación del Estado a cargo de la SENPLADES; y,

En ejercicio de las atribuciones que le confiere el numeral 1 del Art. 154 de la Constitución de la República, Arts. 17 y 17.2 del Estatuto del Régimen Jurídico y Administrativo de la Función Ejecutiva, Art. 3 del Decreto Ejecutivo No. 1372, publicado en el Registro Oficial No. 278 de 20 de febrero de 2004; el literal w) del numeral 6.5.1. del Estatuto Orgánico de Gestión Organizacional por Procesos de la SENPLADES; y el Acuerdo No. SNPD-038-2013 de 30 de mayo de 2013,

ACUERDA:

EXPEDIR EL REGLAMENTO INTERNO PARA LA ASIGNACIÓN, USO Y CONTROL DE LOS SERVICIOS Y ACTIVOS DE TECNOLOGÍA DE INFORMACIÓN Y COMUNICACIONES Y SUS DERIVADOS DE LA SECRETARÍA NACIONAL DE PLANIFICACIÓN Y DESARROLLO SENPLADES

CAPÍTULO I
OBJETO, ÁMBITO Y POLÍTICAS

Art. 1.- Objeto.-El presente reglamento tiene por objeto regular la asignación, uso y control de los servicios y activos de tecnología de información y comunicaciones de la SENPLADES, que permita garantizar la confidencialidad, integridad y disponibilidad de la información que se procesa, intercambia, reproduce y conserva mediante el uso de tecnologías de la información.

Art. 2.- Ámbito de aplicación.- Las disposiciones del presente Reglamento serán observadas y cumplidas en forma obligatoria por todos/as los/as servidores/as y trabajadores/as de la SENPLADES y los usuarios finales definidos en las Políticas de Seguridad de la Información Institucionales, a quienes se les asigne el servicio o uso del bien.

Art. 3.- Políticas generales.- La Coordinación General de Planificación Institucional, a través del responsable de Seguridades de la Información, implementará las medidas preventivas y correctivas mediante las que se garantice la confidencialidad, integridad y disponibilidad de la información que se encuentra en poder de la Institución, de acuerdo a las leyes, normativas y estándares nacionales e internacionales creados para este fin, mediante la emisión de la Política de Seguridad de la Información, que deberá entre otros considerar los siguientes aspectos:

a) **Seguridad de los sistemas de información:** La Coordinación General de Planificación Institucional, a través del responsable de Seguridades de la Información, determinará las políticas, planes y programas a ser implementados en conjunto con la Dirección de Tecnologías de Información y Comunicación (DTIC), para proteger la información que mantienen los servicios, sistemas y aplicaciones, a fin de evitar pérdidas, uso indebido, acceso o divulgación no autorizada, alteraciones o destrucción de la misma.

b) **Confidencialidad:** Toda información que se genere en la SENPLADES, salvo aquella considerada como confidencial, es pública de acuerdo con la Ley Orgánica de Transparencia y Acceso a la

Información Pública LOTAIP. Para su acceso se establecerán los canales y mecanismos que aseguren su disponibilidad.

La determinación de confidencialidad que pudiere realizarse de la información que se obtenga de los servicios, aplicaciones y sistemas de información será difundida a través de los medios oficiales de comunicación de la SENPLADES, de manera que el/la usuario/a conozca en todo momento los cambios que se produzcan en la institución en el marco de la normativa vigente.

c) **Integridad:** La Coordinación General de Planificación Institucional, a través del responsable de Seguridades de la Información garantizará la protección e integridad de los activos tecnológicos e información de la SENPLADES.

Los servidores/as y ciudadanos/as autorizados/as, serán responsables del buen uso y manejo adecuado de la información asegurando su integridad, inalterabilidad y consistencia.

d) **Disponibilidad:** La SENPLADES garantizará el uso y la accesibilidad de la información a las entidades y usuarios/as autorizados/as, en los términos que lo requieran, y el acceso a la información a todos los ciudadanos/as, conforme lo establece la Ley Orgánica de Transparencia y Acceso a la Información Pública y su Reglamento.

e) **Respeto a los derechos de propiedad intelectual:** La SENPLADES respeta los acuerdos de software licenciado o suscrito. Por esto, se prohíbe el uso de recursos de internet y correo electrónico para emplear, copiar o distribuir software licenciado sin la debida autorización del fabricante.

De igual manera, la reproducción de materiales con derechos de autor a través de estos recursos, se debe realizar solamente con el permiso escrito del autor o dueño del documento, aspecto que deberá ser observado tanto por los servidores/as públicos/as como por los ciudadanos en general.

f) **Veracidad de la información:** Toda la información encontrada en internet debe ser considerada como no confiable en su totalidad hasta que se confirme por una fuente oficial. No existe un proceso de control de calidad en el internet, y una gran parte de su información puede estar desactualizada o ser inexacta. Será responsabilidad de los/as servidores/as públicos/as y de los/as ciudadanos/as en general verificar las fuentes de información que se consulte a través de internet, en forma previa a su utilización o divulgación.

g) **Riesgos:** La conectividad en servicios tecnológicos como internet y correo electrónico expone a la SENPLADES a nuevos riesgos que deben ser conocidos para salvaguardar los activos críticos de información.

El acceso no controlado del internet y correo electrónico por parte de los usuarios finales, deriva en el mal uso de los recursos. Actividades que pueden afectar negativamente la productividad e imagen institucional. Adicionalmente, la SENPLADES puede enfrentar pérdida de reputación y posibles acciones legales a través de otros tipos de mal uso de estos recursos.

La DTIC deberá ejecutar las medidas que fuesen necesarias, para prevenir los riesgos del acceso a los recursos tecnológicos asignados.

h) **Auditorías periódicas:** Periódicamente, al menos dos veces por año y sin previo aviso, el responsable de Seguridades de la Información, realizará auditorías internas sobre el uso de los servicios tecnológicos, a los responsables de brindar el servicio y a los usuarios finales definidos en las Políticas de Seguridad de la Información.

Los resultados que se obtengan de estas auditorías serán comunicados oficialmente por la Coordinación General de Planificación Institucional a la máxima autoridad de la Institución para de ser el caso disponga las acciones correctivas o disciplinarias a que hubiere lugar de acuerdo a las Políticas de Seguridad de la Información.

CAPÍTULO II
DEL ACCESO A LOS SERVICIOS DE TECNOLOGÍA

Art. 4.- Asignación del servicio.-El "Alta del Usuario/a" deberá ser solicitada por la Dirección de Administración del Talento Humano de la SENPLADES, a través de la Mesa de Servicios de Tecnología de la DTIC, la misma que se ejecutará por los responsables de la activación de los servicios, sistemas y aplicaciones de acuerdo a los procesos establecidos por la DTIC.

El acceso a los servicios de tecnología se realizará a través de una credencial de usuario, la misma que será entregada al servidor/a o trabajador/a una vez que la DTIC haya ejecutado el "Alta de Usuario/a". Los datos de autenticación y autorización de la cuenta creada, serán entregados únicamente al usuario final a través del procedimiento establecido para la entrega de claves por el responsable de Seguridades de la Información, otorgando al usuario la responsabilidad de todas las acciones que se generen desde esta cuenta y del correcto mantenimiento y confidencialidad absoluta de la contraseña entregada.

La Dirección de Administración del Talento Humano solicitará el "Alta del Usuario" en la forma que se establezca en las Políticas de Seguridad de la Información.

Art. 5.- Desactivación de los servicios.- La "Baja del Usuario/a" deberá ser solicitada por la Dirección de Administración del Talento Humano a la DTIC, en forma inmediata a la cesación de funciones o ausencia temporal del servidor/a.

La DTIC procederá con la Baja del Usuario de todos los servicios, sistemas y aplicaciones de acuerdo a los procesos establecidos para esta actividad, así como con el respaldo de la información necesaria del usuario/a de acuerdo a las Políticas de Seguridad de la Información.

Como medida preventiva, los administradores de sistemas, servicios y aplicaciones de la DTIC revocarán los privilegios que no sean utilizados durante el lapso de 45 días por los usuarios, informando de esta actividad al responsable de Seguridades de la Información para su registro y control. Estos sistemas, servicios y aplicaciones serán reactivados previa solicitud del jefe inmediato del servidor/a ingresada por Mesa de Servicios de Tecnología en caso que el servidor/a todavía se encuentre trabajando para la SENPLADES.

CAPÍTULO III
DEL SERVICIO DE TELEFONÍA MÓVIL Y FIJO

Art. 6.- De las políticas de uso y prohibiciones del teléfono celular y teléfonos fijos.- Para asegurar un buen uso de los servicios de tecnología de información, utilizados por los teléfonos institucionales el usuario deberá observar las siguientes políticas:

1. Utilizar el teléfono celular o fijo, para actividades relacionadas con sus labores.
2. Velar por el cuidado y mantenimiento del teléfono celular y fijo asignado.
3. No almacenar información sensible personal en el equipo celular tal como fotografías, información familiar, claves personales, etc., que puedan ser fácilmente sustraídas en caso de presentarse algún percance con el dispositivo.
4. Solicitar a través de la DTIC, la configuración de una clave de acceso para el teléfono celular, bloqueo automático y configuración de la red de internet de la SENPLADES en el equipo.
5. Respaldar bajo su exclusiva responsabilidad, la información almacenada que requiera en el teléfono celular, a través del software o aplicaciones propias de la marca del equipo. La DTIC realizará la capacitación requerida por los funcionarios, de manera inmediata a la entrega del dispositivo.
6. Realizar un restablecimiento a la configuración de fábrica del equipo celular al momento de realizar un cambio o entrega del teléfono al custodio de los bienes. En caso de desconocimiento del tipo de configuraciones deberá solicitar soporte técnico a la DTIC. El seguimiento de la adecuada configuración del teléfono estará a cargo de la DTIC.
7. No realizar descargas de aplicaciones móviles o archivos de sitios web catalogados como no confiables.

8. No realizar cambios en el software original del teléfono (ej. actualizaciones del sistema operativo). La DTIC se reserva el derecho de aplicar cualquier cambio que considere necesario para salvaguardar el buen funcionamiento del dispositivo. Si el dispositivo necesita actualizaciones de software esta actividad deberá ser solicitada a la DTIC.
9. Mantener la configuración del correo electrónico de la SENPLADES en el teléfono celular institucional que es de uso obligatorio. Se admitirá solo la configuración de una cuenta personal adicional en dicho dispositivo.

CAPÍTULO IV
DEL SERVICIO DE INTERNET Y SUS DERIVADOS

Art. 7.- Asignación general del servicio.-El acceso a internet será provisto a los/as servidores/as de la SENPLADES como una herramienta para que cumplan con las tareas y actividades laborales.

La DTIC garantiza el acceso a internet de todos los/as servidores/as de la SENPLADES y los usuarios finales, a excepción de aquellos que han sido sancionados por acciones u omisiones determinadas como mal uso conforme lo definan las Políticas de Seguridad de la Información.

Los navegadores de internet y otros utilitarios de software para navegación en internet, serán definidos por la DTIC, que entregará los equipos finales configurados con estas herramientas a los servidores/as de acuerdo a lo establecido en las Políticas de Seguridad de la Información.

Únicamente se habilitarán a través de la red de datos de la SENPLADES los servicios de navegación autorizados de acuerdo a las Políticas de Seguridad de la Información, en teléfonos celulares institucionales. No se habilitarán servicios de navegación a través de la red de datos de la SENPLADES en teléfonos celulares personales.

El responsable de Seguridades de la Información autorizará los servicios institucionales que deberán ser habilitados por la DTIC para acceso desde equipos móviles.

El responsable de Seguridades de la Información, a efectos de control del uso adecuado del recurso, podrá acceder a todas las categorías de navegación autorizadas, respetando el principio de privacidad y confidencialidad de la comunicación personal del usuario/a, con el fin de asegurar el cumplimiento de las Políticas de Seguridad de la Información.

Art. 8.- Asignación general del servicio a usuarios externos.- Previa solicitud de la autoridad responsable de la Unidad requirente a la DTIC, se podrá otorgar temporalmente derechos de navegación en computadoras de escritorio o portátiles que no sean parte de los activos tecnológicos de la SENPLADES, a personas que no sean servidores/as de la institución y que permanecerán en las institución por un periodo definido de tiempo, a efecto de garantizar su participación en talleres de capacitación, eventos de participación ciudadana u otros relacionados con la misión de la SENPLADES.

La DTIC asignará el perfil único de acceso y navegación para este tipo de usuarios de acuerdo a las Políticas de Seguridad de la Información.

La solicitud para el acceso de internet a terceros deberá realizarla la autoridad responsable de la Unidad, a través de la Mesa de Servicios de Tecnología, y la DTIC cumplirá el mismo proceso de validación, autorización y activación previsto para el "Alta de Usuario". La solicitud deberá realizarse con al menos 24 horas de anticipación, de manera que se disponga del tiempo necesario para implementar puntos de red y puntos eléctricos, así como para configurar los servicios de tecnología solicitados.

El servidor/a de la SENPLADES que haga las funciones de contraparte de usuarios finales externos que requieran el acceso a recursos institucionales, será el encargado y responsable de que los accesos se utilicen para el fin establecido y exclusivamente durante el tiempo autorizado.

Art. 9.- Aprobación del perfil de navegación.-El perfil de navegación del usuario/a será establecido por el responsable de Seguridades de la Información en coordinación con la Dirección de Administración del Talento Humano, de acuerdo al cargo y funciones que ostente el servidor/a en la Institución.

Art.10.- Remoción de privilegios.- La cuenta de usuario junto con el acceso a internet, telefonía y correo electrónico será suspendida a la terminación de la relación laboral o contractual, ausencia temporal del servidor/a por comisión de servicios a otra institución, licencias de estudios, cualquier causa que motive la ausencia prolongada del servidor/a; y, en el caso de mal uso comprobado de los servicios asignados, previa solicitud del jefe inmediato y el informe de la Unidad Administrativa de Talento Humano.

En el caso de cambio de funciones del usuario que implique una modificación de sus accesos, el perfil original asignado al usuario será deshabilitado. El jefe inmediato solicitará a la DTIC el cambio de categoría de navegación de acuerdo a las nuevas funciones asignadas.

Art. 11.- Del uso y control.- El servicio de internet deberá ser utilizado para el cumplimiento de tareas oficiales relacionadas con el cargo de cada servidor/a, actividades de capacitación, investigación y formación vinculadas con las responsabilidades personales e institucionales asignadas.

Las actividades de investigación con fines académicos o de formación del servidor, podrán realizarse luego de concluida la jornada laboral normal.

Art. 12.- Uso permitido de internet.- El acceso a internet será aprobado y provisto de acuerdo con las necesidades de la Institución, según los permisos y categorías de navegación siguientes:

a) **Permisos generales:** Se considera como uso general del internet las actividades de búsqueda y navegación que realice el/la servidor/a o usuario/a, relacionadas con los siguientes temas:

   - Comunicación entre servidores/as y/o con terceros asociados a procesos institucionales.
   - Investigación y revisión en sitios web que contengan información relacionada o pertinente al cumplimiento de los objetivos institucionales.
   - Sitios web gubernamentales que no representen riesgos para la seguridad de la información de la SENPLADES.

b) **Categorías de navegación:** En el marco de los permisos generales, el acceso a servicios de internet se otorgará conforme a la respectiva categoría de navegación.

De acuerdo al perfil de navegación definido por las necesidades institucionales y la función que desempeñen el servidor/a o usuario final en la Institución, se determinará la categoría de navegación.

La categoría de navegación se determinará en el respectivo formulario de acceso y no estará sujeta a modificación, salvo casos excepcionales debidamente justificados por la autoridad responsable de la respectiva Unidad y aprobados por el responsable de Seguridades de la Información de la SENPLADES o quien haga sus veces en las entidades operativas desconcentradas.

Las categorías de navegación autorizadas serán las siguientes:

Categoría 1: SENPLADES 1

No hay navegación.

Este es un perfil para usuarios que no requieren ningún tipo de acceso a internet (Ej. personal de seguridad, recepcionistas, etc.)

Categoría 2: SENPLADES 2

Está permitido navegar en las categorías: finanzas y bancos, entidades, organismos o empresas gubernamentales en general, sitios de educación, webmails (hotmail, yahoo, gmail, etc.) y la descarga de archivos con extensiones de documentación en general (pdf, xls, etc.)

Se bloquea las categorías de: contenido de adulto, potencialmente responsable (Ej. sitios de drogas, violencia, etc.), sitios catalogados como riesgo de seguridad, redes sociales, youtube y descarga de archivos ejecutables en general, mensajería instantánea, chat.

Este es un perfil para usuarios que requieren navegar en instituciones como el IESS, SRI, bancos, entidades gubernamentales.

También se aplica a proveedores y visitantes que por temas laborales requieran trabajar temporalmente con los recursos de internet de la SENPLADES para lo que se habilitará un periodo de caducidad de los usuarios creados para el acceso (Ej. proveedores de tecnología).

Para estos usuarios se garantiza un ancho de banda de 2Mbps compartido.

Categoría 3: SENPLADES 3

Está permitido navegar en las categorías: finanzas y bancos, entidades, organismos o empresas gubernamentales en general, sitios de educación, noticias y medios de comunicación, redes sociales, youtube, webmails (hotmail, yahoo, gmail, etc.) y la descarga de archivos con extensiones de documentación en general (pdf, xls, etc.)

Se bloquea las categorías de: contenido de adulto, potencialmente responsable (Ej. sitios de drogas, violencia, etc.), sitios catalogados como riesgo de seguridad, descarga de ejecutables en general, mensajería instantánea, chat.

Este es un perfil para usuarios que requieran monitorear medios de comunicación, videos, streaming. (Ej. Comunicación Social).

Para estos usuarios se garantiza un ancho de banda de 2Mbps compartido.

Categoría 4: SENPLADES 4

Está permitido navegar en las categorías: finanzas y bancos, entidades, organismos o empresas gubernamentales en general, sitios de educación, webmails (hotmail, yahoo, gmail, etc.) y la descarga de archivos, software autorizado, noticias y medios de comunicación.

Se bloquea las categorías de: contenido de adulto, potencialmente responsable (Ej. sitios de drogas, violencia, etc.), sitios catalogados como riesgo de seguridad, descarga de ejecutables en general, mensajería instantánea, chat.

Este es un perfil para usuarios de tecnología que requieran descarga de librerías, parches. (Ej. Administrador de redes y comunicaciones.)

Para estos usuarios se garantiza un ancho de banda de 2Mbps compartido.

Categoría 5: SENPLADES 5 JERÁRQUICO SUPERIOR

Está permitido navegar en las categorías: finanzas y bancos, entidades, organismos o empresas gubernamentales en general, sitios de educación, webmails (hotmail, yahoo, gmail, etc.) descargas de archivos, noticias y medios de comunicación, redes sociales, mensajería instantánea, videos (youtube).

Se bloquea las categorías de: contenido de adulto, potencialmente responsable (Ej. sitios de drogas, violencia, etc.), sitios catalogados como riesgo de seguridad, descarga de ejecutables.

Este perfil se aplicará únicamente al Nivel Jerárquico Superior de la SENPLADES que incluye:

- Secretario/a Nacional
- Subsecretarios/as Generales
- Subsecretarios/as Nacionales
- Subsecretario/a Zonales
- Coordinadores/as Generales
- Asesores y Gerentes de Proyectos Emblemáticos
- Directores directamente sujetos a la jerarquía del Secretario Nacional.

Para estos usuarios se garantiza un ancho de banda de 1Mbps compartido.

El ancho de banda garantizado para cada categoría de navegación podrá cambiar de acuerdo a las necesidades institucionales y a la disponibilidad de recursos.

Accesos excepcionales.

La DTIC de acuerdo con las necesidades institucionales y para efecto de comunicación oficial masiva podrá habilitar el acceso a redes sociales a los servidores/as de las distintas unidades administrativas en forma programada y previa solicitud aprobada por el responsable de Seguridades de la Información.

Art. 13.- De las prohibiciones para uso de internet.- El uso del servicio de internet estará sujeto a las siguientes prohibiciones:

No se utilizará el servicio de internet institucional para:

1. Acceder a información personal de terceros, salvo aquella necesaria para confirmar aspectos de capacidad legal, formación profesional o similar.
2. Intentar obtener sin autorización de la DTIC, otros privilegios de navegación o accesos que no estén asignados al servidor/a o usuario final.
3. Fines políticos, participación en cualquier forma de recolección de información interna no autorizada, participación en actividades fraudulentas, difusión de material falso, publicitario o difamatorio.
4. Acceder a páginas web que la DTIC catalogue en las Políticas de Seguridad como atentatorias a principios constitucionales y/o que podrían afectar negativamente la imagen institucional.
5. Acceder a información reservada de la institución que no esté vinculada a las funciones del/a servidor/a y sobre la cual no tenga autorización para consulta.
6. Revelar sin la debida autorización o alteración de información institucional o de terceros, esto incluye cambios no autorizados, compartir información digital o datos institucionales y/o de terceros sin autorización.
7. Redireccionar en forma deliberada los portales y aplicaciones institucionales a otros sitios de internet cuyo contenido puede ser inconsistente o violatorio de los objetivos o políticas de la SENPLADES.
8. Realizar cualquier tipo de pruebas, operaciones, o acciones en la red de la SENPLADES que no estén autorizadas por la DTIC que puedan generar un incidente de seguridad.
9. Instalar y/o configurar redes internas de datos en las instalaciones de la SENPLADES que no hayan sido diseñadas y autorizadas por la DTIC.
10. Fomentar cualquier conducta que pueda constituir delito o que viole regulaciones o leyes nacionales e internacionales o actividades que puedan ser objeto de demanda de los afectados.
11. Transmitir, duplicar o receptar voluntariamente material o documentos que violen los derechos de autor, marcas, secretos de marcas, o derechos de patente de cualquier persona u organización.
12. Crear, transmitir, duplicar, almacenar o receptar voluntariamente cualquier material ofensivo, difamatorio, ilegal, amenazante o de acoso, incluyendo pero no limitado, a comentarios basados en la raza, nacionalidad, etnia, género, estado civil, orientación sexual, edad, estado de salud, discapacidad, religión o creencias políticas.
13. Cualquier tipo de juego, apuestas, etc.
14. Descargar en forma no autorizada shareware o software no licenciado.

15. Realizar cualquier orden o compra/venta de artículos, bienes o servicios a través de internet que sean de tipo personal.
16. Reenviar cadenas de correos, cualquiera sea su naturaleza.
17. Aceptar o negar regalos promocionales en la red como rifas, etc.
18. Navegar en teléfonos celulares personales de los servidores/as en la red de la SENPLADES.

Art. 14.- De la racionalidad y seguridad del consumo.-El ancho de banda dentro de la SENPLADES para su conexión con internet es un recurso compartido y finito, por lo que los usuarios deben realizar esfuerzos razonables para usar este recurso de manera que no se afecten las operaciones y productividad de los sistemas, portales y aplicaciones institucionales, y/o no se afecte al resto de usuarios/as.

La DTIC establecerá guías y directrices en el uso, asignación, distribución de este recurso y podrá prohibir la descarga de tipos particulares de archivos que impliquen un riesgo de seguridad de acuerdo a lo establecido en las Políticas de Seguridad de la Información.

CAPÍTULO V
DEL SERVICIO DE CORREO ELECTRÓNICO INSTITUCIONAL

Art. 15.- De su uso oficial y obligatorio.- El correo electrónico institucional es una herramienta de comunicación proporcionada con el fin exclusivo de enviar y recibir mensajes por escrito. Constituye el medio virtual de comunicación de carácter oficial y de uso obligatorio para el tratamiento de asuntos laborales de los servidores/as de la SENPLADES.

Un correo electrónico es considerado como mensaje de datos de acuerdo a la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, por lo cual tendrá igual valor jurídico que un documento escrito.

Todo correo que sea enviado a través de la cuenta nombredelusuario@SENPLADES.gob.ec, será considerado como proveniente de la SENPLADES, pero su contenido es confidencial y propio del servidor/a asignado, siendo el único y exclusivo responsable del contenido enviado en el mensaje y de la información adjunta que se remita desde su cuenta.

Los servidores/as de la SENPLADES deberán mantener abierto su correo electrónico durante toda la jornada laboral, asegurando de esta forma su uso cotidiano y permanente como medio de comunicación institucional en línea.

Art. 16.- Capacidad y aseguramiento de envío y recepción.- La DTIC establecerá los límites de capacidad para los buzones de correo electrónico, de acuerdo a la capacidad de la infraestructura instalada y a las necesidades institucionales, con el objetivo de evitar el congestionamiento de la red de comunicaciones y garantizar la disponibilidad del servicio.

La DTIC bloqueará automáticamente la recepción de mensajes desde direcciones identificadas como spammers (individuos o empresas que envían correo no deseado), correo basura, código malicioso o cualquier otra que se catalogue como riesgosa.

Art. 17.- De las políticas para el buen uso del correo electrónico.- Para el buen uso del correo electrónico, el servidor/a deberá observar las siguientes políticas:

1. Utilizar el correo electrónico institucional exclusivamente para actividades laborales de los servidores/as.
2. Velar por mantener la confidencialidad del usuario y contraseña de red a través de los que accede a este recurso.

Art. 18.- De las prohibiciones para el uso del correo electrónico.- Para el buen uso del correo electrónico, el servidor/a deberá observar las siguientes prohibiciones:

1. No enviar información sensible por este medio, por cuanto se indica expresamente que los correos en texto plano no aseguran una comunicación confidencial, por tanto la DTIC no puede garantizar que las comunicaciones electrónicas no sean interceptadas.
2. No se utilizará el correo institucional para envío de correos masivos que puedan saturar la red.
3. No reenviar cadenas de mensajes con fines no institucionales.
4. No almacenar, usar o distribuir archivos considerados censurables y/o que puedan afectar al correcto funcionamiento de los sistemas y aplicaciones de la SENPLADES de acuerdo a las definiciones que realice la DTIC.
5. No divulgar información institucional a través del correo electrónico, cuya difusión deba ser autorizada conforme las Políticas de Seguridad de la Información.
6. No crear o distribuir cualquier mensaje discriminatorio, injurioso, doloso o de cualquier otra naturaleza que pueda afectar a la institución, sus servidores o cualquier persona o entidad, de acuerdo con la Constitución y la ley. En el caso de que un servidor/a reciba este tipo de correos deberá reportar esta novedad a su jefe inmediato, quien notificará al responsable de Seguridades de la Información y a la Dirección de Administración del Talento Humano, para que se tomen las acciones y de ser el caso, las sanciones pertinentes de acuerdo con la gravedad del hecho.
7. No abrir mensajes remitidos desde direcciones desconocidas o ejecutar archivos desconocidos adjuntados al correo de origen. Cuando se reciban este tipo de mensajes, el usuario/a final deberá borrarlo inmediatamente y reportar esta novedad a la DTIC para que ejecute las tareas de revisión e investigación pertinentes.
8. No utilizar la cuenta de correo institucional asignada para generar altas de usuarios en sitios web que no estén relacionados con las actividades laborales del servidor/a. En el caso de detectarse esta actividad, el usuario final deberá dar de baja la cuenta en el sitio web creado.

Art. 19.- Monitoreo del uso.- Periódicamente o a pedido de la autoridad responsable de cada Unidad Administrativa o del titular de la Coordinación General Administrativa Financiera, el responsable de Seguridades de Información realizará la verificación del correcto uso del correo electrónico institucional por parte de un usuario o de un grupo de usuarios, garantizando la privacidad de la información almacenada.

De igual forma, la DTIC podrá obtener respaldos periódicos de los buzones institucionales y/o realizar restauraciones de los buzones, de aquellos servidores/as que ya no pertenezcan a la institución, a solicitud de la autoridad responsable de la Unidad y exclusivamente con el fin de garantizar la disponibilidad de información institucional que permita dar continuidad a la gestión de la Entidad.

La responsabilidad del buen uso de la información recaerá en forma exclusiva en la autoridad que solicitó la información. Los archivos restaurados pasarán a formar parte del archivo institucional y serán utilizados exclusivamente para tareas de control posterior de seguridades.

Art. 20.- Confidencialidad del Correo Electrónico.- La DTIC de acuerdo a las necesidades institucionales, podrá proporcionar herramientas y software adicionales, que permitan garantizar la confidencialidad, integridad y disponibilidad de los mensajes enviados a través del correo electrónico institucional a sus destinatarios.

CAPÍTULO VI
DE LAS COMPUTADORAS ASIGNADAS A LOS SERVIDORES

Art. 21.- De su uso.- Las computadoras de propiedad de la SENPLADES, entregadas al servidor/a o a cualquier usuario final, deberán ser utilizadas únicamente para los fines relacionados con sus actividades laborales y con los objetivos y funciones institucionales.

El recurso asignado será responsabilidad del servidor/a o de la autoridad responsable de la unidad administrativa a la que se asigne el equipo tecnológico para usuarios/a finales externos.

La DTIC es la responsable de la determinación del equipo a ser entregado al servidor/a de acuerdo a sus funciones, de la distribución y entrega de las computadoras, configuración, registro y control,

independientemente del inventario actualizado de los equipos que conforman el parque informático de la institución que mantenga la Dirección Administrativa.

Los servidores/as de la SENPLADES y usuarios/as finales, no podrán realizar ningún tipo de cambio, alteración, modificación o actualización de los componentes de software y/o hardware instalado en el equipo entregado. De requerir alguna modificación ésta deberá ser solicitada a la Mesa de Servicios de Tecnología mediante correo electrónico para que esta unidad valide y autorice la ejecución de estos trabajos, asegurando su buen uso, asignación y control de acuerdo con las Políticas de Seguridad de la Información.

Art. 22.- Del software instalado en los equipos.- La DTIC será la responsable de mantener el inventario actualizado del software adquirido e instalado en los equipos tecnológicos del parque informático de la institución, así como de custodiar los medios habilitantes para su utilización.

La DTIC, determinará e instalará el software básico que será utilizado en los equipos tecnológicos institucionales de los servidores/as o usuarios/as finales. El software adicional que requieran los servidores/as o usuarios/as finales será proporcionado de acuerdo con la disponibilidad de licencias y previo análisis de las funciones específicas para las que se lo requiere.

Bajo ninguna circunstancia los servidores/as de la SENPLADES instalarán software que no se encuentre legalmente adquirido por la institución. La DTIC resolverá cualquier consulta sobre el software que se encuentra autorizado y que puede ser instalado en los equipos a través de la Mesa de Servicios de Tecnología.

Art. 23.-De las políticas de uso de las computadoras.- Para el uso de los equipos tecnológicos institucionales se deberán observar las siguientes políticas de uso:

1. Velar por el cuidado y mantenimiento del equipo asignado.
2. Guardar con las seguridades del caso los computadores portátiles y sus componentes para prevenir su pérdida, sustracción o daño.
3. Tomar todas las precauciones necesarias durante el transporte autorizado de los equipos tecnológicos para evitar golpes, caídas o sustracción de los mismos.
4. Solicitar autorización para el traslado del computador portátil asignado, fuera de la institución, al Jefe Inmediato del servidor/a, conforme el procedimiento que determine la Unidad Administrativa Responsable.
5. Reportar de manera inmediata en forma escrita al servidor responsable de la custodia general de bienes de la Entidad, al Jefe inmediato y a la máxima autoridad de la Institución, cualquier pérdida, sustracción o robo del equipo asignado al servidor/a o de cualquiera de sus componentes, con todos los pormenores que fueren del caso, dentro de las 48 horas siguientes al conocimiento del hecho, debiendo coordinar en las acciones legales que correspondan con la Coordinación de Asesoría Jurídica, o quien haga sus veces en las entidades operativas desconcentradas.
6. Usar los equipos en lugares limpios.
7. Evitar el contacto de los equipos con líquidos como café, agua, etc.
8. Conectar los equipos tecnológicos a tomas de energía reguladas marcadas como REGULADA (TER-CR-x). En caso que el usuario no contara con este tipo de toma, deberá solicitar a la DTIC su instalación. Esta unidad realizará la inspección y emitirá el informe en el que se defina la mejor alternativa técnica.
9. Bloquear la sesión de usuario del computador al ausentarse del puesto de trabajo.
10. Almacenar la información institucional en la ubicación asignada por la DTIC, que garantizará que la misma será respaldada en el sistema de respaldos digitales institucional de acuerdo al límite de capacidad establecido en las Políticas de Seguridad de la Información.
11. Activar las medidas y mecanismos de seguridad necesarias, previa a la conexión del equipo portátil institucional a redes externas para evitar la propagación de virus a la red institucional.
12. La DTIC no proporcionará accesos de administradores locales en los equipos tecnológicos de los servidores/as y usuarios finales al momento de la instalación. Cualquier requerimiento que implique esta elevación de privilegios deberá ser solicitado por correo electrónico a la Mesa de Servicios de Tecnología, que escalará la solicitud al responsable de Seguridades de Información de la Coordinación General de Planificación Institucional, quien realizará el análisis técnico y autorizará,

de ser pertinente, los accesos requeridos, para que sean configurados por la DTIC, de acuerdo a las atribuciones correspondientes.

13. Los equipos externos que no sean parte de los activos tecnológicos de la institución y que por razones plenamente justificadas requieran ingresar a la red de la SENPLADES, serán objetos de la aplicación de configuraciones y controles definidos por las Políticas de Seguridad de la Información, para asegurar que éstos no ocasionen incidentes de seguridad y exposición a riesgos a la red institucional.

Art. 24.-De las prohibiciones.- Para el uso de los equipos tecnológicos institucionales se deberán observar las siguientes prohibiciones:

1. No apoyar los equipos portátiles sobre el regazo u obstruir los orificios de ventilación.
2. No exponer los equipos a temperaturas altas o calor excesivo.
3. No cambiar la configuración de red establecida para el equipo.
4. No intentar elevar los privilegios del usuario creado para el uso del equipo a través de herramientas de terceros.

Art. 25.- Del control.- El responsable de Seguridades de la Información en conjunto con la DTIC verificará de manera periódica el uso adecuado de los recursos y reportará por escrito cualquier novedad a la Coordinación General Administrativa Financiera, para el trámite pertinente.

A partir de las acciones se control realizadas, la DTIC podrá proponer cambios y mejoras sobre las tecnologías utilizadas, para incorporarlas en el Plan Anual de Mantenimiento de Equipos Tecnológicos de la SENPLADES.

Art. 26.- De los respaldos de información.- Cada servidor/a o usuario/a final será responsable por la información almacenada en su computadora, y por tanto deberá solicitar en forma periódica, al menos semestralmente, a la DTIC que genere respaldos de la información relevante.

CAPÍTULO VII
DE LAS IMPRESORAS, COPIADORAS Y ESCÁNERES

Art. 27.- De su uso.- Las impresoras, copiadoras y escáneres deberán ser utilizadas solo en actividades y funciones institucionales.

Para el servicio de impresión, copiado y escaneado de documentos, los servidores/as deberán utilizar los equipos disponibles en red, en cada unidad administrativa, de acuerdo a la distribución que en función de la disponibilidad de equipos, realice la DTIC.

Únicamente el Secretario Nacional, Subsecretarios, Coordinadores y Directores directamente sujetos a la jerarquía de la máxima autoridad institucional, podrán disponer de equipos multifuncionales instalados en sus oficinas para el cumplimiento de actividades de la Unidad.

Art. 28.- Políticas de uso de los recursos de impresión, copiado y escaneado.- El servidor/a deberá observar las siguientes políticas para el uso de los recursos de impresión, copiado y escaneado:

1. Los equipos deben estar ubicados en sitios adecuados, evitando su exposición indebida a derrames de agua, humedad, sol, polvo o zonas que generen electricidad estática.
2. La DTIC será responsable de la manipulación y configuración técnica de los equipos.
3. Cumplir con las políticas y mecanismos que establezca la entidad para el uso adecuado de los recursos e insumos, en el marco de acciones de manejo sustentable y ambientalmente equilibrado.

CAPÍTULO VIII
DEL MANTENIMIENTO DE LOS EQUIPOS TECNOLÓGICOS Y CAPACITACIÓN

Art. 29.- Plan Anual de Mantenimiento de Equipos Tecnológicos.- La DTIC será responsable de la elaboración y ejecución del Plan Anual de Mantenimiento de Equipos Tecnológicos de la SENPLADES.

El Plan Anual de Mantenimiento de Equipos Tecnológicos incluirá el levantamiento de las necesidades tecnológicas de las unidades administrativas institucionales a efecto de implementar las modificaciones o correcciones técnicas necesarias o adquirir nuevas tecnologías, funcionalidades y controles que permitan garantizar el uso óptimo de recursos tecnológicos, y las acciones, correcciones o implementaciones que se deban realizar, conforme las mejores prácticas recomendadas por los fabricantes o proveedores de los equipos tecnológicos, para asegurar la optimización de recursos institucionales.

La ejecución del Plan Anual de Mantenimiento de Equipos Tecnológicos deberá realizarse considerando una mínima afectación en la disponibilidad de los servicios de tecnología y de las labores cotidianas de los servidores/as de la SENPLADES, de acuerdo a las Políticas de Seguridad de la Información.

Art. 30.- Capacitación.-La DTIC en coordinación con la Dirección de Administración del Talento Humano propondrá y ejecutará acciones de capacitación periódica al personal de la SENPLADES, sobre el uso autorizado, adecuado y razonable de los recursos y herramientas tecnológicas disponibles en la institución, a través de medios virtuales, presenciales o cualquier otro mecanismo de capacitación e inducción que se establezca en la Institución.

El responsable de Seguridades de la Información absolverá cualquier duda que tenga el usuario/a sobre la aplicación del presente Reglamento.

DISPOSICIONES TRANSITORIAS

PRIMERA: En el plazo de noventa días desde la expedición del presente Reglamento, la Coordinación General de Planificación Institucional elaborará el documento de las Políticas de Seguridad de la Información que será remitido para aprobación del Secretario Nacional.

SEGUNDA: En el plazo de noventa días desde la aprobación de las Políticas de Seguridad de la Información, la Dirección de Administración del Talento Humano, en coordinación con el responsable de Seguridades de Información, elaborará el documento técnico de determinación de perfiles y categorías de navegación de los cargos institucionales y otros usuarios/as finales definidos en la Política de Seguridad de la Información.

TERCERA: En el plazo de ciento veinte días desde la expedición del presente Reglamento, la DTIC presentará para la aprobación de la máxima autoridad un Plan de Capacitación a los servidores/as de la SENPLADES sobre el uso y control de las tecnologías y servicios brindados por la Institución.

DISPOSICIÓN FINAL: De la ejecución del presente Reglamento que entrará en vigencia a partir de la fecha de su suscripción, sin perjuicio de su publicación en el Registro Oficial, encárguense a los titulares de la Coordinación General de Planificación Institucional, la Coordinación General Administrativa Financiera; y; la Coordinación General de Gestión Estratégica de la SENPLADES.

Dado, en el Distrito Metropolitano de Quito, a los 04 días del mes de junio de 2013.

Comuníquese y publíquese.-

PABEL MUÑOZ LÓPEZ
SECRETARIO NACIONAL DE PLANIFICACIÓN Y DESARROLLO (S)

DML/AMM/AMG/TNA/VMR/SCM