

Bogotá D.C., marzo de 2025.

Señores

DEPARTAMENTO NACIONAL DE PLANEACIÓN

Calle 26 No. 13-19

Ciudad

Asunto: Oferta de Prestación de Servicios Profesionales

Respetados señores,

Con toda atención, presento oferta de presentación de servicios profesionales para “Prestar servicios profesionales en la Dirección de Innovación y Desarrollo Empresarial del Departamento Nacional de Planeación por sus propios medios, con plena autonomía técnica y administrativa en actividades relacionadas con la implementación de instrumentos de política pública y análisis de datos para promover la generación y facilitación del comercio y el fortalecimiento de los encadenamientos productivos”..

De la misma forma acepto los términos y condiciones establecidos por la entidad, relacionadas con el plazo de ejecución contractual y los honorarios, estos últimos en el entendido, que incluyen todos los tributos a que haya lugar.

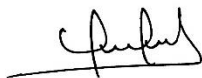
Así mismo, declaro bajo la gravedad de juramento, que no me encuentro incurso en la causal de inhabilidad que trata el artículo 4 de la Ley 1474 de 2011.

“Artículo 4°. Inhabilidad para que ex empleados públicos contraten con el Estado. Adicionase un literal f) al numeral 2 del artículo 8° de la Ley 80 de 1993, el cual quedará así:

Directa o indirectamente las persona que hayan ejercido cargos en el nivel directivo en entidades del Estado y las sociedades en las cuales estos hagan parte o estén vinculados a cualquier título, durante los dos (2) años siguientes al retiro del ejercicio del cargo público, cuando el objeto que desarrollen tenga relación con el sector al cual prestaron sus servicios.

Esta incompatibilidad también operará para las personas que se encuentren dentro del primer grado de consanguinidad, primero civil del ex empleado público”.

Cordialmente,



Firma: _____

Nombre: KELLY JOHANNA SÁNCHEZ SALAMANCA

Cédula de Ciudadanía: 53.039.603 de Bogotá

Bogotá D.C., 11 de marzo de 2025.

Señores

DEPARTAMENTO NACIONAL DE PLANEACIÓN

Calle 26 No. 13-19

Ciudad

Asunto: Declaración juramentada de no estar incurso en causal de inhabilidad o incompatibilidad para contratar con el estado.

Respetados señores,

Por medio de la presente y con ocasión del contrato de prestación de servicios profesionales o apoyo a la gestión, que suscribiré con el Departamento Nacional de Planeación-DNP, me permito declarar bajo la gravedad de juramento que no me encuentro incurso en ninguna de las siguientes causales de inhabilidad o incompatibilidad para contratar con el estado, descritas en la ley, en los artículos 8º de la Ley 80 de 1993; 18 de la Ley 1150 de 2007; 1, 2, 3 y 4 de la Ley 1474 de 2011; 31 y 33 de la Ley 1778 de 2016, y demás normas que complementen, modifiquen o adicioneen causales de inhabilidad o incompatibilidad, sin perjuicio de lo anterior, particularmente según lo establecido en el literal a, b, c y f del numeral 2 del artículo 8 de la ley 80 de 1993:

1. **SI** **NO** he sido miembro de la junta o consejo directivo o servidor público del **DNP** y/o en entidades adscritas al Sector de Planeación (Agencia Nacional de Contratación Pública – Colombia Compra Eficiente, Superintendencia de Servicios Públicos Domiciliarios), desempeñando funciones en el nivel directivo, asesor o ejecutivo en **el último año**, contado a partir de la fecha del retiro (en caso de ser afirmativa su respuesta, indique cargo ejercido y fecha de retiro).

1

2. **SI** **NO** tengo vínculos de parentesco, hasta el segundo grado de consanguinidad (Primer Grado- Padres e Hijos naturales, Segundo Grado- Abuelos, Nietos y Hermanos), segundo de afinidad (Primer Grado- cónyuge, suegro/a (los padres de mi cónyuge), cónyuges de mis hijos/as (yernos y nueras), Cónyuge de mi padre, si no es mi madre- madrastra/ Cónyuge de mi madre, si no es mi padre- padrastro, Segundo Grado-Cónyuges de mis hermanos/as-cuñados, Abuelos/as de mi cónyuge, Cónyuges de mis nietos/as, hermanastros/as (entendiendo como hermanastro/a el hijo/a del cónyuge de mi padre/madre con el que no comparto ningún lazo de sangre) o primero civil (Padre/madre adoptante, Hijo/a adoptado/a) con los servidores públicos de los niveles directivo, asesor ejecutivo o con los miembros de la junta o consejo directivo, o con las personas que ejerzan el control interno o fiscal del **DNP** y/o en entidades adscritas al Sector de Planeación (Agencia Nacional de Contratación Pública – Colombia Compra Eficiente, Superintendencia de Servicios Públicos Domiciliarios).²
3. **SI** **NO** soy el/la cónyuge, compañero o compañera permanente de servidor público en los niveles directivo, asesor, ejecutivo, o de un miembro de la junta o consejo directivo, o de quien ejerza funciones de control interno o de control fiscal en el **DNP** y/o en entidades adscritas al Sector de Planeación (Agencia Nacional de Contratación Pública – Colombia Compra Eficiente, Superintendencia de Servicios Públicos Domiciliarios).³

¹ Literal a del numeral 2 del artículo 8 de la ley 80 de 1993.

² Literal b del numeral 2 del artículo 8 de la ley 80 de 1993.

³ Literal c del numeral 2 del artículo 8 de la ley 80 de 1993.

4. **SI** **NO** he ejercido cargos en el nivel directivo en entidades del Estado (**DNP** y/o en entidades adscritas al Sector de Planeación -Agencia Nacional de Contratación Pública-Colombia Compra Eficiente, Superintendencia de Servicios Públicos Domiciliarios) o las personas que se encuentran dentro de mi primer grado de consanguinidad (**Padres e Hijos naturales**), primero de afinidad (cónyuge, suegro/a-los padres de mi cónyuge, cónyuges de mis hijos/as-yernos y nueras, Cónyuge de mi padre, si no es mi madre- madrastra, Cónyuge de mi madre, si no es mi padre- padrastra), o primero civil (**Padre/Madre adoptante, Hijo/a adoptado/a**) **en mi calidad de ex empleado público** y las sociedades en las cuales estos hagan parte o estén vinculados a cualquier título, cuando el objeto que desarrollen tenga relación con el sector al cual prestaron sus servicios, durante los **dos (2) últimos años**, contados a partir de la fecha del retiro del ejercicio del cargo público (en caso de ser afirmativa su respuesta, indique cargo ejercido y fecha de retiro). _____⁴

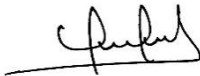
Nota: Téngase presente que el ejercicio del cargo como servidor público o desempeño de las funciones en el nivel directivo, asesor en la entidad pública (**DNP** y/o en entidades adscritas al Sector de Planeación -Agencia Nacional de Contratación Pública-Colombia Compra Eficiente, Superintendencia de Servicios Públicos Domiciliarios), se entiende indistintamente el término o período en el que se ostentó dicha calidad o si fue mediante vínculo directo o bajo encargo.

Así mismo, declaro bajo la gravedad de juramento que **SI** **NO** tengo la condición de deudor o alimentario moroso en cumplimiento a la Ley 2097 de 2021 y Decreto Único Reglamentario 1310 de 2022, por lo tanto, anexo el Certificado del Registro de Deudores Alimentarios Morosos – REDAM.⁵

De igual manera, en caso de presentarse, durante la ejecución del contrato a celebrar con el **DNP**, alguna inhabilidad, incompatibilidad o conflicto de interés, me comprometo a informar de manera **inmediata** al supervisor del contrato, quien a su vez informará a la Subdirección de Contratación, con el fin de adelantar el análisis de la información en aras de mitigar los riesgos de continuar la ejecución del contrato en las situaciones mencionadas.

Por último, manifiesto que tanto el registro de datos e información, así como todos los documentos aportados para la suscripción del contrato, son auténticos, no han sido alterados y contienen información veraz.

Cordialmente,



Firma: _____

Nombre: KELLY JOHANNA SÁNCHEZ SALAMANCA.

Cédula de Ciudadanía No. 53.039.603 de Bogotá.

⁴ Literal f del numeral 2 del artículo 8 de la ley 80 de 1993, literal adicionado por el art. 4, Ley 1474 de 2011.

⁵ Certificado generado a través del link www.redam.gov.co

República de Colombia



La Universidad Libre

Personería Jurídica No. 192 de 1946

y en su representación el Rector y los Profesores, en atención a que

Kelly Johanna Sánchez Salamanca

C.C. No. 53.039.603 de Bogotá, C.E.

ha completado los estudios y demás requisitos que los reglamentos exigen para optar al título de

Especialista en Gerencia Financiera Internacional

en nombre de la República de Colombia y por autorización del Ministerio de Educación Nacional, le expide el presente Diploma que acredita su idoneidad. En testimonio de lo cual se firma y rubrica con el sello mayor de la Institución.

El Decano

UNIVERSIDAD LIBRE
FACULTAD DE CIENCIAS ECONÓMICAS
Y ADMINISTRATIVAS Y CONTABLES
BOGOTÁ
DECANATURA

En la ciudad de Bogotá, C.E.

28 de Agosto del 2015

Acta 265 Folio 265 Libro

El Rector

UNIVERSIDAD LIBRE
RECTORIA NACIONAL

CT. 127798

El Secretario General

UNIVERSIDAD LIBRE
SECRETARÍA GENERAL
BOGOTÁ
Oficina de Admisiones y Registro
28 de agosto del 2015
Registro 46864 Folio 173
Jefe de Admisiones

UNIVERSIDAD LIBRE
SECRETARÍA GENERAL
BOGOTÁ
Registro 024

REPÚBLICA DE COLOMBIA
MINISTERIO DE EDUCACIÓN NACIONAL



LA FUNDACIÓN UNIVERSIDAD DE BOGOTÁ
JORGE TADEO LOZANO

PERSONERÍA JURÍDICA No. 2613 DE 1959. MINJUSTICIA

CON LAS DEBIDAS AUTORIZACIONES LEGALES Y EN CONSIDERACIÓN A QUE

Kelly Johanna Sánchez Salamanca

C. C. 53'039.603 de Bogotá D. C.

TERMINÓ SATISFACTORIAMENTE LOS ESTUDIOS Y CUMPLIÓ LAS PRUEBAS REGLAMENTARIAS,
LE CONFIERE EL TÍTULO DE

***Profesional en
Comercio Internacional***

EN CONSTANCIA SE FIRMA EN BOGOTÁ DISTRITO CAPITAL, A LOS 19 DÍAS DEL MES DE *septiembre*
DEL AÑO 2015

Juanita Linares J
RECTORA

S. Kelson
DECANO

Carlos Sánchez
SECRETARIO GENERAL

LIBRO DE REGISTRO DE GRADO No. 21 , FOLIO 288 , REGISTRO No. 211925

LIBRO ACTAS DE GRADO No. 16 , FOLIO 1568 , ACTA DE GRADO No. 1508

020990

Actuando como vocera del **Patrimonio Autónomo iNNpuls Colombia**, constituido mediante contrato de Fiducia Mercantil No. **006-2017** celebrado de fecha 05 de abril de 2017 y, en consecuencia, comprometiendo única y exclusivamente el patrimonio del citado fideicomiso

CERTIFICA:

Que la señora KELLY JOHANNA SÁNCHEZ SALAMANCA, identificada con cédula de ciudadanía No. 53.039.603 estuvo vinculada al Patrimonio Autónomo iNNpuls Colombia, bajo contrato laboral a término fijo, desde el 16 de noviembre de 2022 hasta el 31 de diciembre de 2024, desempeñando el cargo de EJECUTIVO.

Sus principales funciones fueron:

- Diseñar, ejecutar, evaluar y realizar seguimiento de proyectos, programas y/o instrumentos asignados.
- Investigar, hacer análisis y producir documentos técnicos sectoriales en materia de las temáticas requeridas por el área y afines a los proyectos territoriales.
- Atender las responsabilidades como Supervisor de Contrato que se detallan en el Manual de Contratación
- Gestionar las relaciones con los aliados y operadores con el objetivo de concretar la ejecución de los diferentes proyectos, generando conexiones de valor para el ecosistema de emprendimiento e innovación.
- Participar y atender eventos relevantes de acuerdo a los proyectos asignados.
- Las demás funciones asignadas por su jefe inmediato y que por su naturaleza le correspondan.

Nota: Para validar esta certificación laboral, agradecemos enviar la solicitud correspondiente al correo electrónico administracion.personal@fiducoldex.com.co.

Se expide a solicitud de la interesada, en la ciudad de Bogotá D.C., el 07 de enero de 2025.

Cordialmente,

Firmado digitalmente por
Diana Consuelo Navarro
Fecha: 2025.01.08 08:28:58 -05'00'

DIANA CONSUELO NAVAS NAVARRO
Coordinador de Selección y Contratación.
Fiducoldex S.A.

Proyectó: CM



República de Colombia
Consejo Nacional de Profesiones Internacionales y Afines
CONPIA

CONPIA – PRESIDENCIA 7298/2024

Bogotá D. C., 16 de diciembre de 2024

Señores

A QUIEN INTERESE

E.S.M.

Respetados Señores:

Me permito certificar que la Matrícula Profesional de **KELLY JOHANNA SANCHEZ SALAMANCA**, identificada con cédula de ciudadanía **53039603** de **Bogotá D.C**, **Profesional en Comercio Internacional** egresada de la **Fundación Universidad de Bogotá Jorge Tadeo Lozano**, se encuentra en trámite de aprobación.

Es de aclarar que el parágrafo 2 del artículo 12 del Decreto 717 marzo de 2006 que reglamenta la Ley 556 de febrero 2 de 2000, establece que el CONPIA no expedirá **Tarjeta Profesional, sino Matrícula Profesional**". Es de anotar que si la persona ha proporcionado documentación fraudulenta para la aprobación del presente Certificado de Provisionalidad, el Consejo informará a los organismos de Control del Estado para que estos adelanten las acciones penales pertinentes.

Es importante precisar que la normativa vigente en el Decreto 1083 de mayo de 2015, establece en su **Artículo 2.2.2.3.7**: que *"la experiencia profesional es la adquirida a partir de la terminación y aprobación del pènsum académico de la respectiva formación profesional, en el ejercicio de las actividades propias de la profesión o disciplina académica exigida para el desempeño del empleo"*.

Actualmente la Ley 556 de 2.000, artículo 3º literal g) y las disposiciones reglamentarias que regulan al CONPIA, obliga al Consejo a expedir la matrícula profesional, pero por motivos de implementación tecnológica y de complementación en la normativa de las disposiciones que regulan la expedición de la matrícula profesional, se emite el presente certificado provisional conforme a lo establecido en el inciso segundo del **Artículo 2.2.2.3.3 del Decreto 1083 de 2015 "Certificación Educación Formal"**. Por consiguiente, los certificados que emite el CONPIA física o electrónicamente, donde hace constar que **"se encuentran en trámite de aprobación"** las matrículas profesionales de las personas que ostentan títulos reconocidos en la Ley 556 de 2000 y sus disposiciones reglamentarias, es completamente válido para tomar posesión de cargos públicos o privados, suscribir contratos de prestación de servicios, participar en convocatorias para la provisión de empleos en concurso de méritos y procesos licitatorios, etc.

La presente certificación tiene vigencia de **UN (1) año**, a partir de la fecha de expedición.

"De conformidad con el Decreto 2150 de 1995 y la Ley 962 de 2005, la firma mecánica que aparece a continuación, tiene plena validez para todos los efectos legales y no necesita autenticación, ni sello.

Adicionalmente este documento ha sido firmado digitalmente de conformidad con la ley 527 de 1999 y la resolución 2817 de 2012."

Cordialmente,

HERNÁN ALONSO ZÚÑIGA CARVAJAL

Consejero

CERTIFICADO DE ANTECEDENTES
CERTIFICADO ORDINARIO
No. 266150209



PIB
14:06:54
Hoja 1 de 01

Bogotá DC, 11 de marzo del 2025

La PROCURADURIA GENERAL DE LA NACIÓN certifica que una vez consultado el Sistema de Información de Registro de Sanciones e Inhabilidades (SIRI), el(la) señor(a) KELLY JOHANNA SANCHEZ SALAMANCA identificado(a) con Cédula de ciudadanía número 53039603:

NO REGISTRA SANCIONES NI INHABILIDADES VIGENTES

ADVERTENCIA: La certificación de antecedentes contiene las anotaciones de las sanciones o inhabilidades que se encuentren vigentes. Cuando se trate de nombramiento o posesión en cargos que exijan para su desempeño ausencia de antecedentes, se certificarán todas las anotaciones que figuren en el registro. Anterior, de acuerdo a los incisos 3o. y 4o. del artículo 238 Ley 1952 de 2019.

NOTA: El certificado de antecedentes disciplinarios es un documento que contiene las anotaciones e inhabilidades generadas por sanciones penales, disciplinarias, inhabilidades que se deriven de las relaciones contractuales con el estado, de los fallos con responsabilidad fiscal, de las decisiones de pérdida de investidura y de las condenas proferidas contra servidores, ex servidores públicos y particulares que desempeñen funciones públicas en ejercicio de la acción de repetición o llamamiento en garantía. **Este documento tiene efectos para acceder al sector público, en los términos que establezca la Constitución Política y la ley particular o demás disposiciones vigentes.** El Sistema SIRI reporta como antecedentes solamente las sanciones con debida ejecutoria recibidas de las autoridades nacionales colombianas. En caso de nombramiento o suscripción de contratos con el Estado, es responsabilidad de la Entidad, validar la información de antecedentes del aspirante en la página web: <https://www.procuraduria.gov.co/Pages/certificado-antecedentes.aspx>

Carlos William Rodríguez Millán
Jefe División de Relacionamento con el Ciudadano (C)

ATENCIÓN :

ESTE CERTIFICADO CONSTA DE 01 HOJA(S), SOLO ES VALIDO EN SU TOTALIDAD. VERIFIQUE QUE EL NUMERO DEL CERTIFICADO SEA EL MISMO EN TODAS LAS HOJAS.

LA CONTRALORÍA DELEGADA PARA RESPONSABILIDAD FISCAL ,
INTERVENCIÓN JUDICIAL Y COBRO COACTIVO

CERTIFICA:

Que una vez consultado el Sistema de Información del Boletín de Responsables Fiscales 'SIBOR', hoy martes 11 de marzo de 2025, a las 14:08:51, el número de identificación, relacionado a continuación, NO SE ENCUENTRA REPORTADO COMO RESPONSABLE FISCAL.

Tipo Documento	Cédula de Ciudadanía
No. Identificación	53039603
Código de Verificación	53039603250311140851

Esta Certificación es válida en todo el Territorio Nacional, siempre y cuando el tipo y número consignados en el respectivo documento de identificación, coincidan con los aquí registrados.

De conformidad con el Decreto 2150 de 1995 y la Resolución 220 del 5 de octubre de 2004, la firma mecánica aquí plasmada tiene plena validez para todos los efectos legales.



HERNÁN GUILLERMO JOJOA SANTACRUZ
Contralor Delegado



POLICÍA NACIONAL
DE COLOMBIA



Consulta en línea de Antecedentes Penales y Requerimientos Judiciales

La Policía Nacional de Colombia informa:

Que siendo las 02:10:13 PM horas del 11/03/2025, el ciudadano identificado con:

Cédula de Ciudadanía N° **53039603**

Apellidos y Nombres: **SANCHEZ SALAMANCA KELLY JOHANNA**

NO TIENE ASUNTOS PENDIENTES CON LAS AUTORIDADES JUDICIALES

de conformidad con lo establecido en el artículo 248 de la Constitución Política de Colombia.

En cumplimiento de la Sentencia SU-458 del 21 de junio de 2012, proferida por la Honorable Corte Constitucional, la leyenda “NO TIENE ASUNTOS PENDIENTES CON LAS AUTORIDADES JUDICIALES” aplica para todas aquellas personas que no registran antecedentes y para quienes la autoridad judicial competente haya decretado la extinción de la condena o la prescripción de la pena.

Esta consulta es válida siempre y cuando el número de identificación y nombres, correspondan con el documento de identidad registrado y solo aplica para el territorio colombiano de acuerdo a lo establecido en el ordenamiento constitucional.

Si tiene alguna duda con el resultado, consulte las **preguntas frecuentes** o acérquese a las **instalaciones de la Policía Nacional** más cercanas.



Dirección: Avenida El Dorado # 75
– 25 barrio Modelia, Bogotá D.C.
Atención administrativa: Lunes a
Viernes 8:00 am a 12:00 pm y
2:00 pm a 5:00 pm
Línea de atención al ciudadano:
5159700 ext. 30552 (Bogotá)
Resto del país: 018000 910 112
E-mail: [dijin.araic-
atc@policia.gov.co](mailto:dijin.araic-atc@policia.gov.co)





Presidencia de
la República



Ministerio de
Defensa Nacional



Portal Único
de Contratación



GOV.CO

Todos los derechos reservados.





Portal de Servicios al Ciudadano PSC

Sistema Registro Nacional de Medidas Correctivas RNMC

Consulta Ciudadano

La Policía Nacional de Colombia informa:

Que a la fecha, 11/03/2025 02:11:47 p. m. el ciudadano con Cédula de Ciudadanía N°. **53039603** .

NO TIENE MEDIDAS CORRECTIVAS PENDIENTES POR CUMPLIR.

De conformidad con la Ley 1801 de 2016 "Por la cual se expide el Código Nacional de Seguridad y Convivencia Ciudadana". Registro interno de validación No. **112235693** . La persona interesada podrá verificar la autenticidad del presente documento a través de la página web institucional digitando <https://www.policia.gov.co>, menú ciudadanos/ consulta medidas correctivas, con el documento de identidad y la fecha de expedición del mismo. Esta consulta es válida siempre y cuando el número de cédula corresponda con el documento de identidad suministrado.

Nueva Búsqueda

Imprimir

Información

515 9000

**Dios y
Patria**

Policía Nacional de Colombia
Dirección General - Cra. 59 N° 26 - 21
Centro Administrativo Nacional CAN, Bogotá D.C.
Línea de atención: 018000-910112

**COLOMBIA
POTENCIA DE LA
VIDA**



**MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS
COMUNICACIONES - MINTIC**

CERTIFICA QUE

Una vez consultada la base de datos de deudores alimentarios morosos REDAM, el(la) ciudadano(a) con número de identificación CC 53039603 **NO SE ENCUENTRA INSCRITO EN EL REGISTRO DE DEUDORES ALIMENTARIOS MOROSOS**

Esta certificación es válida en todo el Territorio Nacional, siempre y cuando el tipo y número consignados en el respectivo documento de identificación, coincidan con los aquí registrados.

Se expide en Bogotá el 11/03/2025 02:13 PM



Código Verificación: **439B6WXKEJ**

Válida hasta: **09/06/2025**

Dirección de Gobierno Digital

**MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS
COMUNICACIONES - MINTIC**

CERTIFICADO DE AFILIACIÓN AL POS DE EPS SANITAS

La **EPS SANITAS** en desarrollo de su programa especial para la garantía y prestación del Plan Obligatorio de Salud denominado EPS **SANITAS**,

CERTIFICA

Que Kelly Johanna Sanchez Salamanca, identificado(a) con CC número 53039603, está registrado(a) en el POS DE EPS SANITAS con la siguiente información:

TIPO Y NÚMERO DE IDENTIFICACIÓN	CC 53039603
NOMBRES Y APELLIDOS	Kelly Johanna Sanchez Salamanca
TIPO DE AFILIADO	Titular
PARENTESCO	Titular
FECHA DE NACIMIENTO	24/12/1984
ESTADO DE LA AFILIACIÓN	0 Tiene Derecho A Cobertura Integral
CAUSA ESTADO DE AFILIACIÓN	10 - Cobertura Integral
FECHA DE INGRESO A EPS SANITAS	01/09/2010
FECHA DE RETIRO LABORAL / EPS SANITAS	Activo(a)
SEMANAS COTIZADAS EN EPS SANITAS	430 semanas
SEMANAS COTIZADAS EN OTRA EPS	3000 semanas
SEMANAS COTIZADAS EN ÚLTIMO AÑO	51 semanas
RÉGIMEN	Contributivo
FECHA DE AFILIACIÓN AL RÉGIMEN	04/03/2014
NIVEL SISBEN	No aplica
EMPLEADOR(ES)*	

CEDULA DE CIUDADANIA 53039603 KELLY JOHANNA SANCHEZ
SALAMANCA Desde 21/01/2025 - Vigente N.I.T. 830054060
FIDEICOMISOS SOCIEDAD FIDUCIARIA FIDUCOLDEX Desde
17/11/2022 Hasta 31/12/2024

LA ADMINISTRADORA COLOMBIANA DE PENSIONES - COLPENSIONES

CERTIFICA QUE

Verificada la base de datos de afiliados, el/la señor/a **KELLY JOHANNA SANCHEZ SALAMANCA** identificado/a con documento de identidad **Cédula de Ciudadanía** número **53039603**, se encuentra afiliado/a desde **01/01/2021** al Régimen de Prima Media con Prestación Definida (RPM) administrado por la Administradora Colombiana de Pensiones **COLPENSIONES**.

La presente certificación se expide en Bogotá, el día 11 de marzo de 2025.



Rosa Mercedes Nino Amaya
Dirección de Afiliaciones

Nota: Certificado generado desde la página Web. Este documento no es válido para el reconocimiento de prestaciones económicas, está sujeto a verificación y no tiene costo alguno.

Bogotá D.C., 03/2025

Señores
DEPARTAMENTO NACIONAL DE PLANEACIÓN
Calle 26 #13-19
Ciudad

Asunto: Compromiso de cumplimiento de las responsabilidades de seguridad de la Información

Kelly Johanna Sánchez Salamanca, identificado(a) con **Cédula de ciudadanía** No. 53.039.603 obrando como Proveedor, me comprometo con el cumplimiento de las responsabilidades establecidas en el Modelo de Gobernanza de la Seguridad Digital incluido en el Manual Operativo de Seguridad de la Información(M-PG-07) disponible en <https://colaboracion.dnp.gov.co/CDT/DNP/SIG/M-PG-07%20Manual%20Operativo.Pu.pdf> del Sistema Integrado de Gestión del DNP. Ejerceré mis funciones y/o obligaciones contractuales en la dependencia: **Dirección de Innovación y Desarrollo Empresarial**. Pertenezco a la Entidad **Departamento Nacional de Planeación NIT 899.999.011-0**. Soy usuario del Sistema de información Orfeo, Sisgestión e Intranet.

Cordialmente,

Firma:

Nombre: Kelly Johanna Sánchez Salamanca.

Número de documento de identificación: 53.039.603

"Declaro que la información aquí suministrada es auténtica, veraz, completa, exacta, actualizada. Por lo anterior, cualquier error en la información suministrada será de mi única y exclusiva responsabilidad, asumiéndola por los daños y perjuicios que pudiera ocasionar, como consecuencia de entregar o aportar información falsa, incompleta o inexacta, lo que exonera al DEPARTAMENTO NACIONAL DE PLANEACION - DNP de su responsabilidad ante cualquier proveedor, operador o usuario final, en consecuencia, me someto a las responsabilidades administrativas y/o penales que la legislación colombiana tenga previstos para el efecto y que se deriven de cualquier reticencia o ausencia de integridad o de veracidad de la información suministrada. Autorizo irrevocablemente al DNP, para verificarla o través de los medios que considere conveniente. Igualmente me obligo a actualizar los datos reportados en este documento una vez se produzcan cambios en ellos o cuando el DNP la requiera. Declaro que he leído cuidadosamente el contenido del documento y haberlo comprendido o cabalidad, razón por lo cual entiendo sus alcances, sus implicaciones y autorizo el uso de mi información personal para los fines mencionados y los publicados en el aviso de privacidad disponible en [aviso de privacidad https://www.dnp.gov.co/atencion-al-ciudadano/Paginas/finalidad-de-la-recoleccion-de-datos-personales.aspx](https://www.dnp.gov.co/atencion-al-ciudadano/Paginas/finalidad-de-la-recoleccion-de-datos-personales.aspx)"

Modelo de gobernanza de la seguridad digital incluido en el Manual Operativo de Seguridad de la Información (M-PG-07)

1. Alta Dirección

La Alta Dirección es la máxima autoridad en el sistema. Está conformada por Director(a) General, Subdirector(a) General de Prospectiva y Desarrollo Nacional, Subdirector(a) General de Inversiones, Seguimiento y Evaluación, Subdirector(a) General de Descentralización y Desarrollo Territorial, Subdirector(a) General del Sistema General de Regalías y Secretario(a) General, quienes aseguran la orientación y estructura estratégica y táctica del SIG, la definición y comunicación de las responsabilidades y autoridades requeridas, y realizan las revisiones al desempeño del SIG y aseguran la disponibilidad de recursos. Las responsabilidades en el componente de seguridad de la información son: 1. Propender por la asignación de recursos económicos que permitan el cumplimiento de los objetivos del componente de seguridad de la información y la gestión de la continuidad de negocio (GCN). 2. El Manual del SIG (MC) disponible en <https://colaboracion.dnp.gov.co/CDT/DNP/SIG/MANUAL DEL SIG.Pu.pdf>, en el numeral "Compromiso de la Alta Dirección" describe los compromisos transversales de la Alta Dirección.

2. Comité Institucional de Gestión y Desempeño (CIGD)

Está conformado por el/la Director(a) General o su delegado, el/la Secretario(a) General, quien lo presidirá; el/la Subdirector(a) General de Prospectiva y Desarrollo Nacional o su delegado, el/la Subdirector(a) General de Inversiones, Seguimiento y Evaluación o su delegado, el/la Subdirector(a) General de Descentralización y Desarrollo Territorial o su delegado, el/la Subdirector(a) General del Sistema General de Regalías Territorial o su delegado, el/la Subdirector(a) de Gestión del Talento Humano, el/la Subdirector(a) Administrativo y de relacionamiento con la Ciudadanía, el/la Subdirector(a) Financiero, el/la Subdirector(a) Contractual, el/la Jefe de la Oficina de Tecnología y Sistemas de Información, el/la Jefe de la Oficina Asesora de Comunicaciones, el/la Jefe de la Oficina Asesora Jurídica, el/la Jefe de la Oficina Asesora de Planeación quien será el Secretario Técnico, el/la Jefe de la Oficina de Control Interno, con voz y sin voto. Las responsabilidades en el componente de seguridad de la información son: 1. Asegurar la implementación y desarrollo de las políticas de gestión y directrices en materia de gobierno digital, seguridad digital y de la información. 2. Evaluar las situaciones que hayan dado lugar a un incumplimiento de seguridad de la información y las recomendaciones presentadas por la OTSI. 3. Aprobar las dadas de bajas de software. Autorizar los ejercicios de Ethical hacking e ingeniería social propuestos por la OTSI.

3. Secretaría General (SG)

Formula y hace seguimiento a las acciones necesarias para cumplir las normas y disposiciones que regulan los procedimientos y trámites de carácter administrativo y presupuestal de los planes, programas y proyectos de la Entidad, del Fondo Nacional de Regalías en liquidación y del Sistema General de Regalías según la normatividad vigente. Las responsabilidades en el componente de seguridad de la información son: 1. Evaluar las situaciones que hayan dado lugar a un incidente de seguridad de la información reportados por la OTSI. 2. Liderar la GCN en la Entidad.

4. Oficina de Control Interno Disciplinario (OCID)

Adelanta los procesos disciplinarios en primera instancia contra los servidores o exservidores públicos del DNP, así mismo, promueve políticas, planes y programas de prevención y orientación con el fin de minimizar la ocurrencia de faltas disciplinarias al interior de la Entidad. Las responsabilidades en el componente de seguridad de la información son: 1. Evaluar las situaciones que hayan dado lugar a un incidente de seguridad de la información reportados por la OTSI. 2.Participar en las actividades relacionadas con la GCN en la Entidad.

5. Subdirección de Gestión del Talento Humano (SGTH)

Planea, organiza, dirige, supervisa y controla las actividades relacionadas con el desarrollo y administración del Recurso Humano del DNP, según las disposiciones legales, normativas, institucionales y los criterios técnicos relacionados. Las responsabilidades en el componente de seguridad de la información son: 1. Gestionar las actividades relacionadas con teletrabajo. 2.Informar a la OTSI y a los líderes de técnicos de los sistemas de información, portales y aplicativos el ingreso, retiro y rotación de funcionarios. 3.Hacer uso adecuado de las listas de distribución para envíos masivos correos. 4.Informar a la OTSI los funcionarios autorizados para firmar digitalmente. 5.Participar en las actividades relacionadas con la GCN en la Entidad.

6. Subdirección de Contratación (SCT)

Asesora a la SG en relación con los procesos de contratación en sus diferentes etapas y en los cuales sea parte el DNP, según las disposiciones normativas vigente, legal, institucional y los criterios técnicos relacionados. Las responsabilidades en el componente de seguridad de la información son: 1. Informar a la OTSI y a los líderes de técnicos de los sistemas de información, portales y aplicativos el ingreso, retiro y rotación de contratistas. 2.Apoyar a las dependencias en la cesión de derechos patrimoniales del software. 3.Participar en las actividades relacionadas con la GCN en la Entidad.

7. Subdirección Administrativa y Relacionamento con la Ciudadanía (SARC)

Dirige y guía la prestación de los servicios de apoyo logístico a las diferentes dependencias del DNP, brindando las condiciones físicas adecuadas, de calidad y confort a todos los funcionarios y colaboradores para el desarrollo eficiente de sus actividades misionales. Las responsabilidades en el componente de seguridad de la información son: 1. Ingresar a la póliza de seguridad los bienes adquiridos, transferidos y/o donados al DNP. 2.Gestionar los tokens de firma digital y capacitar a los usuarios en el uso de la firma en el sistema de información ORFEO. Garantizar que los equipos de los centros de datos y de las sedes cuenten con fuentes ininterrumpidas de poder y estabilizadores de potencia. Garantizar el funcionamiento del control de acceso biométrico al centro de datos. 5.Coordinar con la OTSI la limpieza del centro de datos. 6.Garantizar que la Entidad cuente con alarmas de detección de humo y sistemas automáticos de extinción de fuego. 7.Revisar que los equipos de cómputo estén conectados a la red regulada. 8.Garantizar la actualización de los planos conexiones del cableado (voz y eléctricos) en conjunto con el Centro de Servicios. 9.Gestionar la devolución, traslado de los equipos de cómputo. 10.Aprobar el ingreso y salida de equipos de cómputo. 11.Atender las PQRDS (Petición, Quejas, Reclamos, Denuncias y Solicitudes) relacionadas con datos personales. 12.Entregar a las dependencias el mensaje para notificación automática sobre los canales autorizados para radicar las PQRDS en los buzones que reciban y envíen mensajes a los ciudadanos.

8. Oficina Asesora de Comunicaciones (OAC)

Contribuye con la difusión en los círculos académicos, políticos y noticiosos del país, de las actividades adelantadas por el DNP. Las responsabilidades en el componente de seguridad de la información son: 1. Mantener actualizado la relación de delegados web de las dependencias. 2.Entregar las contraseñas de las redes sociales a la OTSI. 3.Velar por el cumplimiento de las políticas de redes sociales. 4.Administrar el grupo de WhatsApp asignado a su dependencia (sí aplica). 5.Hacer uso adecuado de las listas de distribución para envíos masivos correos. 6.Participar en las actividades relacionadas con la GCN en la Entidad.

9. Oficina de Control Interno

Tiene como misión fortalecer el mejoramiento continuo de la gestión institucional, a través de la asesoría multidisciplinaria a las directivas para el adecuado funcionamiento del sistema de control interno fundamentado en el autocontrol, la planeación y la autoevaluación de la gestión. Las responsabilidades en el componente de seguridad de la información son: 1. Realizar auditorías al componente de seguridad de la Información. 2.Participar en las actividades relacionadas con la GCN en la Entidad.

10. Oficina Asesora de Planeación (OAP)

Encargada de coordinar la gestión en los temas de plan de acción, proyectos, presupuesto de inversión y desarrollo organizacional para promover la eficiencia y eficacia del desempeño institucional, según las disposiciones legales, normativas, institucionales y los criterios técnicos relacionados. Las responsabilidades en el componente de seguridad de la información son: 1. Asesorar metodológicamente a las dependencias en las herramientas transversales para la planeación, evaluación y mejora del SIG. 2. Gestionar la aprobación de los cambios en las políticas de seguridad de la información solicitadas por la OTSI. 3.Administrar el grupo de WhatsApp asignado a su dependencia (sí aplica). 4. Articular el desarrollo del plan de articulación de la GCN a nivel de procesos propuesto. 5. Generar los insumos y recomendaciones para la mejora en la fase de implementación de la GCN. 6. Gestionar las actividades de articulación de la GCN con los componentes del SIG.

11. Oficina de Tecnología y Sistemas de Información (OTSI)

Lidera los aspectos relacionados con tecnologías y sistemas de información en el DNP, para el apoyo del cumplimiento de la misión y objetivos institucionales, alineando la tecnología con los procesos de la organización, para ser habilitador del desarrollo de estrategias institucionales de mayor valor agregado para la entidad y el país. Las responsabilidades en el componente de seguridad de la información son: 1. Ejecutar las funciones descritas en el artículo 10 de Decreto 1893 de 2021 y la Resolución 0530 de 2022. 2.Liderar las responsabilidades operacionales del componente de seguridad de la información de acuerdo con numeral "responsabilidad y autoridad" del Manual del SIG (MC) disponible en <https://colaboracion.dnp.gov.co/CDT/DNP/SIG/MANUAL DEL SIG.Pu.pdf>. 3. Presentar al CIGD las situaciones que hayan dado lugar a un incumplimiento de seguridad de la información y las recomendaciones en el componente de seguridad de la información. 4.Presentar al CIGD los ejercicios de Ethical hacking e ingeniería social para aprobación. 5.Reportar a OCID y la SG los incidentes de seguridad que requieran investigación disciplinaria. 6.Presentar junto con SARC las dadas de bajas de software. 7.Apoyar a la Entidad en las actividades de GCN. 8.Realizar la creación, modificación y cancelación de las cuentas de los usuarios en los servicios a su cargo previa solicitud. 9.Analizar las solicitudes de uso de nuevas herramientas de recolección de información. 10.Implementar medidas de seguridad para la protección de la plataforma tecnológica. 11.Gestionar los cambios de acuerdo con el procedimiento de control de cambios. 12.Mantener actualizada la documentación de los servicios tecnológicos. 13.Implementar acuerdos de niveles de servicio con los proveedores de TIC. 14.Establecer los procedimientos tecnológicos para el teletrabajo. 15.Atender las auditorías realizadas por la OCI.

12. Jefes de dependencia, coordinadores de grupo y/o supervisores

Son los conductores operativos de un procedimiento, responsable de velar por la ejecución de las actividades, métodos y documentos descritos, así como de su seguimiento, medición, análisis y mejora. Las responsabilidades en el componente de seguridad de la información son: 1. Garantizar que los colaboradores a su cargo conozcan, cumplan las políticas y participen en las sensibilizaciones de seguridad de la información de conformidad con el Manual de Supervisión e Interventoría(M-CT-02) disponible en <https://colaboracion.dnp.gov.co/CDT/DNP/SIG/M-CT-02 MANUAL DE SUPERVISI% c3% 93N E INTERVENTOR% c3% 8dA.Pu.pdf>. 2.Verificar que los contratos y/o convenios con componente tecnológico que realice la dependencia incluyan los lineamientos en seguridad de la información del Manual de contratación(M-CT-01) disponible en <https://colaboracion.dnp.gov.co/CDT/DNP/SIG/M-CT-01 Manual de Contrataci% c3% b3n.Pu.pdf>. 3.Reportar al centro de servicios las violaciones sobre el uso adecuado de software, incidentes y/o requerimientos. 4.Informar a la SGTH, SCT y líderes de los sistemas de información cuando se registre el ingreso, retiro y/o traslado de un colaborador para que se realice la creación, inactivación de usuario en los activos de información. 5.Verificar la entrega de la información almacenada en los equipos de cómputo, correo electrónico y servicios de Office 365 cuando un colaborador se retire y/o traslade de dependencia. 6.Verificar la devolución de los activos a la SARC cuando un colaborador se retire y/o traslade de dependencia. 7.Supervisar el traslado de activos en su dependencia. 8.Velar por el cumplimiento de las políticas de Whatsapp, confidencialidad, datos personales, GCN (sí aplica). 9.Liderar la actualización, clasificación de los activos de información asignados a la dependencia. 10.Liderar la identificación de riesgos de seguridad de la información. 11.Solicitar concepto técnico a la OTSI para la contratación de servicios profesionales, el licenciamiento, la adquisición, adaptación, construcción y/o mantenimiento de sistemas de información o plataformas digitales. 12.Velar por el cumplimiento del Manual Operativo para la Implementación y Mantenimiento de Sistemas de Información en el diseño y desarrollo de sistemas de disponible en <https://colaboracion.dnp.gov.co/CDT/DNP/SIG/M-TI-01 Manual Op. Implementaci% C3% B3n y Mantenimiento de S.I. DNP.Pu.pdf> en la dependencia. 13.Gestionar ante la SCT la cesión de derechos patrimoniales del software, sistemas de información, aplicativos y portales

desarrollados en la dependencia. 14. Informar a la OTSI sobre los hardware y software que vaya a adquirir, conectar a la plataforma tecnológica del DNP. 15. Velar porque el software adquirido o licenciado por los proyectos y/o programas sea entregado a la OTSI y quede a nombre del DNP. 16. Solicitar al centro de servicios la actualización de las listas de distribución de correo electrónico, las actualizaciones en las restricciones de acceso a páginas de Internet de acuerdo con las necesidades de la dependencia. 17. Aprobar las solicitudes de autorización de software, los permisos de administrador, solicitudes de acceso remoto de su dependencia. 18. Verificar la organización, contenido, permisos y custodia de los discos de red asignados a la dependencia. 19. Ejercer control de las impresiones realizadas en su dependencia. 20. Informar a OAC la actualización de los delegados web. 21. Informar a SGTH la terminación del teletrabajo de los colaboradores de su dependencia. 22. Gestionar que la dependencia configure el mensaje de notificación automática que la SARC definió sobre los canales autorizados para radicar las PQRDS para los buzones que reciben y envían mensajes a los ciudadanos.

13. Gestores SIG

Son los facilitadores designados en cada dependencia, que actúa como enlace directo entre el Administrador del Sistema, los jefes y demás integrantes de la dependencia a la cual pertenecen. Se encargan de difundir todo lo relacionado con el sistema; realizar los requerimientos al Administrador, y mantener actualizados los reportes de indicadores, riesgos, acciones de mejora, entre otros. Las responsabilidades en el componente de seguridad de la información son: 1. Fomentar al interior de la dependencia la participación de los colaboradores en las sensibilizaciones de seguridad de la información. 2. Articular al interior de su dependencia la actualización de los activos de información y la gestión de riesgos de seguridad de la información. 3. Alinear los productos de los planes institucionales con las líneas de acción estratégica del proceso de gestión TIC y clasificadores de productos (Seguridad digital, Gobierno Digital, PETI, Compromisos estratégicos instituciones). 4. El Manual del SIG (MC) disponible en https://colaboracion.dnp.gov.co/CDT/DNP/SIG/MANUAL_DEL_SIG.Pu.pdf, en el numeral "responsabilidad y autoridad" describe los compromisos transversales de los gestores SIG.

14. Líderes funcionales, técnicos y administradores de los sistemas de información

El rol de líder de los servicios de información (sistemas de Información, aplicativos y portales), líder de servicios tecnológicos, personal de sitio e infraestructura del Centro de servicios y/o la OTSI, proveedores con contratos vigentes que apoyen la gestión de la plataforma tecnológica. Las responsabilidades en el componente de seguridad de la información son: 1. Activar y desactivar usuarios en los activos de información (sistemas, aplicativos, y portales) a su cargo de acuerdo con los reportes de las dependencias. 2. Cumplir con los permisos asignados en los servidores y estaciones cliente relacionados con los activos de información. 3. Cumplir con las políticas de software, derechos de autor, confidencialidad, datos personales, GCN. 4. Dar cumplimiento a lo establecido en el Manual Operativo para la Implementación y Mantenimiento de Sistemas de Información en el diseño y desarrollo de sistemas de disponible en <https://colaboracion.dnp.gov.co/CDT/DNP/SIG/M-TI-01 Manual Op. Implementaci%C3%B3n y Mantenimiento de S.I. DNP.Pu.pdf> en el diseño y desarrollo de sistemas de información, aplicativos y portales desarrollados en la dependencia. 5. Implementar el lineamiento de desarrollo seguro de aplicaciones para los activos de información a su cargo. 6. Gestionar la mitigación de las vulnerabilidades en los activos de información a su cargo reportadas por la OTSI. 7. Implementar las medidas técnicas y procedimientos para brindar un nivel apropiado de seguridad de la información en los activos de información a su cargo. 8. Gestionar los cambios en los en los activos de información a su cargo de acuerdo con los procedimientos establecidos. 9. Realizar la sesión de derechos patrimoniales. 10. Reportar las violaciones sobre el uso inadecuado de software, incidentes y/o requerimientos. 11. Gestionar la recolección de evidencia de los incidentes de seguridad de la información. 12. Realizar la gestión de riesgos de seguridad de la información para los activos de información a su cargo. 13. Realiza la actualización de los catálogos y hojas técnicas de servicios de los activos de información a su cargo. 14. Entregar a la OTSI las claves de los activos de información a su cargo. 15. Incluir parámetros de seguridad basado en usuarios, perfiles y roles de los activos de información a su cargo. 16. Velar porque los ambientes productivos de los activos de información a su cargo no tengan versiones de backup. 17. Coordinar pruebas de recuperación de los activos de información a su cargo. 18. Cambiar las contraseñas establecidas por defecto en los activos de información a su cargo. 19. Almacenar el código fuente en Microsoft DevOps Server.

15. Colaboradores (funcionarios, contratistas, pasantes)

Son los encargados de mantener y mejorar el SIG, con el cumplimiento de sus funciones y obligaciones, según corresponda. Las responsabilidades en el componente de seguridad de la información son: 1. Conocer, cumplir el Manual Operativo de Seguridad de la Información (M-PG-07) disponible en <https://colaboracion.dnp.gov.co/CDT/DNP/SIG/M-PG-07 Manual Operativo.Pu.pdf>, el Manual Datos Personales (M-PG-12), Código Único Disciplinario y el Código de Integridad disponible en https://www.dnp.gov.co/LaEntidad/_secretaria-general/subdireccion-gestion-talento/Paginas/codigo-de-integridad.aspx. 2. Presentar las evaluaciones de conocimiento de seguridad de la Información. 3. Dar uso apropiado a los recursos entregados, al usuario y/o claves asignadas. 4. Cumplir con las políticas de correo electrónico, redes sociales, Whatsapp, puesto de trabajo, software, derechos de autor, confidencialidad, datos personales, GCN, acceso remoto, conexión a la red, teletrabajo. 5. Almacenar la información institucional en la plataforma tecnológica del DNP. 6. Entregar a su jefe inmediato y/o supervisor la información almacenada en los equipos de cómputo, correo electrónico y servicios de Office 365 al retirarse y/o trasladarse de dependencia. 7. Devolver los activos a su cargo, gestionar los traslados, salidas de activos y reportar el extravío o hurto a SARC. 8. Reportar al Centro de Servicios cualquier novedad, requerimiento y/o incidente de seguridad en la prestación de algún servicio de TIC. 9. Informar a su jefe inmediato y/o supervisor los incumplimientos en el uso de software y/o derechos de autor. 10. Los delegados web deben mantener la información actualizada. 11. Participar en la actualización, clasificación de los activos de información asignados a la dependencia y la gestión de riesgos de seguridad de la información. 12. Usar el antivirus institucional y herramientas autorizadas por la OTSI recolectar y/o compartir información. 13. Registrar en la portería de los edificios los equipos de su propiedad.

16. Proveedores

Un proveedor cualquier persona o entidad que brinda al DNP bienes, obras o servicios que apoyan a la misión institucional, los servicios tecnológicos y/o fortalecen los controles de seguridad de la información o de tecnología. Las responsabilidades en el componente de seguridad de la información son: 1. Conocer, cumplir el Manual Operativo de Seguridad de la Información (M-PG-07) disponible en <https://colaboracion.dnp.gov.co/CDT/DNP/SIG/M-PG-07 Manual Operativo.Pu.pdf>, el Manual Datos Personales (M-PG-12) disponible en <https://colaboracion.dnp.gov.co/CDT/DNP/SIG/M-PG-12 Manual Datos Personales.Pu.pdf>, Manual Operativo para la Implementación y Mantenimiento de Sistemas de Información en el diseño y desarrollo de sistemas de disponible en <https://colaboracion.dnp.gov.co/CDT/DNP/SIG/M-TI-01 Manual Op. Implementaci%C3%B3n y Mantenimiento de S.I. DNP.Pu.pdf> en el diseño y desarrollo de sistemas de información (si aplica). 2. Cumplir las políticas de confidencialidad, acceso remoto. 3. Gestionar los cambios en los en los activos de información a su cargo de acuerdo con los procedimientos establecidos. 4. Registrar en la portería de los edificios los equipos de su propiedad. 5. Solicitar autorización a la OTSI conectarse a la red. 6. Cumplir los acuerdos de niveles de servicio. 7. Gestionar los riesgos de los servicios ofrecidos. 8. Gestionar incidentes de seguridad e informar de forma oportuna. 9. Identificar áreas de mejora y recomendaciones en el servicio ofrecido. 10. Asegurarse que las personas que hace parte del servicio o soporte cumplan con los requisitos de seguridad establecidos en el contrato. 11. Atender auditorías internas solicitadas por la OTSI evaluar la eficacia de los controles de seguridad relacionados con proveedores. 12. Gestionar la recolección de evidencia de los incidentes informáticos relacionados con la infraestructura tecnológica. 13. Gestionar la mitigación de las vulnerabilidades reportadas por la OTSI. 14. Gestionar la mitigación de las vulnerabilidades reportadas por la OTSI. 14. Mantener la integridad, reserva y confidencialidad de la información que conozca con ocasión del acceso a los activos de información (que incluyen documentos, bases de datos, sistemas de información, material físico, videos, grabaciones de audio e información digital), que la Entidad proporcione, de conformidad con la normativa vigente que incluye Derechos de Autor, Protección de datos personales, Transparencia y Acceso a la Información Pública y Reserva y Responsabilidad, y se encuentra incluida en la normativa del DNP disponible en <https://www.dnp.gov.co/normativa/normograma>. 15. Reconocer la propiedad intelectual y los derechos sobre la información que se genera en el DNP y que son de propiedad exclusiva de la entidad. 16. esperar la confidencialidad de la información entregada por otras fuentes al DNP. 17. Abstenerse de revelar y divulgar la información clasificada, reservada, confidencial y/o con datos personales sensibles, privados, que utilice el DNP, ni dentro de los dos años siguientes a la finalización de estas, sin previo consentimiento por escrito del DNP, siendo consciente de las penas, multas y sanciones derivadas del incumplimiento, al igual de las demás acciones que puedan llegar a derivarse de éste. 18. Realizar un uso y manejo adecuado de la información suministrada por el DNP de acuerdo con las instrucciones que imparta la Entidad y en los lineamientos del Sistema Integrado de Gestión disponible en https://www.dnp.gov.co/LaEntidad/_Direccion-general/oficina-asesora-planeacion/sig/Paginas/sgi.aspx.

17. Usuarios externos sistemas de información

Un usuario externo es cualquier persona o entidad que no hace parte del DNP y que interactúa con los sistemas de información, aplicativos y/o portales institucionales, para realizar tareas específicas o acceder a la información que estos proporcionan. Las responsabilidades en el componente de seguridad de la información incluidas en el Manual Operativo de Seguridad de la Información (M-PG-07) disponible en <https://colaboracion.dnp.gov.co/CDT/DNP/SIG/M-PG-07 Manual Operativo.Pu.pdf> son: Gestionar e implementar los controles de seguridad de la información en su ambiente personal y/o laboral que incluyen la activación y desactivación de usuarios, protección de las contraseñas, actualización del software y dispositivos, conexión segura, identificación de amenazas potenciales, uso de herramientas de seguridad, navegación segura, protección de los dispositivos (equipo de cómputo, dispositivo móvil), medidas de seguridad para equipos compartidos, controles de seguridad física, notificación de incidentes de seguridad, anonimización de datos personales.