Bogotá D.C, **25 DE ENERO DE 2026**

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

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

JORGE IVA RINCON CÓRDOBA , identificado(a) con **Cédula de ciudadanía** No. 79969434 obrando como Contratista 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%20%20Manual%20Operativo.Pu.pdf del Sistema Integrado de Gestión del DNP. Ejerzo mis funciones y/o obligaciones contractuales en la dependencia: **OFICINA ASESORA JURÍDICA.** Pertenezco a la Entidad **DEPARTAMENTO NACIONAL DE PLANEACIÓN NIT899999011 .** Soy usuario del Sistema de información**: Correo electornico, Orfeo**

Cordialmente,

Firma:



Nombre: JORGE IVAN RINCÓN CÓRDOBA.
Número de documento de identificación: 79969434

"Declaro que la información aquí suministrada es auténtica, veraz, completa, exacta, actualizada. Por lo anterior, cualquier error en lo 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 o 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"

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 lideres 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 lideres 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 Relacionamiento 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 (Peticiones, 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 extravió 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. espetar 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.