En ejercicio de las atribuciones conferidas en el numeral 1 del artículo 154 de la Constitución de la República del Ecuador y los artículos 17 y 55 del Estatuto del Régimen Jurídico Administrativo de la Función Ejecutiva,

Acuerda:

Artículo 1.- Delegar al señor Embajador del Ecuador en los Estados Unidos Mexicanos, Excmo, Leonardo Arízaga Schmegel, para que a nombre y representación del Ministro del Interior, suscriba el Convenio de Cooperación de relacionamiento migratorio entre el Ministerio del Interior de la República del Ecuador y la República de México, cuyo objeto es el intercambio de información migratoria entre la Policía Nacional y Servicios Migratorios de ambas partes, con el fin de implementar mecanismos que faciliten la movilidad internacional de personas.

Artículo 2.- El delegado, informará al Ministro del Interior de las acciones adoptadas en ejercicio de la presente delegación.

Artículo 3.- El presente Acuerdo Ministerial, se pondrá en conocimiento de la Secretaría Nacional de la Administración Pública y del Ministro de Relaciones Exteriores y Movilidad Humana y entrará en vigencia a partir de su suscripción, sin perjuicio de su publicación en el Registro Oficial.

COMUNÍQUESE y PUBLÍQUESE.- Dado en Quito, Distrito Metropolitano, a 26 de octubre del 2016.

f.) José Ricardo Serrano Salgado, Ministro del Interior.

MINISTERIO DEL INTERIOR.- Certifico que el presente documento es fiel copia del original que reposa en el archivo de la Dirección de Secretaría General de este Ministerio al cual me remito en caso necesario.- Quito a, 14 de noviembre del 2016.- f.) Secretaría General.

Nº 044-NG-DINARDAP-2016

LA DIRECTORA NACIONAL DE REGISTRO DE DATOS PÚBLICOS

Considerando:

Que, el numeral 25 del artículo 66 de la Constitución de la República del Ecuador reconoce y garantiza a las personas: "*El derecho a acceder a bienes y servicios públicos y privados de calidad, con eficiencia, eficacia, buen trato, así como a recibir información adecuada y veraz sobre su contenido y características*";

Que, el artículo 66 de la Norma Fundamental, en su numeral 19, establece: "*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*"; por su parte, en su numeral 25, prescribe: "*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*"; y, en su numeral 28, dispone: "*El derecho a la identidad personal y colectiva, que incluye tener nombre y apellido, debidamente registrados y libremente escogidos; y conservar, desarrollar y fortalecer las características materiales e inmateriales de la identidad, tales como la nacionalidad, la procedencia familiar, las manifestaciones espirituales, culturales, religiosas, lingüísticas, políticas y sociales*";

Que, el artículo 227, de la norma suprema, indica 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, la Ley del Sistema Nacional de Registro de Datos Públicos, promulgada en el Registro Oficial Suplemento No. 162 de 31 de marzo del 2010, tiene el carácter de orgánica de conformidad con la Ley publicada en el Registro Oficial Segundo Suplemento No. 843 de 3 de diciembre de 2012;

Que, el artículo 3 de la referida Ley dispone que los datos públicos registrales deben ser: "*(...) completos, accesibles, en formatos libres, sin licencia alrededor de los mismos, no discriminatorios, veraces, verificables y pertinentes en relación al ámbito y fines de su inscripción (...)*";

Que, El artículo 4 de la ley citada determina: "*Las instituciones del sector público y privado y las personas naturales que actualmente o en el futuro administren bases o registros de datos públicos, son responsables de la integridad, protección y control de los registros y bases de datos a su cargo. Dichas instituciones responderán por la veracidad, autenticidad, custodia y debida conservación de los registros. La responsabilidad sobre la veracidad y autenticidad de los datos registrados, es exclusiva de la o el declarante cuando esta o este provee toda la información (...)*";

Que, el artículo 31 de la Ley del SINARDAP determina las atribuciones y facultades de la Dirección Nacional de Registro de Datos Públicos, entre las cuales están: "*1. Presidir el Sistema Nacional de Registro de Datos Públicos, cumpliendo y haciendo cumplir sus finalidades y objetivos; 2. Dictar resoluciones y normas necesarias para la organización y funcionamiento del sistema; (...) 5. Consolidar, estandarizar y administrar la base única de datos de todos los Registros Públicos, para lo cual todos los integrantes del Sistema están obligados a proporcionar información digitalizada de sus archivos, actualizada y de forma simultánea conforme ésta se produzca (...)*";

Que, el artículo 2 del Reglamento a la Ley del Sistema Nacional de Registro de Datos Públicos determina: "*El Sistema Nacional de Registro de Datos Públicos.- Está conformado por las Instituciones públicas y privadas*

determinadas en la Ley Orgánica del Sistema Nacional de Registro de Datos Públicos, y las que en el futuro determine, mediante resolución, el Director Nacional de Registro De Datos Públicos, en ejercicio de sus competencias";

Que, el artículo 6 del mencionado Reglamento indica: *"Los entes del sistema, además de las atribuciones y funciones previstas en sus propias leyes, tienen las siguientes: 1.- Acatar y observar las resoluciones y disposiciones que expida la Dirección Nacional de Registro de Datos Públicos para la interconexión e interoperabilidad de las bases de datos, sistemas, aplicaciones o componentes tecnológicos, para el correcto funcionamiento de la plataforma del Sistema; 2.- Almacenar, conservar, custodiar, usar, velar por la seguridad e integridad de la información que se mantiene en sus registros; y, 3.- Proporcionar información veraz y actualizada mediante la interoperabilidad de los datos o registros que se generen en su actividad, debiendo cumplir las resoluciones que para el efecto dicte la Dirección Nacional"*;

Que, el artículo 9 del referido documento determina que: *"Sin perjuicio de las competencias que ejercen los entes de control, definidos en la Constitución de la República, la Dirección Nacional de Registro de Datos Públicos es el órgano de regulación, control, auditoría y vigilancia de todos los integrantes del Sistema Nacional de Registro de Datos Públicos en torno a la interoperabilidad de datos. La regulación, control, auditoría y vigilancia comprenden todas las acciones necesarias para garantizar la disponibilidad del servicio. Las decisiones administrativas internas de cada ente registral corresponden exclusivamente a sus autoridades, pero la Dirección Nacional de Registro de Datos Públicos arbitrará las medidas que sean del caso cuando perjudiquen la disponibilidad de los servicios"*;

Que, el artículo 1 del Decreto Ejecutivo No. 1384 del 13 de diciembre de 2012, publicado en el Registro Oficial Segundo Suplemento No. 86, del 2 de enero de 2013, dispone: *"Establecer como política pública, el desarrollo de la interoperabilidad gubernamental, que consiste en el esfuerzo mancomunado y permanente de todas las entidades de la Administración Central, dependiente e institucional para compartir e intercambiar entre ellas, por medio de las tecnologías de la información y comunicación, datos e información electrónicos que son necesarios en la prestación de los trámites y servicios ciudadanos que prestan las entidades, así como en la gestión interna e interinstitucional"*;

Que, es menester expedir una Norma Técnica de Interoperabilidad, para que se regulen los aspectos técnicos en el intercambio de información a través de la plataforma del SINARDAP, tanto para las fuentes de dicha información, ya sean propias o externas, como para los consumidores;

Que, mediante Acuerdo Ministerial No. 003-2015, del 16 de enero de 2015, publicado en el Registro Oficial No. 447, del 27 de febrero de 2015, el Ministro de Telecomunicaciones y de la Sociedad de la Información, ingeniero Augusto Espín Tobar, nombró a la infrascrita, abogada Nuria Butiñá Martínez, como Directora Nacional de Registro de Datos Públicos.

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

NORMA TÉCNICA DE INTEROPERABILIDAD DEL SISTEMA NACIONAL DE REGISTRO DE DATOS PÚBLICOS

Art. 1.- Ámbito: La presente norma deberá ser cumplida por todas las instituciones consideradas como proveedoras y consumidoras ahora y en el futuro de información de la plataforma SINARDAP.

Art. 2.- Objetivo: Establecer la norma técnica de interoperabilidad y estándares de los servicios de información que ofrece la Plataforma SINARDAP y definir los mecanismos tecnológicos que la plataforma considera para integrar a una nueva fuente de datos (proveedor)

Art. 3.- Glosario.- Para efectos de la presente norma, apliquese los siguientes conceptos:

SINARDAP: Sistema Nacional de Registro de Datos Públicos, creado en base a la Ley, cuyo objetivo es garantizar la seguridad jurídica, organizar, regular, sistematizar e interconectar la información, así como: la eficacia y eficiencia de su manejo, su publicidad, transparencia, acceso e implementación de nuevas tecnologías.

VPN IPSEC: IPsec (abreviatura de Internet Protocol security) es un conjunto de protocolos cuya función es asegurar las comunicaciones sobre el Protocolo de Internet (IP) autenticando y/o cifrando cada paquete IP en un flujo de datos. IPsec también incluye protocolos para el establecimiento de claves de cifrado.

SLA (ANS): Un acuerdo de nivel de servicio o ANS (en inglés Service Level Agreement o SLA), es un acuerdo escrito entre un proveedor de servicio y su cliente con objeto de fijar el nivel acordado para la calidad de dicho servicio. El ANS es una herramienta que ayuda a ambas partes a llegar a un consenso en términos del nivel de calidad del servicio, en aspectos tales como tiempo de respuesta, disponibilidad horaria, documentación disponible, personal asignado al servicio, etc.

XML: siglas en inglés de eXtensible Markup Language ("lenguaje de marcas Extensible"), es un meta-lenguaje que permite definir lenguajes de marcas desarrollado por el World Wide Web Consortium (W3C) utilizado para almacenar datos en forma legible. Proviene del lenguaje SGML y permite definir la gramática de lenguajes específicos (de la misma manera que HTML es a su vez un lenguaje definido por SGML) para estructurar documentos grandes

WSDL: WSDL son las siglas de Web Services Description Language, un formato XML que se utiliza para describir servicios Web . La versión 1.0 fue la primera recomendación por parte del W3C y la versión 1.1 no alcanzó nunca tal estatus. La versión 2.0 se convirtió en la recomendación actual por parte de dicha entidad.

WSDL describe la interfaz pública a los servicios Web. Está basado en XML y describe la forma de comunicación, es decir, los requisitos del protocolo y los formatos de los mensajes necesarios para interactuar con los servicios listados en su catálogo. Las operaciones y mensajes que soporta se describen en abstracto y se ligan después al protocolo concreto de red y al formato del mensaje.

XSD: XML Schema es un lenguaje de esquema utilizado para describir la estructura y las restricciones de los contenidos de los documentos XML de una forma muy precisa, más allá de las normas sintácticas impuestas por el propio lenguaje XML. Se consigue así una percepción del tipo de documento con un nivel alto de abstracción.

SOAP: SOAP (originalmente las siglas de Simple Object Access Protocol) es un protocolo estándar que define cómo dos objetos en diferentes procesos pueden comunicarse por medio de intercambio de datos XML.

REST: La Transferencia de Estado Representacional (Representational State Transfer) o REST es un estilo de arquitectura software para sistemas hipermedia distribuidos como la World Wide Web.

JDBC: Java Database Connectivity, más conocida por sus siglas JDBC,1 2 es una API que permite la ejecución de operaciones sobre bases de datos desde el lenguaje de programación Java, independientemente del sistema operativo donde se ejecute o de la base de datos a la cual se accede, utilizando el dialecto SQL del modelo de base de datos que se utilice.

ODBC: Open DataBase Connectivity (ODBC) es un estándar de acceso a las bases de datos desarrollado por SQL Access Group (SAG) en 1992. El objetivo de ODBC es hacer posible el acceder a cualquier dato desde cualquier aplicación, sin importar qué sistema de gestión de bases de datos (DBMS) almacene los datos. ODBC logra esto al insertar una capa intermedia (CLI) denominada nivel de Interfaz de Cliente SQL, entre la aplicación y el DBMS. El propósito de esta capa es traducir las consultas de datos de la aplicación en comandos que el DBMS entienda. Para que esto funcione tanto la aplicación como el DBMS deben ser compatibles con ODBC, esto es que la aplicación debe ser capaz de producir comandos ODBC y el DBMS debe ser capaz de responder a ellos.

FIREWALL: Un cortafuegos (firewall) es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas

Art. 4.- Intervinientes.- Para efectos de la presente norma, los intervinientes necesarios para la inteorperabilidad son:

- **Proveedores de Información**: Son las instituciones públicas o privadas que proveen información considerada como registro de dato público a la plataforma SINARDAP.
- **Plataforma SINARDAP**: Es el concentrador información tipificada como registro de dato público, donde se establece la seguridad jurídica y se permite el acceso a la información a los consumidores estableciendo controles y auditorias de acceso.
- **Consumidores de Información**: Son las instituciones públicas que acceden a la información considerada registro de datos públicos mediante mecanismos de tecnológicos de consumo de manera controlada y auditada.

CAPITULO I

DE LA INTEGRACIÓN DE FUENTES PROPIAS Y EXTERNAS

Art. 5.- Integración.- Para la integración de los entes registrales, fuentes propias y fuentes externas, considerados proveedores de información de registro de datos públicos, se deben considerar los siguientes componentes:

- Conectividad
- Mecanismo de Integración
- Seguridad

Art. 6.- Conectividad.- la capacidad de conexión de la fuente, se determinará de conformidad con los siguientes medios de acceso:

- **Enlace privado de datos, entre el proveedor y la plataforma SINARDAP**: será provisto por la entidad proveedora de información, se debe realizar un análisis técnico para establecer la capacidad y características del ancho de banda necesarias.
- **Red Nacional Gubernamental:** este mecanismo es idóneo para las instituciones que ya cuenten con el acceso a la Red Nacional Gubernamental.
- **Internet:** se procederá con el establecimiento de un enlace a internet, previó el debido análisis técnico para determinar la capacidad y características del ancho de banda.

Art. 7.- Mecanismos de entrega de información.- Los mecanismos de integración permiten el intercambio de información desde las instituciones proveedoras a la plataforma SINARDAP, si bien dentro de la industria tecnológica se prevén varios mecanismos de integración, para efectos de la presente norma ha considerado los siguientes:

- **Base de Datos de Frontera, Vista Materializada**: Cada institución debe mantener una base de datos de frontera mediante la cual proveerá información al concentrador de información. La base de datos de frontera deberá ser una instancia de base de datos diferente a la de producción y no deberá comprometer el rendimiento o degradación de los procesos de la institución proveedora de información. Así mismo

deberá contener todos los campos requeridos por la DINARDAP, en el caso de existir un código deberá incluir la descripción en un campo adicional. La vista materializada debe ser compatible con el lenguaje de consulta estructurado (SQL, por sus siglas en inglés) y sus variantes

- **Servicios Web:** consiste en otro mecanismo de integración, se realiza mediante servicios web los cuales generan los proveedores debiendo considerar los siguientes estándares:
  - Especificación SOAP 1.1
  - Utilización de patrón Contract First, el WSDL y XSD que será entregado por la DINARDAP. Es decir, definir las operaciones, métodos y datos del servicio como fase inicial del análisis, para implementar posteriormente el código. Los diseños Contract-First permiten dar mayor robustez al servicio frente a variaciones. También mejora los aspectos de reusabilidad, rendimiento y versionado, haciendo que sea una de las características más habituales en el diseño de webservices.
  - El servicio web debe tener establecido los parámetros de cabecera SOAP Action, donde se especificarán los métodos que pueden ser invocados.
  - El enlace WSDL a ser utilizado será "document-literal ", (style="document", use="literal").
  - Controlar incidencia y excepciones en el servicio web en el elemento FAULT
  - Estándar de Mensaje SOAP: El estándar de mensaje SOAP, para ser implementado se incluye en el documento del ANEXO 1.
- **Archivos Planos**: La integración mediante archivos planos deben considerar los siguientes estándares.
  - Formato XML
  - Únicamente se pueden utilizar tipos de datos simples
  - El documento XML será validado en su estructura XSD antes de ser cargado en la plataforma de interoperabilidad.
  - El estándar que será leído deberá ser guardado como Hoja de Cálculo XML de Excel 2003 / 2004 en EXCEL u Open Office.

La DINARDAP contará con un servidor de archivos seguro (SFTP) de frontera, donde los proveedores cargarán la información, en el proceso de carga de datos la DINARDAP establecerá los respectivos mecanismos de validación de la información.

Art. 8.- Seguridad.- Para asegurar la comunicación entre el proveedor de información y la SINARDAP, se establecerán las siguientes consideraciones:

- VPN IPSEC (Red Privada Virtual) entre el proveedor de información y la SINARDAP
- Control de acceso a nivel de enrutamiento de firewall de IP a IP
- Permisos de consumo se realizarán a nivel de IP

Art. 9.- Monitoreo del Servicio.- Cuando la institución proveedora de información haya sido incorporada a la plataforma SINARDAP, deberá entregar todas las facilidades a la DINARDAP para realizar el monitoreo de los componentes de hardware y software orientados a cumplir lo que indica en el SLA, de conformidad con el ANEXO 3 (Acuerdo de Nivel de Servicio DINARDAP) de la presente norma.

Art. 10.- Soporte y Disponibilidad.- La institución que sea incorporada como proveedor de información de la plataforma SINARDAP, deberá cumplir con el SLA requerido por la DINARDAP.

Art. 11.- Control de Cambios.- Cuando una institución sea incorporada como proveedor de información de la plataforma SINARDAP, la infraestructura de hardware y software que se utilice para tal fin, será considerada parte de la plataforma SINARDAP, por tal motivo si se requiere realizar algún cambio este deberá ser coordinado con la DINARDAP para establecer el mapa de ruta, cronograma y evaluación de riesgos del cambio a ser realizado.

Por lo expuesto se prohíbe a las fuentes modificar, eliminar o degradar el servicio provisto sin previa autorización formal de la DINARDAP.

CAPITULO II

DE LOS CONSUMIDORES

Art. 12.- Acceso a la Información.- los consumidores de información podrán acceder a la información que provee la plataforma SINARDAP en formatos abiertos y de forma estandarizada, para lo cual, la DINARDAP cuenta con la plataforma de concentrador y el consolidación de datos.

a) **Concentrador de Datos:** Se considera al concentrador de datos todos los componentes de hardware, software, normas políticas y procesos, que permiten entregar datos en línea desde las instituciones proveedoras de información, estos datos no se almacenan en la DINARDAP y su forma de consumo se encuentra basado en una consulta una respuesta, se prevé que el único mecanismo de acceso es mediante servicios web. El acceso a la información se realizará de manera controlada según proceso de consumo de información.

b) **Consolidador de Datos**: Se considera al consolidador de datos a los componentes de hardware, software, normas, políticas y procesos que permiten entregar datos que se encuentran almacenados en la DINARDAP, estos datos almacenados han de tener un tiempo de

refresco desde los proveedores de información hacia la DINARDAP. El consolidador de información tiene la característica que permite consultas masivas de información y los mecanismos de acceso será mediante, servicios web REST, SOAP, JDBC, ODBC, OData. El acceso a la información se realizará de manera controlada según proceso de consumo de información.

Art. 13.- Conectividad.- Es el mecanismo que tiene la institución para establecer la comunicación de datos con la plataforma SINARDAP para el consumo de la información, para lo cual se podrán utilizar los siguientes medios de acceso:

- **Enlace privado de datos, entre el proveedor y la plataforma SINARDAP**: será provisto por la entidad proveedora de información, se debe realizar un análisis técnico para establecer la capacidad y características del ancho de banda necesarias.

- **Red Nacional Gubernamental:** este mecanismo es idóneo para las instituciones que ya cuenten con el acceso a la Red Nacional Gubernamental. Para asegurar el canal se establecerá una VPN (Red Privada Virtual)

- **Internet:** se procederá con el establecimiento de un enlace a internet, previó el debido análisis técnico para determinar la capacidad y características del ancho de banda. Para asegurar el canal se establecerá una VPN (Red Privada Virtual).

Art. 14.- Mecanismos de Consumo.- Los mecanismos de integración que provee la plataforma SINARDAP a los consumidores son los siguientes:

- **Servicios Web.-** La plataforma SINARDAP para el consumo desde el concentrador de datos, presenta un servicio web con mensaje estándar basado en entidad, campo y valor, el detalle técnico se encuentra en el ANEXO 1 (Estándar de Mensajes para Interoperabilidad), el servicio web cumple con los siguientes lineamientos de servicios web. Para poder tener acceso a la información mediante los servicios web, deberán observarse los siguientes lineamientos:

  - Especificación SOAP 1.1

  - Mensaje canónico, para provisión de servicios, establecido en el documento Estándar de Mensaje de Consumidor.

  - El servicio web debe tener establecido los parámetros de cabecera SOAP Action, donde se especificarán los métodos que pueden ser invocados.

  - El enlace WSDL a ser utilizado será "document-literal", (style="document", use="literal").

  - El estándar de mensaje SOAP, para ser implementado se incluye en el documento incluido ANEXO 2, de la presente.

- REST: El método REST es otra forma de exposición desde el concentrador de información, orientado a la exposición masiva de información.

- JDBC: Se tendrá acceso a la plataforma del concentrador de información mediante JDBC que será el mismo que contendrá un usuario y password, el acceso a la plataforma es únicamente de consulta de manera controlada a los datos que la institución consumidora tenga acceso.

- OBDC: Se tendrá acceso a la plataforma del concentrador de información mediante ODBC que será el mismo que contendrá un usuario y password, el acceso a la plataforma es únicamente de consulta de manera controlada a los datos que la institución consumidora tenga acceso.

- Otros mecanismos de acceso: Con forme al avance tecnológico la DINARDAP se reserva el derecho de incorporarán nuevos mecanismos de acceso a la información que se encuentre en el concentrador de datos como por ejemplo ODATA u otras nuevas tecnologías.

Art. 15.- Para asegurar la comunicación entre la SINARDAP y el consumidor de información, se establecerán las siguientes consideraciones:

- VPN IPSEC (Red Privada Virtual) la SINARDAP y el consumidor de información

- Control de acceso a nivel de enrutamiento de firewall de IP a IP

- Permisos de consumo se realizarán a nivel de IP

- La entrega de credenciales de acceso se realizará mediante el procedimiento de gestión de usuarios y contraseñas incluido en el ANEXO 4 (PR-No. 02 Procedimiento Gestión De Usuarios Y Contraseñas – CISI), de la presente norma.

DISPOSICIÓN GENERAL:

Encárguese de la ejecución de la presente norma a la Coordinación de Seguridad Informática de la Dirección Nacional de Registro de Datos Públicos.

Esta Resolución entrará en vigencia a partir de la presente fecha sin perjuicio de su publicación en el Registro Oficial.

Dado en la ciudad de Quito, Distrito Metropolitano, el 22 de septiembre de 2016.

f.) Abg. Nuria Susana Butiñá Martínez, Directora Nacional de Registro de Datos Públicos.

DIRECCIÓN NACIONAL DE REGISTRO DE DATOS PÚBLICOS.- Certifico que es copia auténtica del original.- Quito, a 20 de octubre de 2016.- f.) Ilegible, Archivo.

ANEXO 1

ESTÁNDAR DE MENSAJE INTEROPERABILIDAD

COORDINACIÓN DE INFRAESTRUCTURA Y SEGURIDAD DE LA INFORMACIÓN

DIRECCIÓN DE TECNOLOGÍA Y DESARROLLO

Agosto de 2016

DATOS PÚBLICOS

Formato de mensajes para el intercambio de información a través de la plataforma de Interoperabilidad

ESTANDAR DE MENSAJES PARA INTEROPERABILIDAD

Formato de mensajes para el intercambio de información a través de la plataforma de Interoperabilidad

CONTROL DE VERSIONES

FECHA	AUTOR	VERSION	DESCRIPCION	FIRMA
2016-07-27	Rubén López	V. 1.0	Emisión Inicial	
2016-09-21	Orlando Chamorro	V. 1.0	Revisión final	

TABLA DE CONTENIDOS:

Antecedentes

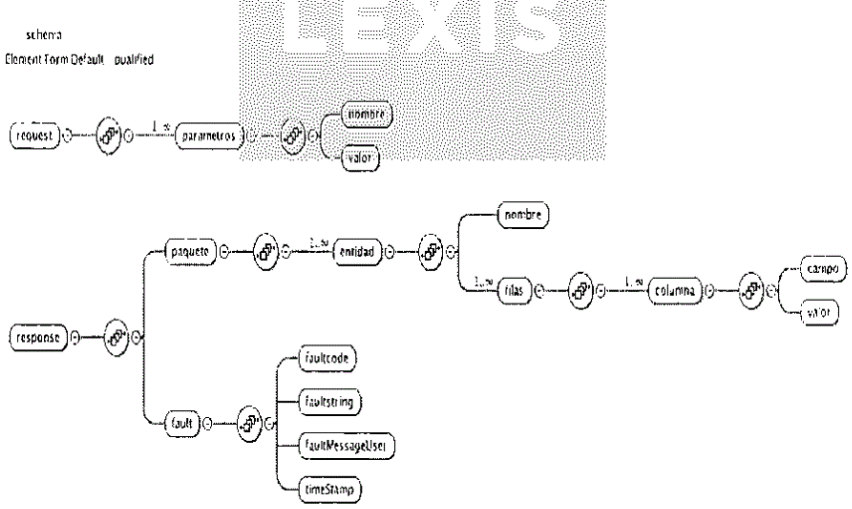
Antecedentes.

Con la finalidad que el intercambio de información que se realiza a través de la plataforma de interoperabilidad sea transparente, se hace necesario plantear un estándar de mensajes que permita garantizar que las partes que intervienen en el intercambio conozcan el significado preciso de la información intercambiada, además, que la misma pueda ser entendida por cualquier aplicación cliente, esto permitirá que las aplicaciones y sistemas informáticos puedan intercambiar y tratar la información interpretándola de la misma manera sin posibilidad de confusión.

Estándar de mensaje de consumidor

Estándar de mensaje de consumidor.

En esta sección se describe el esquema de mensajes de petición y respuesta que manejara la plataforma.



Esquema de WSDL propuesto para el servicio web entregado por la DINARDAP.

```
<?xml arámet="1.0" encoding="UTF-8" standalone="no"?>

<wsdl:definitions xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/"
xmlns:tns="http://interoperabilidad.dinardap.gob.ec/interoperador/"
xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/"
xmlns:xsd="http://www.w3.org/2001/XMLSchema" name="interoperador"
targetNamespace="http://interoperabilidad.dinardap.gob.ec/interoperador/">

 <wsdl:types>

  <xsd:schema targetNamespace="http://interoperabilidad.dinardap.gob.ec/interoperador/">

   <xsd:element name="consultar" type="tns:consultar">


   </xsd:element>

   <xsd:element name="consultarResponse" type="tns:consultarResponse">

   </xsd:element>

   <xsd:complexType name="parametro">

        <xsd:sequence>

                <xsd:element name="nombre" type="xsd:string" minOccurs="0"></xsd:element>

                <xsd:element name="valor" type="xsd:string" minOccurs="0"></xsd:element>

        </xsd:sequence>

   </xsd:complexType>

   <xsd:complexType name="consultar">

        <xsd:sequence>

                <xsd:element name="parametros" type="tns:parametros" minOccurs="0"
maxOccurs="1"></xsd:element>

        </xsd:sequence>

   </xsd:complexType>

   <xsd:complexType name="columna">
```

```
        <xsd:sequence>
            <xsd:element name="campo" type="xsd:string" minOccurs="0"></xsd:element>
            <xsd:element name="valor" type="xsd:string" minOccurs="0"></xsd:element>
        </xsd:sequence>
    </xsd:complexType>
    <xsd:complexType name="fila">
        <xsd:sequence>
            <xsd:element name="columnas" type="tns:columnas" minOccurs="0"
maxOccurs="1"></xsd:element>
        </xsd:sequence>
    </xsd:complexType>
    <xsd:complexType name="entidad">
        <xsd:sequence>
            <xsd:element name="nombre" type="xsd:string" minOccurs="0"></xsd:element>
            <xsd:element name="filas" type="tns:filas" minOccurs="0"
maxOccurs="1"></xsd:element>
        </xsd:sequence>
    </xsd:complexType>
    <xsd:complexType name="paquete">
        <xsd:sequence>
            <xsd:element name="numeroPaquete" type="xsd:string"
                minOccurs="0">
            </xsd:element>
            <xsd:element name="entidad" type="tns:entidad" minOccurs="0"
maxOccurs="1"></xsd:element>
        </xsd:sequence>
```

```
    </xsd:complexType>
    <xsd:complexType name="consultarResponse">
        <xsd:sequence>
            <xsd:element name="paquete" type="tns:paquete" minOccurs="0"
maxOccurs="1"></xsd:element>
        </xsd:sequence>
    </xsd:complexType>

    <xsd:complexType name="parametros">
        <xsd:sequence>
            <xsd:element name="parametro" type="tns:parametro" minOccurs="0"
maxOccurs="unbounded"></xsd:element>
        </xsd:sequence>
    </xsd:complexType>

    <xsd:complexType name="filas">
        <xsd:sequence>
            <xsd:element name="fila" type="tns:fila" minOccurs="0"
maxOccurs="unbounded"></xsd:element>
        </xsd:sequence>
    </xsd:complexType>

    <xsd:complexType name="columnas">
        <xsd:sequence>
            <xsd:element name="columna" type="tns:columna" minOccurs="0"
maxOccurs="unbounded"></xsd:element>
```

```
        </xsd:sequence>
    </xsd:complexType>
  </xsd:schema>
 </wsdl:types>
 <wsdl:message name="consultar">
  <wsdl:part element="tns:consultar" name="parameters"/>
 </wsdl:message>
 <wsdl:message name="consultarResponse">
  <wsdl:part element="tns:consultarResponse" name="parameters"/>
 </wsdl:message>
 <wsdl:portType name="interoperador">
  <wsdl:operation name="consultar">
   <wsdl:input message="tns:consultar" name="consultar"/>
   <wsdl:output message="tns:consultarResponse" name="consultarResponse"/>
  </wsdl:operation>
 </wsdl:portType>
 <wsdl:binding name="interoperadorSoapBinding" type="tns:interoperador">
        <soap:binding style="document"
                transport="http://schemas.xmlsoap.org/soap/http" />
        <wsdl:operation name="consultar">
                <soap:operation
        soapAction="http://interoperabilidad.dinardap.gob.ec/interoperador/consultar" />
                <wsdl:input name="consultar">
                        <soap:body use="literal" />
                </wsdl:input>
                <wsdl:output name="consultarResponse">
                        <soap:body use="literal" />
                </wsdl:output>
        </wsdl:operation>
 </wsdl:binding>
 <wsdl:service name="interoperador">
  <wsdl:port binding="tns:interoperadorSoapBinding" name="InteroperadorPort">
   <soap:address location="http://localhost/interoperador"/>
  </wsdl:port>
 </wsdl:service>
</wsdl:definitions>
```

```
        </arámetro>
       </arámetros>
     </int:consultar>
   </soapenv:Body>
</soapenv:Envelope>
```

Esquema de mensaje de respuesta (Response)

Atributo	Descripción
paquete	Número de paquete consultado
entidad	Tipo complejo que representa la entidad consultada
nombre	Nombre de la entidad consultada
columnas	Tipo complejo que representa un registro consultado
columnas	Tipo complejo que representa un campo consultado
campo	Nombre del campo consultado
valor	Valor del campo consultado

Ejemplo:

```
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <soap:Body>
    <ns2:consultarResponse
xmlns:ns2="http://interoperabilidad.dinardap.gob.ec/interoperador/">
      <paquete>
        <numeroPaquete>999</numeroPaquete>
        <entidad>
          <nombre>Registro Civil</nombre>
          <filas>
            <fila>
              <columnas>
                <columna>
```

Esquema de mensaje de petición (Request)

Atributo	Descripción
parámetros	Lista de parámetros de consulta
nombre	Nombre del parámetro
valor	Valor del parámetro

Ejemplo

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:int="http://interoperabilidad.dinardap.gob.ec/interoperador/">
  <soapenv:Header/>
  <soapenv:Body>
    <int:consultar>
      <!—Optional:→
      <parametros>
        <!—Zero or more repetitions:→
        <arámetro>
          <!—Optional:→
          <nombre>numeroPaquete</nombre>
          <!—Optional:→
          <valor>999</valor>
        </arámetro>
        <arámetro>
          <!—Optional:→
          <nombre>cedula</nombre>
          <!—Optional:→
          <valor>1002003001</valor>
```

```
            <campo>cedula</campo>
            <valor>1002003001</valor>
          </columna>
          <columna>
            <campo>nombre</campo>
            <valor>JUAN PEREZ</valor>
          </columna>
        </columnas>
      </fila>
      <fila>
        <columnas>
          <columna>
            <campo>cedula</campo>
            <valor>1002003001</valor>
          </columna>
          <columna>
            <campo>nombre</campo>
            <valor>JUAN PEREZ</valor>
          </columna>
        </columnas>
      </fila>
    </filas>
  </entidad>
 </paquete>
</ns2:consultarResponse>
```

```
</soap:Body>
</soap:Envelope>
```

Código de Errores

Código de errores.

Especificación Soap Fault

El esquema SOAP, para el mensaje de la parte SOAP Fault es la siguiente:

Atributo	Descripción
codigo	Código de Error
descripcion	Mensaje de Error Técnico
mensaje	Mensaje de Error para Usuario
timeStamp	Fecha de generación de Consumo

Tabla de referencia de código de errores conocidos:

Código	Descripción	Mensaje	Aplicabilidad
0100	Catch error	La Fuente (Consultada) no se encuentra disponible	Se utiliza cuando la fuente de datos no se encuentra disponible
0101		Institución no Autorizada	Se utiliza cuando la institución esta tratando de acceder a un paquete que no tiene autorización
0102		Usuario no Autorizado	Se genera cuando el usuario no logra autenticar con la plataforma SINARDAP
0103		Excedido número de consultas	Se presenta cuando la institución ha excedido el número de consultas configuradas en el sistema
0104		No se valida con el XSD	Se presenta cuando el

			wsdl no se logra validar con su respectivo XSD

Ejemplo:

```
<fault>
  <faultcode>0100</faultcode>
  <faultstring></faultstring>
  <faultMessageUser> La Fuente (Consultada) no se encuentra disponible </faultMessageUser>
  <timeStamp>2016-09-14 14:27:04</timeStamp>
</fault>
```

Estándar de mensaje de proveedor de información

Estándar de mensaje de proveedor de información

Para la implementación del Servicio Web se aplicará el patrón "Contract First" para lo cual la DINARDAP entregará el contrato del servicio web a implementar mediante un archivo WSDL donde se especificará:

- Nombre del servicio
- Nombre del método
- Parámetros de entrada
- Parámetros de salida
- Estructura de código de error

Este contrato deberá ser cumplido estrictamente por el proveedor para que el servicio web pueda se integrado a la plataforma de Interoperabilidad.

Reglas para formato de datos

Regla para formato de datos

En esta sección se definen las reglas que se aplicarán para el formato de las estructuras de datos.

- Si no existe un valor para un campo en la etiqueta valor irá null.
  - **Ejemplo: <valor>null</valor>**
- El formato para campos de fecha y hora será el siguiente yyyy/mm/dd año, mes, día con hh:mm:ss si no existe las hh:mm:ss se llenará con 00:00:00
  - **Ejemplo: <valor>2016/01/01 00:00:00</valor>**
- Se debe indicar que los datos de valor se establecerá el punto (.) decimal, no la coma (,) decimal.
  - **Ejemplo: <valor>1234567.89</valor>**
- Números negativos debe mantener el signo de menos (-) que precede al número
  - **Ejemplo: <valor> -12345</valor>**

ANEXO 2

ACUERDO DE NIVEL DE SERVICIO DINARDAP

SLA DINARDAP-INTEROPERABILIDAD

DATOS PÚBLICOS

ACUERDO DE NIVEL DE SERVICIO DINARDAP

COORDINACIÓN DE INFRAESTRUCTURA Y SEGURIDAD DE LA INFORMACIÓN

DIRECCION DE TECNOLOGÍA Y DESARROLLO

Septiembre de 2016

dato

Av. Río Amazonas N21-147 y Roca, Edificio Río Amazo
t593 2) 2504200/ 2500288
info.dinardap@dinardap.gob.ec www.datospublic
Quito - Ecuador

TABLA DE CONTENIDOS:

1. TERMINOS GENERALES

El presente Acuerdo de Nivel de Soporte, define y documenta los compromisos adquiridos por parte de la Dirección Nacional de Registro de Datos Públicos, para la provisión de servicios de soporte técnico en la plataforma de Interoperabilidad.

1.1. VIGENCIA

El presente acuerdo estará vigente desde la fecha de suscripción en adelante.

2. OBJETIVO

El presente documento tiene como finalidad:

- Establecer el acuerdo de niveles de servicio de soporte técnico que la DINARDAP deberá entregar en la plataforma de interoperabilidad
- Establecer los términos, condiciones, alcance y limitaciones del servicio de soporte técnico que prestará la DINARDAP en la plataforma de interoperabilidad
- Establecer los tipos de incidentes y los respectivos tiempos de respuesta y atención.
- Establecer los mecanismos de notificación de solución de incidentes y ventanas de mantenimiento que puedan afectar temporalmente el servicio considerado.

3. DESCRIPCION DEL SERVICIO

Se define como servicio a la disponibilidad de la plataforma de Interoperabilidad, misma que permite el intercambio de información de los distintos entes registrales que alimentan el SINARDAP.

4. DISPONIBILIDAD DEL SERVICIO

La disponibilidad del servicio es de **99,6%** en modalidad 24X7 (**24** horas diarias los 7 días de la semana) con un tiempo de respuesta por consulta de hasta 3 segundos.

Se entiende como disponibilidad al tiempo en horas que el servicio está operativo y disponible para el uso por parte de los consumidores.

Se entiende por tiempo de respuesta, el tiempo que toma la infraestructura de la DINARDAP en atender un requerimiento de información (consulta) desde que ésta ingresó en la plataforma hasta se entrega la información a los componentes que están bajo responsabilidad del consumidor.

El valor de disponibilidad se calculará con la siguiente expresión:

D = (TD / (TT – TM)) * 100 [%]

Donde:

D (%) = Disponibilidad mensual del servicio, expresado como un porcentaje.

TD (minutos) = Tiempo Disponible, tiempo que el servicio estuvo disponible en minutos durante el mes.

TT (minutos) = Tiempo Total, tiempo total de días del mes multiplicadas por 1440

TM (minutos) = Tiempo de Mantenimiento, tiempo que el servicio estuvo fuera de servicio debido a mantenimientos preventivos planificados y previamente notificados por la DINARDAP; o ante cualquiera de los motivos considerados como caso fortuito o fuerza mayor siempre que tales eventos, según lo establecido en el artículo 30 del Código Civil Ecuatoriano, impidan que de forma continua las partes cumplan sus obligaciones contractuales, sin derecho a reclamo de indemnización alguna entre las partes; sin perjuicio de que, también se produzcan los eventos que se indican a continuación:

- Desastres naturales, atentados, hurto, vandalismo, accidente, incendio, alteración del orden público, etc., que afecten el servicio provisto por la **DINARDAP**
- Fallas en las instalaciones de la **DINARDAP** tales como equipos de cómputo, enlaces de datos y equipos de comunicación de dato o conexión de internet.
- Interrupciones autorizadas y/o requeridas por la **DINARDAP**.

5. ESCALAMIENTO TÉCNICO

Los niveles de escalamiento técnico son:

Primer Nivel: Correo de soporte de la **DINARDAP:** soportetics@dinardap.gob.ec

Segundo Nivel: Equipo técnico de la **DINARDAP** que verificará el origen de la incidencia identificada

Tercer Nivel: Director de Tecnología y Desarrollo de la **DINARDAP** o su delegado que será el encargado de realizar el seguimiento a la incidencia.

La notificación del problema o incidente se la deberá realizar de forma obligatoria a través de correo electrónico dirigido a la cuenta soportetics@dinardap.gob.ec

El correo electrónico deberá contener lo siguiente:

- Hora en que se identificó el incidente técnico
- Detalle del Incidente o problema técnico detectado
- Datos de contacto de la persona que notifica (nombre, número de contacto y correo electrónico)
- Impacto del problema o incidente técnico: Situación o estado del servicio (sin servicio, intermitente)
- Información adicional que le sirva a la DINARDAP para analizar la causa del incidente (eje., captura de pantallas, mensajes de errores, otros)

Solo en casos excepcionales se podrá notificar por vía telefónica a:

NIVEL	Dirección	CONTACTO	TELEFONO	EXT
3	Dirección de Tecnología y Desarrollo	Infraestructura	023563130	800

6. MANTENIMIENTOS

El tiempo de inactividad para mantenimientos de la plataforma de interoperabilidad del servicio se planificará por lo menos con 24 horas de anticipación y bajo circunstancias normales se notificará

con 48 horas de anticipación, la DINARDAP podrá realizar los mantenimientos en días laborables o no laborables (fines de semana, días sábados y/o domingos, feriados). Sólo en casos excepcionales se considerarán mantenimientos con notificaciones menores a 24 horas de antelación.

La DINARDAP informara por correo electrónico los motivos de mantenimiento, la descripción de las actividades que se van a realizar, el tiempo de inicio y la duración. Al final del mantenimiento programado la DINARDAP notificará mediante correo electrónico a las instituciones consumidoras la finalización del trabajo realizado y la confirmación de disponibilidad del sistema.

7. ESTRUCTURA Y PROCESO DE SOPORTE

La DINARDAP prestará el servicio soporte técnico en la plataforma de interoperabilidad de forma ininterrumpida durante 24 horas, los 7 días de la semana.

Los requerimientos de Soporte Técnico, serán atendidos bajo el siguiente esquema de priorización que considera el tipo de caso escalado de acuerdo a su severidad:

CRITERIOS PARA DEFINIR PRIORIDAD DE REQUERIMIENTOS	
Prioridad	**Criterios**
Alta	Atención de incidentes tipo críticos: El servicio se encuentra indisponible, fuera de servicio o existe un impacto crítico en la operación por causas atribuibles a la DINARDAP. Su indisponibilidad afecta los servicios que las plataformas consumidoras exponen. La DINARDAP se compromete a dedicar recursos a tiempo completo hasta solucionar el incidente. Esta condición está generalmente caracterizada por una falla grave que requiere corrección inmediata.

Media	Atención de incidentes tipo importantes. El sistema se encuentra parcialmente indisponible o bien se mantiene operativo aunque con ciertas limitaciones o afectaciones en sus funciones, severamente degradado o en algunos aspectos significativos de la operación presentan un impacto negativo por un rendimiento inadecuado, pero mantiene cierta funcionalidad. La DINARDAP se compromete a dedicar recursos a tiempo completo para resolver la situación. La porción afectada del servicio, se considera menos grave que los incidentes calificados como críticos.
Baja	Atención de incidentes tipo no importantes. El sistema está operativo, pero se detecta alguna condición que pudiera modificar su disponibilidad. Esta no representa un impacto de ninguna manera a las operaciones de los servicios. La DINARDAP se compromete a entregar recursos durante las horas de oficina para atender las solicitudes de soporte.

En cualquier escenario de criticidad definidos en el cuadro precedente, la DINARDAP actuará como responsable del seguimiento, atención, solución y notificación hacia las instituciones consumidoras; quedan exentos de responsabilidad de la DINARDAP los incidentes y problemas atribuibles a los recursos bajo dominio de las instituciones consumidoras.

La DINARDAP se compromete a cumplir de los siguientes tiempos de respuesta una vez recibida la notificación en la cuenta soportetics@dinardap.gob.ec:

Prioridad	Tiempo de alternativa o resolución de la falla	Modalidad de notificación	Observaciones

Alta	Hasta 4 horas	Correo electrónico dirigido a la cuenta soportetics@dinardap.gob.ec y/o por teléfono de acuerdo a los niveles de comunicación establecidos.	Tiempo de solución se cuenta a partir del registro de la incidencia en la cuenta soportetics@dinardap.gob.ec
Media	Hasta 6 horas	Correo electrónico dirigido a la cuenta soportetics@dinardap.gob.ec y/o por teléfono de acuerdo a los niveles de comunicación establecidos.	Tiempo de solución se cuenta a partir del registro de la incidencia en la cuenta soportetics@dinardap.gob.ec
Baja	Hasta 24 horas	Correo electrónico dirigido a la cuenta soportetics@dinardap.gob.ec	Tiempo de solución se cuenta a partir del registro de la incidencia en la cuenta soportetics@dinardap.gob.ec

Utilizando correo electrónico la DINARDAP notificará a los consumidores el cierre de un requerimiento; las instituciones por este medio manifestarán su conocimiento y conformidad.

8. RESPONSABILIDADES

8.1. DINARDAP

Será de responsabilidad de la DINARDAP:

- Mantener su equipo de soporte disponible 24 x 7
- Cumplir con las condiciones de este Acuerdo de Nivel de Servicio (ANS)
- Ejecutar las acciones necesarias para garantizar la disponibilidad, continuidad y rendimiento de los servicios

8.2. CONSUMIDORES

Será de responsabilidad de los consumidores:

- Aceptar y cumplir con las condiciones de este Acuerdo de Nivel de Servicio.
- Notificar y escalar los incidentes o problemas de los servicios por los canales establecidos y de forma oportuna.
- Colaborar con la DINARDAP para la solución de los incidentes o problema que notifique o escale.

9. ACEPTACION Y APROBACION

Máxima Autoridad o Delegado Ente Registral	
Coordinador del SINARDAP Ente Registral	

Coordinador Infraestructura y Seguridad Informática DINARDAP	
Director de Gestión y Registro DINARDAP	
Director de Control y Evaluación DINARDAP	

ANEXO 3

ACUERDO DE NIVEL DE LOS ENTES REGISTRALES

SLA DINARDAP-ENTE REGISTRAL

Septiembre de 2016

ACUERDO DE NIVEL DE LOS ENTES REGISTRALES

TABLA DE CONTENIDO:

1. TERMINOS GENERALES

El presente Acuerdo de Nivel de Soporte, define y documenta los compromisos adquiridos por parte de los Entes Registrales que conforman la plataforma SINARDAP, ante la Dirección Nacional de Registro de Datos Públicos, en adelante **DINARDAP**, por la provisión de servicios de soporte técnico a los servicios expuestos en dicha plataforma.

1.1 VIGENCIA

El presente acuerdo estará vigente desde la fecha de suscripción en adelante.

2. OBJETIVO

El presente documento tiene como finalidad:

- Establecer el acuerdo de niveles de servicio de soporte técnico que los Entes Registrales deberán entregar a la DINARDAP.
- Establecer los términos, condiciones, alcance y limitaciones del servicio de soporte técnico que prestarán los Entes Registrales a la DINARDAP.
- Establecer los tipos de incidentes y los respectivos tiempos de respuesta y atención
- Establecer los mecanismos de notificación de solución de incidentes y ventanas de mantenimiento que puedan afectar temporalmente el servicio considerado.

3. DESCRIPCION DEL SERVICIO

Se define como servicio a la disponibilidad de los servicios expuestos por los Entes Registrales en la plataforma SINARDAP, misma que permite el intercambio de información entre instituciones.

4. DISPONIBILIDAD DEL SERVICIO

La disponibilidad del servicio esperado deberá ser del **99,6%** en modalidad 24X7 (24 horas diarias los 7 días de la semana) con un tiempo de respuesta por consulta de hasta 3 segundos.

Se entiende como disponibilidad al tiempo en horas que el servicio está operativo y disponible para el uso por parte de la DINARDAP.

Se entiende por tiempo de respuesta, el tiempo que toma la infraestructura del Ente Registral en atender un requerimiento de información (consulta) desde que ésta ingresó a la infraestructura del Ente Registral hasta que dicha infraestructura entrega la información a los componentes que están bajo responsabilidad de la DINARDAP.

5. ESCALAMIENTO TÉCNICO

Los niveles de escalamiento técnico son:

Primer Nivel: El ente registral debe contar con una cuenta de correo única que sea el contacto de primer nivel para escalar las incidencias.

Segundo Nivel: Se debe contar con un número telefónico y una matriz de comunicación del equipo técnico que se encargara de verificar el origen de la incidencia, para seguimiento.

Tercer Nivel: Se debe contar con el contacto del Director de Tecnología o su delegado que será el contacto de Tercer Nivel, en caso de que las incidencias superen los tiempos establecidos.

Las incidencias serán escaladas al correo electrónico designado como soporte de primer nivel en primera instancia, y contara con la siguiente información:

- Hora en que se identificó el incidente técnico
- Detalle del Incidente o problema técnico detectado

- Datos de contacto de la persona que notifica (nombre, número de contacto y correo electrónico)
- Información adicional que le sirva a la DINARDAP para analizar la causa del incidente (eje., captura de pantallas, mensajes de errores, otros)

6. MANTENIMIENTOS

El tiempo de inactividad para mantenimientos de los servicios expuestos en la plataforma SINARDAP se planificará por lo menos bajo circunstancias normales con 72 horas de anticipación. Sólo en casos excepcionales se considerarán mantenimientos con notificaciones menores a 24 horas de antelación.

El Ente Registral informara por correo electrónico los motivos para la solicitud de mantenimiento, la descripción de las actividades que se van a realizar, el tiempo de inicio y la duración a los correos: Info.Sinardap@dinardap.gob.ec y soportetics@dinardap.gob.ec. Al final del mantenimiento programado el Ente Registral notificará mediante correo electrónico a la DINARDAP la finalización del trabajo realizado y la confirmación de disponibilidad del sistema.

7. ESTRUCTURA Y PROCESO DE SOPORTE

El Ente Registral prestará el servicio soporte técnico en la plataforma SINARDAP de forma ininterrumpida durante 24 horas, los 7 días de la semana.

Los requerimientos de Soporte Técnico, serán atendidos bajo el siguiente esquema de priorización que considera el tipo de caso escalado de acuerdo a su severidad:

CRITERIOS PARA DEFINIR PRIORIDAD DE REQUERIMIENTOS	
Prioridad	**Criterios**

Alta	Atención de incidentes tipo críticos: El servicio se encuentra indisponible, fuera de servicio o existe un impacto crítico en la operación por causas atribuibles a la falta de información expuesta por el Ente Registral, su indisponibilidad afecta las plataformas de la DINARDAP. El ente registral se compromete a dedicar recursos a tiempo completo hasta solucionar el incidente. Esta condición está generalmente caracterizada por una falla grave que requiere corrección inmediata.
Media	Atención de incidentes tipo importantes. El sistema se encuentra parcialmente indisponible o bien se mantiene operativo aunque con ciertas limitaciones o afectaciones en sus funciones, severamente degradado o en algunos aspectos significativos de la operación presentan un impacto negativo por un rendimiento inadecuado, pero mantiene cierta funcionalidad. El ente registral se compromete a dedicar recursos a tiempo completo hasta solucionar el incidente. La porción afectada del servicio, se considera menos grave que los incidentes calificados como críticos.
Baja	Atención de incidentes tipo no importantes. El sistema está operativo, pero se detecta alguna condición que pudiera modificar su disponibilidad. Esta no representa un impacto de ninguna manera a las operaciones de los servicios. El ente registral se compromete a entregar recursos durante las horas de oficina para atender las solicitudes de soporte.

En cualquier escenario de criticidad definidos en el cuadro precedente, el Ente Registral actuará como responsable del seguimiento, atención, solución y notificación hacia las instituciones consumidoras.

El ente registral se compromete a cumplir con los siguientes tiempos de respuesta una vez recibida la notificación en la cuenta correo por parte de la **DINARDAP**:

Prioridad	Tiempo de alternativa o resolución de la falla	Modalidad de notificación	Observaciones
Alta	Hasta 4 horas	Correo electrónico dirigido a la cuenta proporcionada y/o por teléfono de acuerdo a los niveles de comunicación establecidos.	Tiempo de solución se cuenta a partir del registro de la incidencia en la cuenta de correo electrónico proporcionada
Media	Hasta 6 horas	Correo electrónico dirigido a la cuenta proporcionada y/o por teléfono de acuerdo a los niveles de comunicación establecidos.	Tiempo de solución se cuenta a partir del registro de la incidencia en la cuenta de correo electrónico proporcionada

Baja	Hasta 24 horas	Correo electrónico dirigido a la cuenta proporcionada y/o por teléfono de acuerdo a los niveles de comunicación establecidos.	Tiempo de solución se cuenta a partir del registro de la incidencia en la cuenta de correo electrónico proporcionada

Utilizando correo electrónico el Ente Registral notificará a la DINARDAP el cierre de un requerimiento; las instituciones por este medio manifestarán su conocimiento y conformidad.

8. RESPONSABILIDADES

8.1. ENTE REGISTRAL

Será de responsabilidad del Ente Registral:

- Mantener su equipo de soporte disponible 24 x 7
- Cumplir con las condiciones de este Acuerdo de Nivel de Servicio (ANS)
- Ejecutar las acciones necesarias para garantizar la disponibilidad, continuidad y rendimiento de los servicios

8.2 .DINARDAP

Será de responsabilidad de la DINARDAP

- Notificar y escalar los incidentes o problemas de los servicios por los canales establecidos y de forma oportuna.

9. ACEPTACION Y APROBACION

Máxima Autoridad o Delegado Ente Registral	
Coordinador del SINARDAP Ente Registral	
Coordinador Infraestructura y Seguridad Informática DINARDAP	
Director de Gestión y Registro DINARDAP	
Director de Control y Evaluación DINARDAP	

ANEXO 4

GESTIÓN DE USUARIOS Y CONTRASEÑAS - CISI

PROCEDIMIENTO

GESTIÓN DE USUARIOS Y CONTRASEÑAS - CISI

Versión 1.6

TABLA DE CONTENIDOS:

1) Objetivo.

El objetivo del procedimiento es normar la *gestión de usuarios y contraseñas* para los servicios de red, bases de datos, sistemas operativos, elementos activos de red, infraestructura de servidores y toda aplicación que requiera de contraseña para su uso y administración

2) Alcance.

Este procedimiento es de cumplimiento obligatorio para los funcionarios de la Coordinación de Infraestructura y Seguridad Informática de la Dirección Nacional de Registro de Datos Públicos, y abarca todos los elementos de hardware y software para la prestación de servicios informáticos, en las que se utilicen factores de autenticación para su uso y administración.

De igual forma el equipo de trabajo que se encuentra en el desarrollo de proyectos de la Dirección Nacional de Registro de Datos Públicos deberá acogerse a las políticas plasmadas en el presente documento para trabajar en el mismo ambiente e infraestructura.

3) Responsables.

Coordinador de Infraestructura y Seguridad Informática

Es el responsable de receptar las credenciales de los servicios tecnológicos institucionales y redirigirlos para su respectivo almacenamiento y gestión. Así mismo será el responsable de verificar la necesidad de recuperar las contraseñas de los mismos para la respectiva aprobación o negación de la solicitud.

Dueño de la Información o Responsable del Servicio

Es la persona responsable de llevar la administración de los servicios o sistemas que están a su cargo para administrar el mismo de una manera correcta.

Oficial de Seguridad

Es el responsable de dar cumplimiento y seguimiento al procedimiento. A su vez el Oficial de Seguridad podrá designar un funcionario de la Dirección de Seguridad Informática para actuar como delegado para el seguimiento del procedimiento.

Responsable de Control de Accesos

Es el delegado del Director de Seguridad informática para la gestión de usuarios y contraseñas de todos los servicios tecnológicos de la institución.

Es el responsable de administrar la herramienta de Gestión de Usuarios y contraseñas adquirido por la institución para automatizar el proceso y a través del cual se manejará los usuarios y contraseñas de los, bases de datos, sistemas operativos, elementos activos de red, infraestructura de servidores y toda aplicación que requiera de contraseña en conjunto con los responsables designados para cada servicio, además de realizar la gestión de control de accesos a los activos tecnológicos de la Institución.

4) Condiciones/Normativas.

4.1 Características de la contraseña

Toda contraseña debe cumplir con las siguientes características, las cuales deberán ser configuradas en la herramienta encargada de la administración de las contraseñas a nivel institucional:

- Contar con al menos: dos letras mayúsculas, cuatro números, dos caracteres especiales *-+()#$&()=¡¡"@, letras minúsculas.

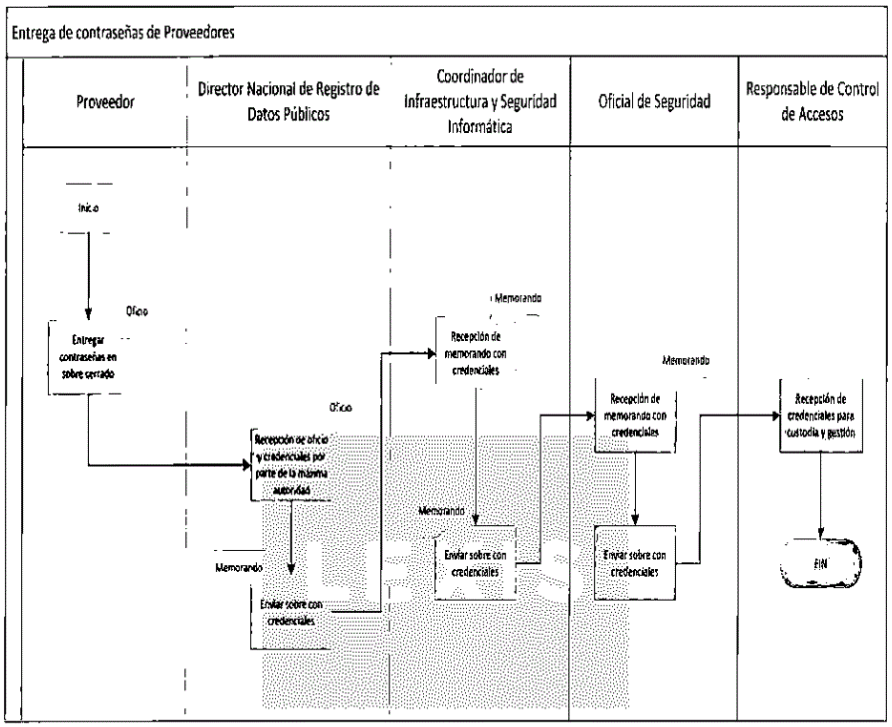
- La contraseña deberá tener mínimo nueve caracteres.
- Nunca dejar en blanco la contraseña.
- No se podrá utilizar una contraseña que anteriormente haya sido registrada. Teniendo en cuenta un historial de hasta 4 (cuatro) contraseñas utilizadas.
- Las contraseñas no deberán tener similitudes con contraseñas ya utilizadas. Teniendo en cuenta un historial de hasta 4 (cuatro) contraseñas utilizadas
- La contraseña no deberá estar basada en información personal fácilmente identificable o relacionada con: su nombre, número telefónico, fechas de nacimiento, nombre de miembros de su familia, etc.
- Las contraseñas serán privadas e intransferibles.

4.2 Uso de la contraseña

La herramienta encargada de la gestión de las contraseñas a nivel institucional almacenará las mismas en una boveda virtual, en caso de necesitar las contraseñas para algún tema específico se configurarán los accesos respectivos a través de la herramienta eliminando de este modo el manejo manual de las mismas y por ende su mala utilización o divulgación.

4.3 Entrega de contraseñas por parte de proveedores

Todos los proveedores que brinden servicios a la DINARDAP, deberán entregar las contraseñas de los servicios, infraestructura, aplicaciones y demás componentes tecnológicos implementados en todos los ambientes, en sobre cerrado a la Dirección Nacional de Registro de Datos Públicos, a través de un oficio dirigido a la máxima autoridad o su representante, quien a su vez hará la entrega formal mediante memorando a la Coordinación de Infraestructura y Seguridad Informática y este a su vez remitirá las credenciales de manera formal a la Dirección de Seguridad Informática para la custodia y gestión respectiva



4.4 Entrega de contraseñas por parte del personal de la DINARDAP

El dueño de la información o responsable del servicio, deberá entregar las credenciales de los servicios, infraestructura, aplicaciones y demás componentes tecnológicos implementados en todos los ambientes, en sobre cerrado a la Coordinación de Infraestructura y Seguridad Informática, a través de un memorando, quien a su vez hará la entrega formal por el mismo medio del sobre con las contraseñas para la custodia y gestión respectiva a la Dirección de Seguridad Informática.

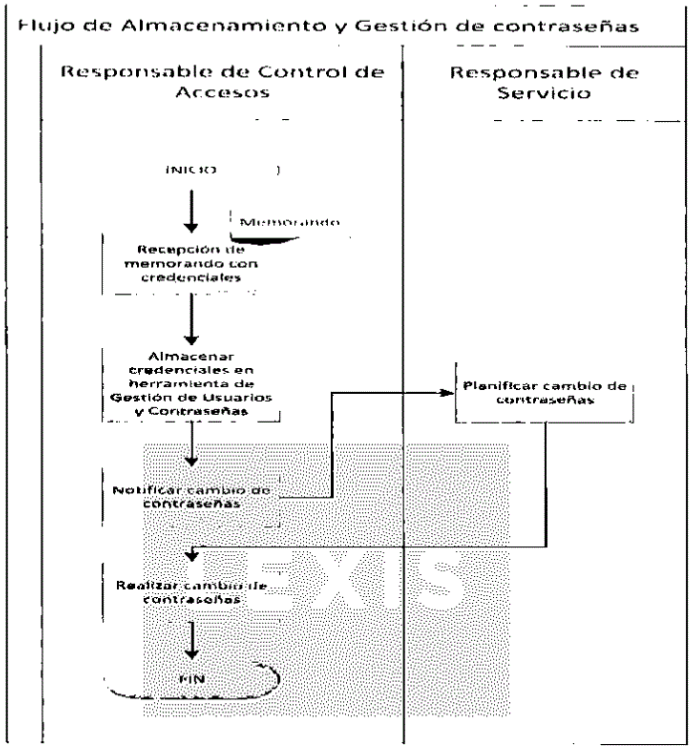
Para el caso de los nuevos servicios institucionales que van surgiendo ante las necesidades institucionales, se deberán regir a lo inscrito en la política de "Creación de Servicios Nuevos" aprobada y vigente en la DINARDAP.

4.5 Administración de Credenciales

4.5.1 Custodia y Gestión de Contraseñas

El Responsable de la Gestión de Control de Accesos de la institución será el responsable de registrar las credenciales dentro de la herramienta de Gestión de Usuarios y contraseñas. Se deberá coordinar el cambio de las mismas en conjunto con los responsables designados para cada servicio para lo cual se deberá:

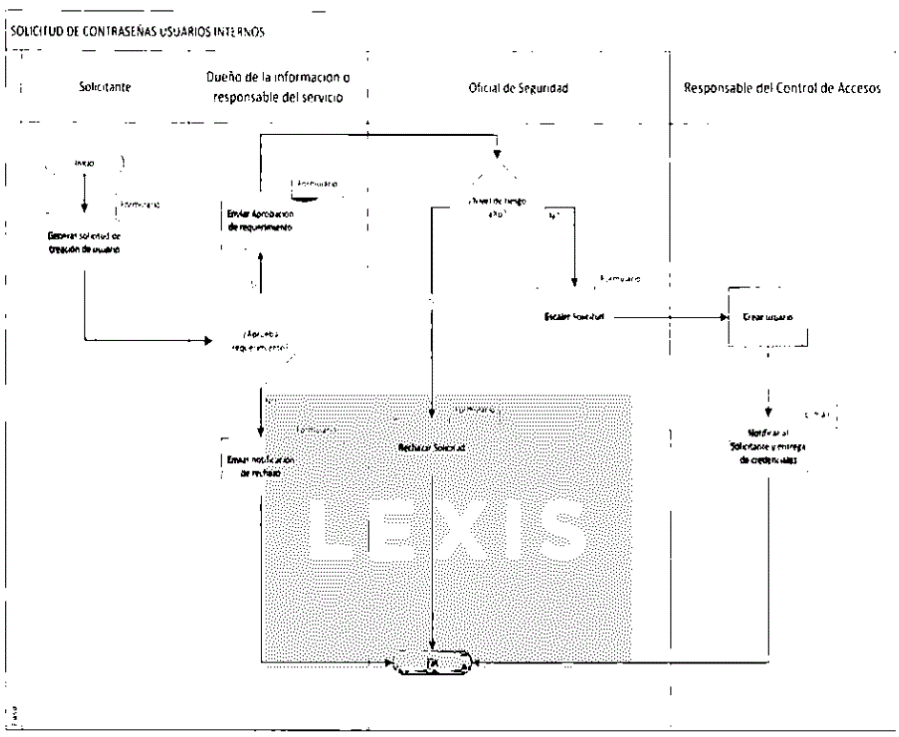
- Cambiar las contraseñas entregadas según el procedimiento, esto se realizará mediante la herramienta de Gestión de Usuarios y contraseñas con las características explicadas en el presente documento y en coordinación con los administradores de cada servicio.
- Guardar, registrar y custodiar las nuevas credenciales establecidas, las contraseñas estarán almacenadas en una bóveda virtual.
- Para los servicios tecnológicos de la DINARDAP se planificarán dos (2) veces al año la ejecución del cambio de contraseña de igual forma en coordinación con los responsables de los servicios.



4.5.2 Solicitud de contraseñas usuarios internos

Cada servidor dentro de la herramienta de Gestión de Usuarios y Contraseñas estará categorizado por la función especifica que cumple, por tal motivo los accesos a los mismos están distribuidos de acuerdo al cargo y responsabilidad que los funcionarios desempeñan en la institución.

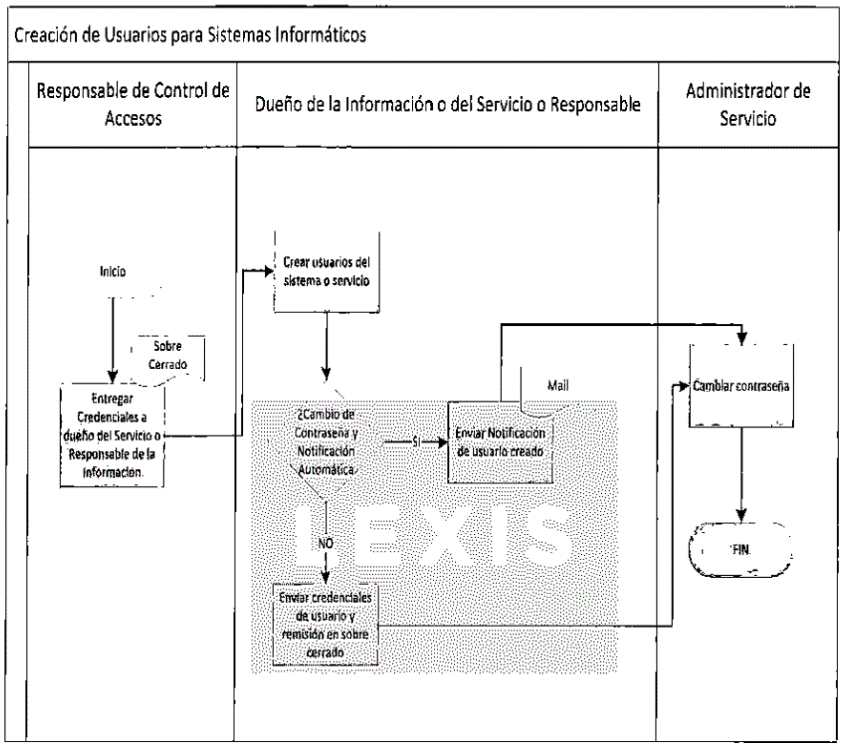
En el caso que se requiera la contraseña de uno de los servidores para ejecutar una tarea o servicio específico, se deberá solicitar de manera formal la creación de un usuario en el servidor que se requiera, y de esta manera se podrán utilizar las credenciales del mismo para realizar las respectivas actividades.



4.5.3 Creación de usuarios en Sistemas Informáticos.

El dueño de la información o responsable del servicio será el encargado de administrar los usuarios y roles respectivo dentro de cada servicio o sistema que este a su cargo para su administración adecuada.

Para esto deberá basarse en el siguiente proceso:



4.5.4 Descubrimiento de Cuentas de Usuarios

Se realizará una detección automática de cuentas de usuarios mensual, la misma será ejecutada mediante la herramienta de Usuarios y Contraseñas institucional de todos los servicios tecnológicos de la institución (servidores, aplicaciones, bases de datos, etc.).

Para las cuentas que sean detectadas mediante este análisis y de las cuales no se cuente con sus credenciales se procederá de la siguiente forma:

- Para las cuentas nuevas de las cuales no se tenga registro se solicitará las credenciales de las mismas para su custodia y gestión respectiva.
- Se procederá a realizar el cambio de las contraseñas de las cuentas encontradas de acuerdo al procedimiento que consta en el presente documento.

4.6 Sanciones

En caso de:

- Uso de las contraseñas para actividades que no se establecen en sus funciones.
- Uso o divulgación de contraseñas para acceso en caso de situaciones de vandalismo.
- Préstamo momentáneo o temporal de la contraseña.
- Divulgación de las contraseñas.
- Olvido de contraseñas por más de tres ocasiones consecutivas.

Los funcionarios de la Coordinación de Infraestructura y Seguridad Informática que incumplan con lo descrito, serán sancionados dependiendo de la gravedad del incidente, bajo sustentos comprobados; por solicitud del Coordinador de Infraestructura y Seguridad Informática de acuerdo a las políticas establecidas por el área de Talento Humano.

5). Descripción macro de actividades.

Los responsables de las contraseñas de usuario *Administrador* de los servicios de red, bases de datos, sistemas operativos, elementos activos de red, infraestructura de servidores y toda aplicación que requiera de contraseña para su uso y administración, estarán regidos bajo las políticas configuradas en la herramienta de Gestión de Usuarios y contraseñas en donde se realizará el cambio de las mismas dos (2) veces por año con la previa supervisión de los administradores de los servicios.

6) Documentación de Referencia.

- Official (ISC) Guide to the ISSAP CBK – Harold F. Tipton, CISSP-ISSAP, ISSMP
- Política de creación de servicios nuevos
- Resolución No. 007–DN–DIANRDAP-2013
  - Capítulo XI artículos 53, 54, 55, 56, 58. 60, 61, 62, 63
- Esquema Gubernamental de Seguridad de la Información.
  - Política 7 Control de Acceso

7) Glosario.

- ***DINARDAP:*** Dirección Nacional de Registro de Datos Públicos
- ***CISI:*** Coordinación de Infraestructura y Seguridad Informática.
- ***Backup:*** Funcionario del Área de Infraestructura que de acuerdo a sus funciones, sustituye al Administrador de Red en el caso que sea delegado para suplir en sus actividades.
- ***DSI:*** Dirección de Seguridad Informática.
- ***Elementos activos de la red:*** Equipos conmutadores como switches, firewall o appliance's para la transmisión de datos.