

RESOLUCIÓN No. 009-NG-DINARDAP-2012**EL DIRECTOR NACIONAL DE REGISTRO DE DATOS PÚBLICOS****CONSIDERANDO:**

Que el numeral noveno del artículo 11 de la Constitución de la República del Ecuador, determina que el más alto deber del Estado consiste en respetar y hacer respetar los derechos garantizados en ella;

Que el acceso a la información pública es un derecho consagrado en el artículo 18 de la Carta Magna: *“Todas las personas, en forma individual o colectiva, tienen derecho a: (...) 2. Acceder libremente a la información generada en entidades públicas, o en las privadas que manejen fondos del Estado o realicen funciones públicas. No existirá reserva de información excepto en los casos expresamente establecidos en la ley...”*;

Que el artículo 66 de la Norma Suprema señala: *“Se reconoce y garantizará a las personas: (...) 19. El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley. (...) 25. El derecho a acceder a bienes y servicios públicos y privados de calidad, con eficiencia, eficacia y buen trato, así como a recibir información adecuada y veraz sobre su contenido y características...”*;

Que el artículo 227 de la Constitución establece 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, transparencia y evaluación;

Que el literal a) del artículo 4 de la Ley Orgánica de Transparencia y Acceso a la Información Pública, sobre los principios de aplicación, estipula que la información pública pertenece a los ciudadanos y el Estado y las instituciones privada depositarias de archivos públicos, son sus administradores y están obligados a garantizar el acceso a la información;

Que el artículo 10 de la misma ley determina que: *“Es responsabilidad de las instituciones públicas, personas jurídicas de derecho público y demás entes señalados en el artículo 1 de la presente Ley, crear y mantener registros públicos de manera profesional, para que el derecho a la información se pueda ejercer a plenitud, por lo que, en ningún caso se justificará la ausencia de normas técnicas en el manejo y archivo de la*

información y documentación para impedir u obstaculizar el ejercicio de acceso a la información pública, peor aún su destrucción. Quienes administren, manejen, archiven o conserven información pública, serán personalmente responsables, solidariamente con la autoridad de la dependencia a la que pertenece dicha información y/o documentación, por las consecuencias civiles, administrativas o penales a que pudiera haber lugar, por sus acciones u omisiones, en la ocultación, alteración, pérdida y/o desmembración de documentación e información pública. Los documentos originales deberán permanecer en las dependencias a las que pertenezcan, hasta que sean transferidas a los archivos generales o Archivo Nacional...”;

Que el artículo 31 de la Ley del Sistema Nacional de Registro de Datos Públicos, señala entre otras, las siguientes atribuciones y facultades a la Dirección Nacional de Registro de Datos Públicos: “1.- *Presidir el Sistema Nacional de Registro de Datos Públicos, cumpliendo y haciendo cumplir sus finalidades y objetivos; 2.- Dictar las resoluciones y normas necesarias para la organización y funcionamiento del sistema...*”;

Que mediante Acuerdo Ministerial No. 0126, de 28 de febrero de 2011, el Ing. Jaime Guerrero Ruiz, Ministro de Telecomunicaciones y de la Sociedad de la Información, designó al doctor Willians Saud Reich, Director Nacional de Registro de Datos Públicos;

En ejercicio de las facultades que le otorga el artículo 31 de la Ley del Sistema Nacional de Registro de Datos Públicos, resuelve expedir el siguiente:

INSTRUCTIVO PARA EL MANEJO DE CONTRASEÑAS PARA EL INGRESO AL SERVICIO DATO SEGURO

Art. 1.- Objeto.- El presente Instructivo tiene por objeto normar el manejo de contraseñas por parte de los usuarios del servicio “Dato Seguro” que provee la Dirección Nacional de Registro de Datos Públicos.

Art. 2.- Ámbito.- Esta norma rige para todos los usuarios del servicio “Dato Seguro”.

Art. 3.- Características de la contraseña.- Toda contraseña debe cumplir con las siguientes características:

- a) Contener mínimo nueve caracteres.
- b) Tener entre los caracteres al menos dos letras mayúsculas, cuatro números, dos signos especiales (*-+()#\$%&/()=?|”@) y letras minúsculas.
- c) No estar relacionada con: el nombre, número telefónico, fecha de

WSD
Eury

nacimiento, nombre de miembros de su familia, situación personal que permita su fácil identificación, etc.

d) Nunca dejar en blanco la contraseña.

e) No ser una contraseña que haya sido anteriormente registrada.

Art. 4.- Confidencialidad.- Los usuarios de este servicio serán responsables del manejo y confidencialidad de sus contraseñas.

Art. 5.- Bloqueos.- Luego de tres intentos erróneos al momento de ingresar la contraseña, el servicio bloqueará automáticamente la cuenta de usuario, y enviará un correo electrónico con un enlace para su correspondiente desbloqueo.

Art. 6.- Vigencia.- La contraseña tendrá una vigencia de tres meses, el servicio solicitará de forma automática el cambio de contraseña.

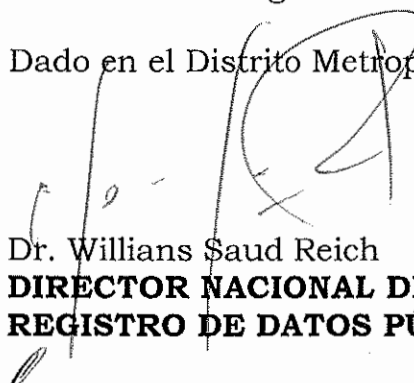
Art. 7.- Olvido o pérdida de contraseña.- El usuario que requiera una nueva contraseña, por pérdida u olvido de la misma, podrá acceder a la opción "Olvido de Contraseña" del portal del servicio de Dato Seguro, y el sistema enviará automáticamente un correo electrónico con un enlace y el código de seguridad aleatorio. El requirente deberá acceder al enlace y digitar el código para que pueda realizar el cambio de contraseña e imagen de seguridad.

Art. 8.- Olvido de usuario.- En caso que el ciudadano haya olvidado su usuario, deberá acceder a la opción "Olvido de Usuario", la cual a través de correo electrónico, enviará el nombre de usuario para ingresar al servicio.

Art. 9.- Responsabilidades del Director de Seguridad Informática.- El Director de Seguridad Informática es el responsable de vigilar el cumplimiento del presente Instructivo. De igual forma tendrá la potestad de designar un funcionario de su Dirección para que actúe como su delegado.

Disposición final.- Encárguese la ejecución de la presente Resolución al Director de Seguridad Informática.

Dado en el Distrito Metropolitano de Quito, el 3 de mayo de 2012



Dr. Willians Saud Reich
**DIRECTOR NACIONAL DE
REGISTRO DE DATOS PÚBLICOS**