

RESOLUCIÓN No. DP-DPG-DAJ-2018-0 020

Ernesto Pazmiño Granizo
DEFENSOR PUBLICO GENERAL

CONSIDERANDO:

QUE, según lo determina el artículo 191 de la Constitución de la República, la Defensoría Pública es un órgano autónomo de la Función Judicial, indivisible, con autonomía administrativa, económica y financiera.

QUE, la norma de control interno 410-10 emitida por la Contraloría General del Estado, para las entidades, organismos del sector público y personas jurídicas de derecho privado que dispongan de recursos públicos, estipula, que la Unidad de Tecnología de Información, establecerá mecanismos que protejan y salvaguarden contra pérdidas y fugas los medios físicos y la información que se procesa mediante sistemas informáticos.

QUE, con memorando No. DP-SGT-2018-0024-M, de 6 de febrero de 2018, el ingeniero Juan Francisco Espín, Subdirector de Gestión Tecnológica, solicita al Defensor Público General, se disponga a la Dirección Nacional de Asesoría Jurídica la elaboración de la Resolución de Políticas de Acceso a Internet.

QUE, mediante memorandos Nos. DP-DPR2-2018-0003-M de 8 de febrero de 2018 y, DP-DPR2-2018-0008-M de 7 de marzo de 2018, el abogado Andrés Sánchez López, Defensor Público Regional Centro Norte, encargado, emite criterios y solicita se proceda con la elaboración dicha resolución.

QUE, de acuerdo con el numeral 3 del artículo 288 del Código Orgánico de la Función Judicial, compete al Defensor Público General expedir, mediante resolución, reglamentos internos, instructivos, circulares, manuales de organización y procedimientos y cuanto instrumento se requiera para funcionar eficientemente.

En ejercicio de sus facultades constitucionales y legales,

RESUELVE:

Artículo 1.- Instaurar la política de acceso a internet para todos los funcionarios de la Defensoría Pública, conforme el Anexo 1 que forma parte integrante de esta resolución.

Artículo 2.- Delegar al Director Nacional de Gestión y Administración de Recursos, para que por intermedio de la Jefatura de Talento Humano y Capacitación de la Defensoría Pública, ejecute las acciones necesarias para la aplicación de las sanciones disciplinarias consideradas en la ley.



Artículo 3.- Disponer al Subdirector de Gestión Tecnológica, la difusión e implementación de la presente política, en la Defensoría Pública a nivel nacional.

Artículo Final.- La presente Resolución entrará en vigencia a partir de esta fecha y prevalecerá sobre cualquier otra norma de igual o inferior jerarquía que se le oponga.

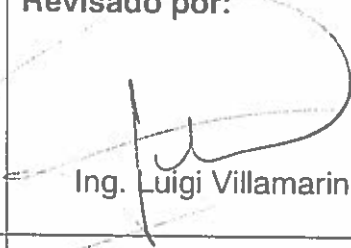
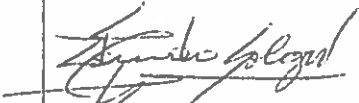
CÚMPLASE.-

Dada y firmada en la Defensoría Pública, en la ciudad de San Francisco de Quito, Distrito Metropolitano, el **20 MAR. 2018**


Dr. Ernesto Pazmiño Granizo
DEFENSOR PÚBLICO GENERAL



	SUBDIRECCIÓN DE GESTIÓN TECNOLÓGICA	Código: PL-SGT-006
	PROCESO DE SEGURIDAD DE TI	Versión: 01
	POLÍTICA DE ACCESO A INTERNET	Cláusula: 6.3
		Página 1 de 4

Elaborado Por:  Ing. Juan Francisco Espín	Revisado por:  Ing. Luigi Villamarín	Aprobado por:  Eco. Estuardo Salazar
Fecha: 01/02/2018	Fecha: 05/02/2018	Fecha: 21/02/2018



M/D

	SUBDIRECCIÓN DE GESTIÓN TECNOLÓGICA	Código: PL-SGT-006
	PROCESO DE SEGURIDAD DE TI	Versión: 01
	POLÍTICA DE ACCESO A INTERNET	Cláusula: 6.3
		Página 2 de 4

1. Objetivo

Establecer normas que aseguren el buen funcionamiento del internet, para optimizar y facilitar las labores de trabajo de los funcionarios de la Defensoría Pública.

2. Aplicación

La presente política aplica a todos los funcionarios, asesores, personal de contratistas, empleados temporales y terceros que usen equipos dentro de la Defensoría Pública o aquellos que accedan a internet de la institución.

3. Definiciones

3.1 Usuario: Persona que utiliza una computadora personal, tableta o portátil para realizar múltiples operaciones con aplicaciones, sistemas o plataformas.

3.2 Virus: Malware que tiene por objeto alterar el funcionamiento normal del ordenador, sin el permiso o el conocimiento del usuario. Los virus, habitualmente, reemplazan archivos ejecutables por otros infectados con el código de este. Los virus pueden destruir, de manera intencionada, los datos almacenados en una computadora, aunque también existen otros más inofensivos que solo se caracterizan por ser molestos.

3.3 Spam: es la denominación del correo electrónico no solicitado que recibe una persona. Dichos mensajes, también llamados correo no deseado o correo basura, suelen ser publicidades de toda clase de productos y servicios.

4. Referencias

Normativa de Contraloría:

- 410.04 Políticas y Procedimientos
- 410.10 Seguridad de Tecnología de Información.
- Estatuto Orgánico de Gestión Organizacional por Procesos

5. Responsables

El Subdirector de Gestión Tecnológica, de elaborar y actualizar la presente política.

M/L

	SUBDIRECCIÓN DE GESTIÓN TECNOLÓGICA	Código: PL-SGT-006
	PROCESO DE SEGURIDAD DE TI	Versión: 01
	POLÍTICA DE ACCESO A INTERNET	Cláusula: 6.3
		Página 3 de 4

El Director de Gestión de Calidad, de revisar la presente política.

El Director Nacional de Gestión y Administración de Recursos, de aprobar la presente política.

De velar por el cumplimiento de la política son el Jefe de Redes e Infraestructura y los Analistas de TI.

6. Política

Sobre el uso de Internet

Los privilegios de uso de Internet estarán limitados por la necesidad de acceso que requiera el desarrollo de la función de cada usuario.

Para los funcionarios de la Defensoría Pública, que requieran permisos de navegación o accesos a un determinado servicio; debe realizar la Solicitud para habilitar permisos de navegación o accesos a servicios aprobada por el jefe de departamento como se establece en el procedimiento PR-SGT-019.

Se podrán otorgar derechos de acceso a personas ajenas a la Defensoría Pública, siempre y cuando la Solicitud para habilitar permisos de navegación o accesos a servicios haya sido aprobada por el jefe de departamento en el que trabajarán. Estos derechos tendrán una vigencia de 30 días o menos, pero podrán ser extendidos, previa solicitud del jefe de departamento respectivo. Dicha solicitud estará publicada en la base de conocimientos de la mesa de servicios de TI (<http://soporte.defensoria.gob.ec/kb/faq.php?cid=6>).

Sobre el uso adecuado de internet

Debe entenderse que el acceso a Internet en las dependencias de la Defensoría Pública responde a la utilización de una herramienta de uso estrictamente laboral. Para estos efectos, cualquier propósito ajeno a las funciones estrictamente laborales será restringido.

Sobre el mal uso del internet

MJM

- Está estrictamente prohibido el ingreso a Páginas Web con contenido pornográfico.

	SUBDIRECCIÓN DE GESTIÓN TECNOLÓGICA	Código: PL-SGT-006
	PROCESO DE SEGURIDAD DE TI	Versión: 01
	POLÍTICA DE ACCESO A INTERNET	Cláusula: 6.3
		Página 4 de 4

- No se permitirá el uso del denominado "CHAT" en ningún horario a menos que su jefe directo lo autorice.
- El usuario no debe descargar ningún programa o software, sin la debida autorización, tales como: Ultrasurf, Psiphon, extensiones de navegadores web (Hola), etc.
- El usuario no debe instalar ningún programa para reproducir videos o emisoras de televisión vía Internet. (REAL AUDIO, BWV, etc.), dado que estos no poseen licencia para su uso.
- El usuario no debe abrir, ni revisar correos electrónicos considerados inseguros, debido al riesgo de contener mensajes de dudosa procedencia o archivos contaminados con virus que perjudique el equipo en uso, propiedad de la Defensoría Pública y que puedan afectar a la red institucional.
- No se debe usar Internet para realizar llamadas internacionales personales. Sólo los usuarios autorizados podrán realizar video conferencias de acuerdo a la descripción de sus funciones y necesidades del Servicio para el que responde.
- Se prohíbe cualquier tipo de transmisión vía Internet que no se autorizada (escuchar música y ver vídeo).

Sobre las Sanciones

Si el personal de TI detecta el uso inadecuado de internet o que un funcionario está utilizando un programa o aplicativo que permita evadir los controles de seguridad, notificara a la Jefatura de Talento Humano con las debidas pruebas para las sanciones pertinentes.

7. Registros

Solicitud para habilitar permisos de navegación o accesos a servicios

8. Anexos

NA

9. Histórico de Documentos

Versiones realizadas:

V01: Versión inicial

MIA