Plan Operativo de Seguridad de la Información

2024

OIDT

Bogotá, Enero de 2024

Contenido

OBJETIVO

Optimizar el plan de seguridad y privacidad de la información del INM con el fin de alinearse con la estrategia de gobierno en línea de Ministerio TIC, y la norma de seguridad ISO27001:2022 de tal forma que se establezcan los controles necesarios para mantener la confidencialidad, integridad y disponibilidad de la información del INM.

ALCANCE

La implementación del plan se llevará acabo basado en los controles de la ISO27001:2022, los lineamientos de seguridad de gobierno en línea y el resultado del análisis de riesgos de seguridad de la información.

Se realizará una evaluación del estado actual del INM frente a los controles de seguridad de dicha norma y se continuará con el plan de actualización de la ISO 27001:2022 que inició en el 2023, para lograr incrementar la madurez del SGSI.

Los controles que requieran inversión se evaluará su viabilidad.

ABREVIATURAS O SÍMBOLOS

INM: Instituto Nacional de Metrología

MinTic: Ministerio de las telecomunicaciones

SGSI: Sistema de gestión de seguridad de la información

DEFINICIONES

- **Activos**

En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC 27000).

- **Control**

Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido.

Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

- **Riesgo**

Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

- **Seguridad de la información**

Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).

- **Sistema de Gestión de Seguridad de la Información SGSI**

Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000.

- **Partes interesadas (Stakeholder)**

Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.

MARCO NORMATIVO

- NTC/ISO 27001:2022
- Modelo de Seguridad y Privacidad de la Información V.3.0.2 – MPSI de la Estrategia de Gobierno en Línea – GEL _ Habilitador Gobierno Digital -Seguridad – Decreto 1078 de 2015; Decreto 1008 de 2018.

POLITICAS O LINEAMIENTOS GENERALES

La continuación de la implementación del plan será liderada por el responsable de seguridad de la información. Sin embargo, para el éxito de la implementación de éste es necesaria la participación de personal de diferentes áreas.

Es necesario continuar con el compromiso y apoyo de la alta dirección.

Para la implementación de los controles tecnológicos es necesario el compromiso y colaboración del personal de OIDT.

Es necesaria la participación de otras áreas como Recursos humanos y Jurídico para optimizar los controles de personal.

Todos los empleados y contratistas deben participar en actividades específicas que el plan lo requiera.

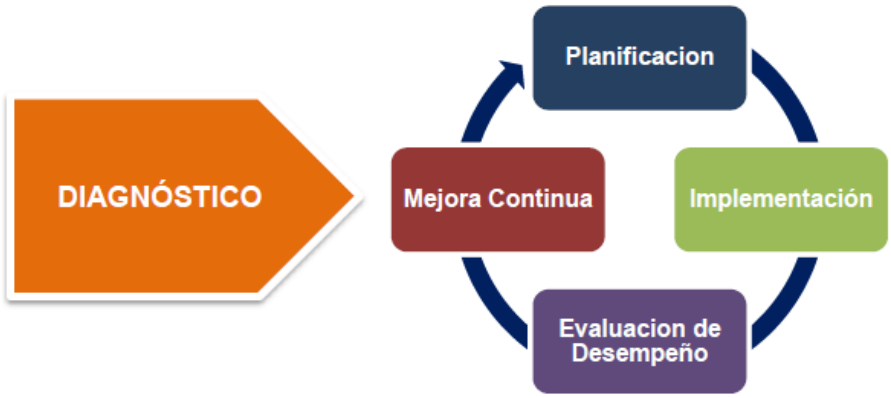
CONDICIONES DE SEGURIDAD

Todas las implementaciones resultantes del plan van orientadas a mantener la confidencialidad, disponibilidad e integridad de la información del INM.

DESCRIPCIÓN DE ACTIVIDADES O CONTENIDO PRINCIPAL

La seguridad y privacidad de la información, es un componente transversal a la Estrategia de Gobierno en línea. Este va alineado con la implementación del modelo de seguridad enfocado a preservar la confidencialidad, integridad y disponibilidad de la información, lo que contribuye al cumplimiento de la misión y los objetivos estratégicos de la entidad.

El INM ha venido avanzando en la implantación de este modelo de seguridad y el objetivo es seguir madurándolo a través de este año 2024, cumpliendo con el ciclo de operación del modelo de seguridad y privacidad de la información, donde siempre se hace énfasis en una mejora continua.



Ciclo de operación del modelo de seguridad y privacidad de la información[1]

Para el desarrollo del plan se llevarán a cabo las fases planteadas en el modelo de seguridad y privacidad de la información:

- **Fase de diagnóstico**

Se realizará una revisión del estado de la seguridad del INM a través de herramienta de diagnóstico para evaluar el estado de madurez del SGSI a inicio del año.

- **Fase de planificación**

En esta fase, se continua con el plan establecido en el 2023.

- **Fase de implementación**

En esta fase se da el cumplimiento al plan, con las actividades planteadas para 2024.

- **Fase de evaluación del desempeño y mejora continua**

[1] Modelo de seguridad y privacidad de la información. MinTIC

Con base en la medición de los indicadores se establecen acciones de mejora y se evalúa el progreso del sistema de seguridad de la información.

Estándares utilizados para el desarrollo del Plan

Debido a la actualización de la norma ISO27001, a la versión 2022, la evaluación de diagnóstico se llevará basándose en dicha norma y se actualizará también el formato MSPI.

Los controles de la norma ISO27001:2022 a evaluar e implementar son los siguientes:

Controles de seguridad de la información ISO2001:2022		
No.	**Descripción del control**	**Relación con controles del Anexo A ISO27001:2013**
A5	**Controles organizacionales**	
A.5.1	Política de seguridad de la información	05.1.1, 05.1.2
A.5.2	Roles y responsablidades de seguridad de la información	06.1.1
A.5.3	segregación de tareas	06.1.2
A.5.4	Responsabilidades de la dirección	07.2.1
A.5.5	Contacto con autoridades	06.1.3
A.5.6	Contacto con grupos especiales de interés	06.1.4
A.5.7	Inteligencia de amenzas	New
A.5.8	Seguridad de la información en la administración de proyectos	06.1.5, 14.1.1
A.5.9	Inventario de información y otros activos asociados	08.1.1, 08.1.2
A.5.10	Uso aceptable de la información y otros activos asociados	08.1.3, 08.2.3
A.5.11	Devolución de activos	08.1.4

A.5.12	Clasificación de información	08.2.1
A.5.13	Etiquetado de la información	08.2.2
A.5.14	Transferencia de información	13.2.1, 13.2.2, 13.2.3
A.5.15	Control de acceso	09.1.1, 09.1.2
A.5.16	Gestión de identidades	09.2.1
A.5.17	Authentication information	09.2.4, 09.3.1, 09.4.3
A.5.18	Derechos de acceso	09.2.2, 09.2.5, 09.2.6
A.5.19	Seguridad de la información en relación con proveedores	15.1.1
A.5.20	Abordar la seguridad de la información en los acuerdos con los proveedores	15.1.2
A.5.21	Gestionar la seguridad de la información en la información y la cadena de suministro de tecnologías de la comunicación (TIC)	15.1.3
A.5.22	Seguimiento, revisión y gestión de cambios de servicios de proveedores	15.2.1, 15.2.2
A.5.23	Seguridad de la información en el uso de servicios cloud	New
A.5.24	Planificación y preparación de la gestión de incidentes de seguridad de la información	16.1.1
A.5.25	Evaluación y decisión sobre eventos de seguridad de la información	16.1.4
A.5.26	Respuesta a incidentes de seguridad de la información	16.1.5
A.5.27	Aprender de los incidentes de seguridad de la información	16.1.6
A.5.28	Recolección de evidencia	16.1.7
A.5.29	Seguridad de la información durante la disrupción	17.1.1, 17.1.2, 17.1.3
A.5.30	Preparación de las TIC para la continuidad del negocio	New
A.5.31	Requisitos legales, estatutarios, reglamentarios y contractuales	18.1.1, 18.1.5
A.5.32	Derechos de propiedad intelectual	18.1.2

A.5.33	Protección de registros	18.1.3
A.5.34	Privacidad y protección de la información de identificación personal (PII)	18.1.4
A.5.35	Revisión independiente de la seguridad de la información	18.2.1
A.5.36	Cumplimiento de políticas, normas y estándares de seguridad de la información	18.2.2, 18.2.3
A.5.37	Procedimientos operativos documentados	12.1.1
A6	**Controles de personal**	
A.6.1	Proceso de selección	07.1.1
A.6.2	Términos y condiciones de empleo	07.1.2
A.6.3	Concientización, educación y capacitación en seguridad de la información	07.2.2
A.6.4	Proceso Disciplinario	07.2.3
A.6.5	Responsabilidades después de la terminación o cambio de empleo	07.3.1
A.6.6	Acuerdos de confidencialidad o no divulgación	13.2.4
A.6.7	Trabajo remoto	06.2.2
A.6.8	Informes de eventos de seguridad de la información	16.1.2, 16.1.3
A7	**Controles físicos**	
A.7.1	Seguridad de perímetro físico	11.1.1
A.7.2	Entrada física	11.1.2, 11.1.6
A.7.3	Asegurar oficinas, salas e instalaciones	11.1.3
A.7.4	Monitoreo de seguridad física	New
A.7.5	Protección contra amenazas físicas y ambientales.	11.1.4
A.7.6	Trabajar en áreas seguras	11.1.5
A.7.7	Escritorio y pantalla limpia	11.2.9

A.7.8	Emplazamiento y protección de equipos	11.2.1
A.7.9	Seguridad de los activos fuera de las instalaciones	11.2.6
A.7.10	Medios de almacenamiento	08.3.1, 08.3.2, 08.3.3, 11.2.5
A.7.11	Utilidades de apoyo	11.2.2
A.7.12	seguridad en el cableado	11.2.3
A.7.13	Mantenimiento de equipos	11.2.4
A.7.14	Eliminación segura o reutilización de equipos	11.2.7
A8	**Controles tecnológicos**	
A.8.1	Uso de dispositivos móviles	06.2.1, 11.2.8
A.8.2	Derechos de acceso privilegiado	09.2.3
A.8.3	Restricción de acceso a la información	09.4.1
A.8.4	Acceso al código fuente	09.4.5
A.8.5	Autenticación segura	09.4.2
A.8.6	Gestión de capacidad	12.1.3
A.8.7	Protección contra malware	12.2.1
A.8.8	Gestión de vulnerabilidades técnicas	12.6.1, 18.2.3
A.8.9	Gestión de la configuración	New
A.8.10	Eliminación de información	New
A.8.11	Enmascaramiento de datos	New
A.8.12	Prevención de fuga de datos	New
A.8.13	Copia de seguridad de la información	12.3.1
A.8.14	Redundancia de las instalaciones de procesamiento de información	17.2.1

A.8.15	Inicio sesión	12.4.1, 12.4.2, 12.4.3
A.8.16	Actividades de monitoreo	New
A.8.17	Sincronización de reloj	12.4.4
A.8.18	Uso de programas de utilidad privilegiados	09.4.4
A.8.19	Instalación de software en sistemas operativos	12.5.1, 12.6.2
A.8.20	Seguridad en redes	13.1.1
A.8.21	Seguridad de los servicios de red.	13.1.2
A.8.22	Separación de redes	13.1.3
A.8.23	Filtrado web	New
A.8.24	Uso de criptografía	10.1.1, 10.1.2
A.8.25	Ciclo de vida de desarrollo seguro	14.2.1
A.8.26	Requisitos de seguridad de la aplicación	14.1.2, 14.1.3
A.8.27	Principios de arquitectura e ingeniería de sistemas seguros	14.2.5
A.8.28	Codificación segura	New
A.8.29	Pruebas de seguridad en desarrollo y aceptación.	14.2.8, 14.2.9
A.8.30	Desarrollo subcontratado	14.2.7
A.8.31	Separación de los entornos de desarrollo, prueba y producción	12.1.4, 14.2.6
A.8.32	Gestión del cambio	12.1.2, 14.2.2, 14.2.3, 14.2.4
A.8.33	Información de prueba	14.3.1
A.8.34	Protección de los sistemas de información durante las pruebas de auditoría	12.7.1

El plan de seguridad y privacidad de la información de 2024, se encuentra en el Anexo Seguimiento al Plan de Seguridad y Privacidad de la Información - VIGENCIA 2024 de la OIDT.

DOCUMENTOS RELACIONADOS

Seguimiento al plan de Seguridad y Privacidad de la Información - VIGENCIA 2024

REFERENCIAS BIBLIOGRÁFICAS

1. Norma ISO27001:2022

2. Modelo de Seguridad y Privacidad de la Información. MinTIC.

ANEXOS

Anexo Seguimiento al Plan de Seguridad y Privacidad de la Información - VIGENCIA 2024.

Cronograma de actividades:

ACTIVIDAD	PRODUCTO / ENTREGABLE	PROGRAMACIÓN											
		M1	M2	M3	M4	M5	M6	M7	M8	M9	M10	M11	M12
Actualización del diagnóstico del estado de implementación de SGSI y MSPI	Documento Evaluación SGSI ISO27001:2022 y MSPI												
Documentar la operación de un sistema de monitoreo de ciber seguridad en el SIG	1. Plan de trabajo												
	2. Informes de avance												
Realizar actualización de matriz de activos de información a raíz de cambios en la caracterización de los procesos	Inventario de activos de información actualizado y aprobado												
Actualizar y ejecutar el plan de implementación de controles de la norma ISO 27001:2022	1. Documento con hoja de ruta de implementación de controles												
	2. informes de avance												
Ejecutar un plan de cierre de hallazgos que se relacionen con Seguridad y privacidad de la información	1. Plan de intervención												
	2. Informes de avance (3)												
Ejecutar plan de remediación de vulnerabilidades detectadas en la vigencia 2023	1. Plan de remediación												
	2. informes de avance (3)												
Desarrollar actividades de uso y apropiación del Modelo de Seguridad y Privacidad de la Información	Informe con evidencias de las actividades realizadas												

FICHA DE APROBACION Y CONTROL DE CAMBIOS

Tabla 1. Ficha de aprobación de documentos.

Elaborado por:	**Revisado por:**	**Aprobado por:**
Nombre: Liliana Pineda Aponte **Cargo**:Responsable Seguridad de la información **Fecha**: 2023-12-26	**Nombre**: Rodolfo Gómez **Cargo**: Jefe OIDT **Fecha**: 2023-12-26	Comité Institucional de Gestión y Desempeño/ Acta de aprobación de documentos. **Acta No**. ___ **Fecha**: ____-__-__

Tabla 2. Control de Cambios

FECHA	DESCRIPCIÓN DEL CAMBIO	VERSIÓN
2023-12-26	Creación del documento	1

SERVICIO DE INTERCAMBIO DE INFORMACIÓN HACIENDO USO DEL LENGUAJE COMÚN DE INTERCAMBIO

OIDT

Bogotá

Fecha (2023-12-28)

1. INTRODUCCIÓN

El presente informe trata sobre los desarrollos adelantados para la construcción de los webservices que faciliten el intercambio de información entre el INM y MinCIT, para propósitos de presentar información de laboratorios que solicitan servicios en el INM en el buscador de laboratorios BUSCALAB proyecto de SICAL.

2. ALCANCE

El informe detalla los pormenores técnicos relacionados con la construcción de webservices tipo SOAP Y REST, basados en las definiciones del Diccionario de elementos de datos conceptualizados por las entidades del estado, para el estándar de Lenguaje Común de Intercambio de Información en Colombia.

3. DESCRIPCIÓN METODOLÓGICA

Los sistemas de información se construyen con base en requerimientos que expresan los usuarios y que exige la tecnología actual. La metodología que se utiliza en cada uno de los casos de implementación de software depende de la modalidad de la implementación del software, que bien puede ser por construcción propia in house o adquirida a terceros.

En cualquier caso, la construcción o implantación de software está enmarcada dentro del ciclo de vida de los sistemas de información que siempre incluyen de una forma u otra las etapas de levantamiento de requerimientos, análisis, diseño, construcción, pruebas, ajustes e implementación.

4. RESULTADOS

La estructura de datos resultado de la interacción con este webservice por parte del MinCIT fue definida por MinCIT y contiene la siguiente información:

- Identificador de persona
- Tipo de documento
- Número de documento
- Nombre Empresa
- Dirección
- Código Dane
- Ciudad
- Código Departamento

- Nombre Departamento
- Código País
- Nombre País
- Nombre Fuente
- Autorización publicación

Con base en la consulta de lenguaje común, la cual se encuentra en la url https://lenguaje.mintic.gov.co/utiliza-el-lenguaje/diccionario-de-elementos, se determinaron las siguientes estructuras de datos a utilizar en la definición y respuesta de los webservices construidos

Nombre elemento dato	Identificador	Tipo elemento dato	Capa de uso
Identificador Persona	idPersona	Simple	USO LOCAL
Nombre Tipo Identificación Nacional Persona	nomTipoIdNacionPersona	Simple	USO LOCAL
Número Identificación Tributaria	numIdTributaria	Simple	USO LOCAL
Nombre Persona Jurídica	nombrePersonaJuridica	Simple	USO COMÚN
Dirección	direccion	Compuesto	USO COMÚN
Código DANE	codDANE	Simple	USO LOCAL
Nombre Ciudad	nomCiudad	Simple	USO COMÚN
Código Departamento Alfanumérico 2	codDepartamentoAlf2	Simple	USO LOCAL
Nombre Departamento	nomDepartamento	Simple	USO LOCAL
Código País Alfabético 2	codPaisAlf2	Simple	USO COMÚN
Nombre País ISO 3166-2	nomPaisISO31662	Simple	USO COMÚN
Nombre Fuente Origen	nomFuenteOrigen	Simple	USO LOCAL
Estado Autorización	estadoAutorizacion	Simple	USO LOCAL
Número Teléfono	numTelefono	Simple	USO COMÚN
Dirección Correo Electrónico	direccionCorreoElectronico	Simple	USO COMÚN

Webservice SOAP

El webservice SOAP se construye con base en la librería NuSOAP, la cual es una biblioteca PHP que permite a los desarrolladores crear y consumir servicios web basados en SOAP. Fue creada por Tim A. Bedard, quien es el fundador y desarrollador principal de NuSOAP.

El resultado de las definiciones de campos y estructuras xml para definir el servicio se encuentran en la siguiente url:

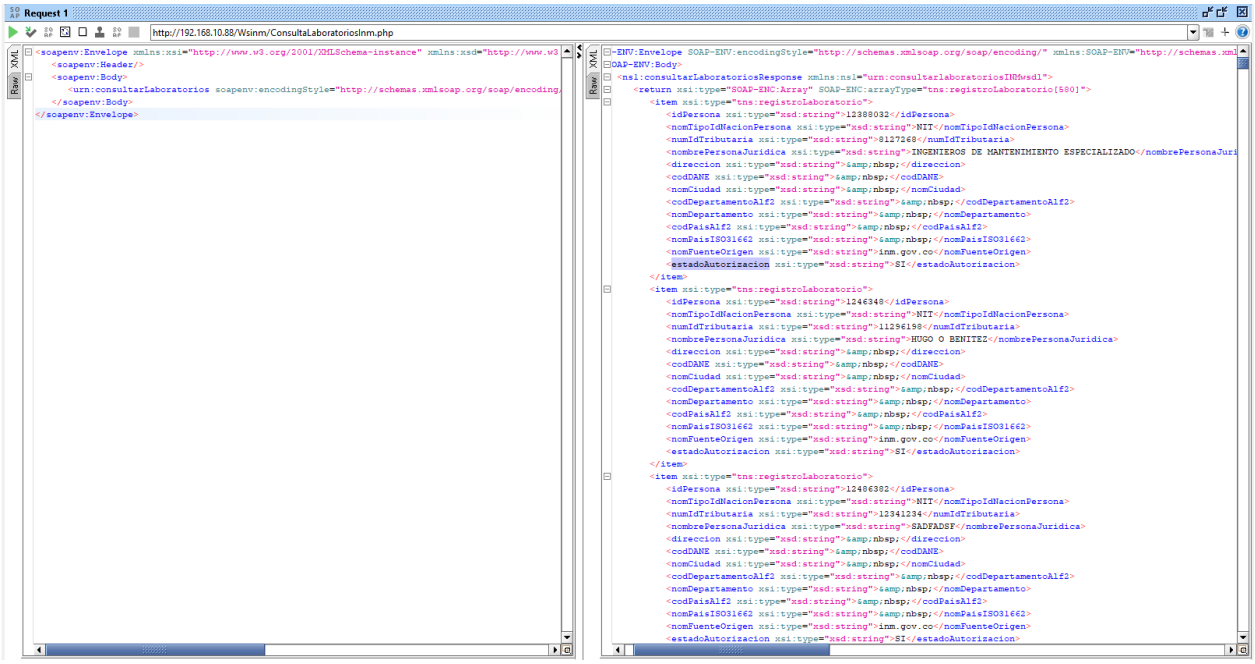
http://192.168.10.88/Wsinm/ConsultaLaboratoriosInm.php?wsdl

Cuya definición se encuentra a continuación

```
<definitions xmlns:SOAP-
ENV="http://schemas.xmlsoap.org/soap/envelope/" xmlns:xsd="http://www.w3.org/2
001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance" xmlns:SOAP-
ENC="http://schemas.xmlsoap.org/soap/encoding/" xmlns:tns="urn:consultarlabora
toriosINMwsdl" xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/" xmlns:wsdl="
http://schemas.xmlsoap.org/wsdl/" xmlns="http://schemas.xmlsoap.org/wsdl/" tar
getNamespace="urn:consultarlaboratoriosINMwsdl">
<types>
<xsd:schema targetNamespace="urn:consultarlaboratoriosINMwsdl">
<xsd:import namespace="http://schemas.xmlsoap.org/soap/encoding/"/>
<xsd:import namespace="http://schemas.xmlsoap.org/wsdl/"/>
<xsd:complexType name="registroLaboratorio">
<xsd:all>
<xsd:element name="iden_pers" type="xsd:string"/>
<xsd:element name="tipo_docu" type="xsd:string"/>
<xsd:element name="nume_docu" type="xsd:string"/>
<xsd:element name="nomb_pers" type="xsd:string"/>
<xsd:element name="domi_dicl" type="xsd:string"/>
<xsd:element name="codi_dane" type="xsd:string"/>
<xsd:element name="nomb_cicl" type="xsd:string"/>
<xsd:element name="codi_regi" type="xsd:string"/>
<xsd:element name="nomb_regi" type="xsd:string"/>
<xsd:element name="codi_pais" type="xsd:string"/>
<xsd:element name="nomb_pacl" type="xsd:string"/>
<xsd:element name="nume_tecl" type="xsd:string"/>
<xsd:element name="dire_emai" type="xsd:string"/>
<xsd:element name="fuen_orig" type="xsd:string"/>
<xsd:element name="pres_terc" type="xsd:string"/>
<xsd:element name="usun_labo" type="xsd:string"/>
<xsd:element name="serv_pres" type="xsd:string"/>
<xsd:element name="auto_publ" type="xsd:string"/>
</xsd:all>
</xsd:complexType>
<xsd:complexType name="arrayLaboratorios">
<xsd:complexContent>
<xsd:restriction base="SOAP-ENC:Array">
<xsd:attribute ref="SOAP-
ENC:arrayType" wsdl:arrayType="tns:registroLaboratorio[]"/>
</xsd:restriction>
```

```
</xsd:complexContent>
</xsd:complexType>
</xsd:schema>
</types>
<message name="consultarLaboratoriosRequest"/>
<message name="consultarLaboratoriosResponse">
<part name="return" type="tns:arrayLaboratorios"/>
</message>
<portType name="consultarlaboratoriosINMwsdlPortType">
<operation name="consultarLaboratorios">
<documentation>Consultar Laboratorios: Este servicio permite la consulta de
laboratorios del INM<br></documentation>
<input message="tns:consultarLaboratoriosRequest"/>
<output message="tns:consultarLaboratoriosResponse"/>
</operation>
</portType>
<binding name="consultarlaboratoriosINMwsdlBinding" type="tns:consultarlaborat
oriosINMwsdlPortType">
<soap:binding style="rpc" transport="http://schemas.xmlsoap.org/soap/http"/>
<operation name="consultarLaboratorios">
<soap:operation soapAction="urn:consultarlaboratoriosINMwsdl#consultarLaborato
rios" style="rpc"/>
<input>
<soap:body use="encoded" namespace="urn:consultarlaboratoriosINMwsdl" encoding
Style="http://schemas.xmlsoap.org/soap/encoding/"/>
</input>
<output>
<soap:body use="encoded" namespace="urn:consultarlaboratoriosINMwsdl" encoding
Style="http://schemas.xmlsoap.org/soap/encoding/"/>
</output>
</operation>
</binding>
<service name="consultarlaboratoriosINMwsdl">
<port name="consultarlaboratoriosINMwsdlPort" binding="tns:consultarlaboratori
osINMwsdlBinding">
<soap:address location="http://192.168.10.88/Wsinm/ConsultaLaboratoriosInm.php
"/>
</port>
</service>
</definitions>
```

A continuación un ejemplo del consumo de este servicio por medio de la herramienta SoapUI



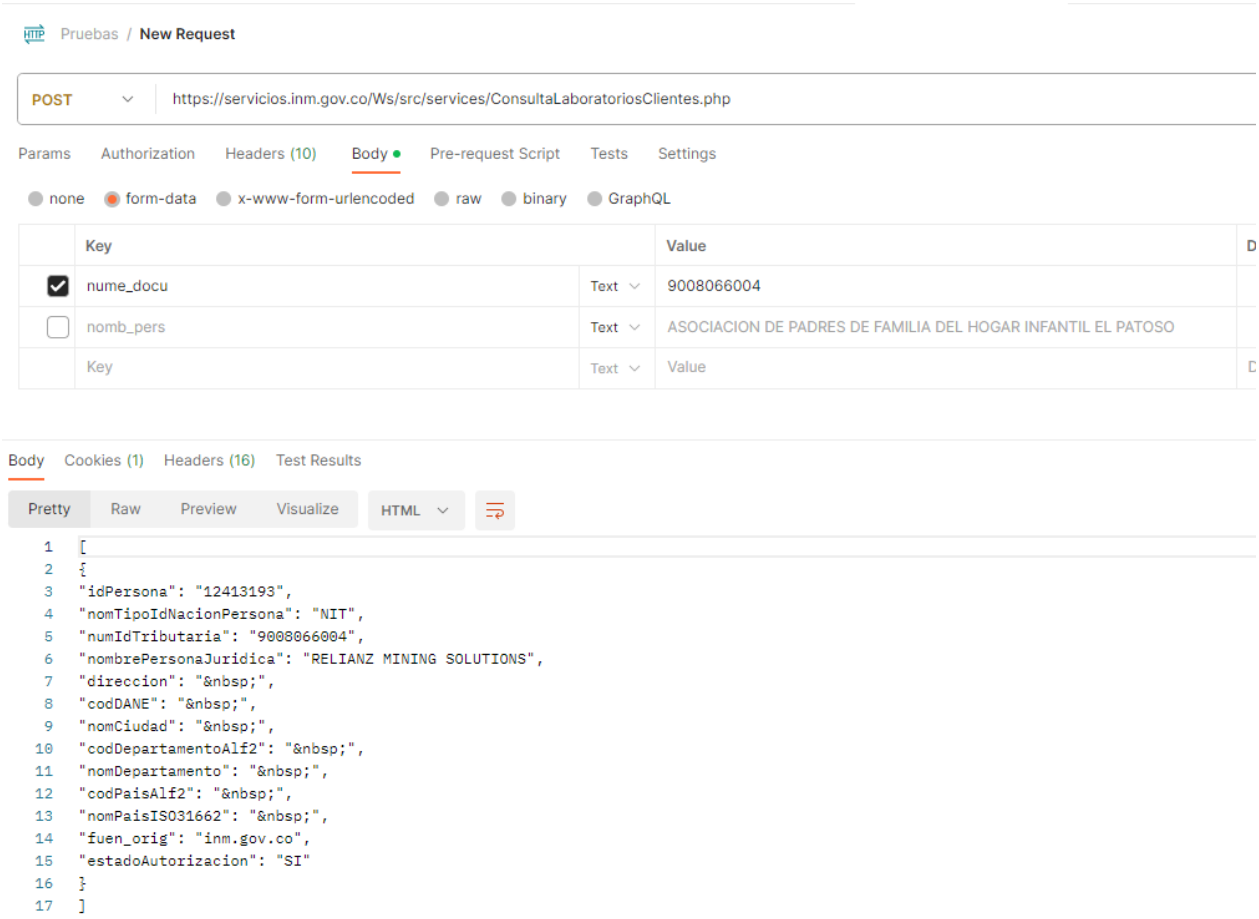
Webservice REST

Esta consulta de laboratorios también tiene su definición en la modalidad REST que permite la consulta parametrizada y resultado mediante estructuras json y se accede mediante petición tipo POST.

La url de este webservice es la siguiente:

https://servicios.inm.gov.co/Ws/src/services/ConsultaLaboratoriosClientes.php

Y el siguiente es un ejemplo del consumo de este servicio parametrizado utilizando la herramienta Postman.



5. CONCLUSIONES

En la actualidad el INM cuenta con los puntos de acceso necesarios para acceder a los webservices de consulta de información de laboratorios que solicitan servicios en la entidad.

El INM se ha preocupado por la versatilidad del acceso y presentación de esta consulta, brindando la posibilidad de accederla vía webservices tipo SOAP o tipo REST.

Si bien por parte del MinCIT en la actualidad no se encuentra definida la continuidad del proyecto del buscador de laboratorios BUSCALAB de SICAL, el INM se encuentra disponible técnicamente para brindar la información necesaria.

Con respecto de la integración del webservice del INM en el catálogo de servicios del Sistema de Información de Gestión del Marco de Interoperabilidad, el cual permite gestionar el proceso estandarización de datos y la publicación de servicios de intercambio Información, para cumplir con los dominios definidos en el Marco de Interoperabilidad para Gobierno Digital, se encuentra en proceso de configuración el servidor XROAD, previendo el apoyo por parte de la Agencia Nacional Digital, una vez se encuentre disponible este recurso.

6. ANEXOS

Cronograma de actividades

Realizó:

José Laureano Urrego
Contratista Desarrollo
Fecha: 2023-12-28