REPÚBLICA DE COLOMBIA

Libertad y Orden

INSTITUTO NACIONAL DE SALUD

RESOLUCIÓN NÚMERO 0839 **DE** 2025

21 JUL 2025

Por la cual se derogan las resoluciones 0309 de 2022 y 186 del 27 de febrero de 2019 de la Política de Seguridad y Privacidad de la Información en el Instituto Nacional de Salud y se dictan otras disposiciones

LA DIRECTORA GENERAL DEL INSTITUTO NACIONAL DE SALUD

En uso de sus facultades legales contempladas en el numeral 23 del artículo 5 del Decreto 2774 de 2012 y

CONSIDERANDO

Que el artículo 209 de la Constitución Política de Colombia establece que *"la función administrativa está al servicio de los intereses generales y debe desarrollarse con base en los principios de igualdad, moralidad, eficacia, economía, celeridad, imparcialidad y publicidad"*, lo cual implica que todas las actuaciones de las entidades públicas deben orientarse a garantizar el bienestar colectivo, mediante una gestión transparente, eficiente y responsable.

Que el artículo 15 de la misma Constitución reconoce que *"Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en los bancos de datos y en archivos de entidades públicas y privadas. En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución. La correspondencia y demás formas de comunicación privada son inviolables. Sólo pueden ser interceptados o registrados mediante orden judicial, en los casos y con las formalidades que establezca la ley.*

Que la Ley Estatutaria 1581 de 2012, en desarrollo del artículo 15 constitucional, establece el Régimen General de Protección de Datos Personales, imponiendo a las entidades públicas y privadas la obligación de adoptar medidas técnicas, humanas y administrativas que garanticen la seguridad de los datos personales y eviten su adulteración, pérdida, consulta, uso o acceso no autorizado.

Que el Decreto 1074 de 2015, *Decreto Único Reglamentario del sector comercio, industria y turismo,* reglamenta parcialmente la Ley 1581 de 2012, y exige a las entidades públicas la formulación e implementación de políticas internas de tratamiento de datos personales, como parte de su deber de garantizar el derecho fundamental al habeas data.

Que el *Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones 1078 de 2015,* en su artículo 2.2.9.1.2.1, subrogado por el Decreto 767 de 2022, establece como habilitador de la Política de Gobierno Digital *la Seguridad y Privacidad de la Información,* orientando a las entidades públicas a implementar lineamientos que aseguren la confidencialidad, integridad, disponibilidad y privacidad de los datos en todos sus procesos y activos de información.

Que la Resolución 500 de 2021 del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) *"por medio de la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digitaln (MSPI),* incluyendo la gestión de riesgos, la atención de incidentes de seguridad digital y la adopción de estándares técnicos y organizacionales para la protección de la información.

Que la Resolución 2239 de 2024 del MinTIC *"por la cual se actualiza la Política General de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación del Ministerio/Fondo Único de Tecnologías de la Información y las Comunicaciones, se definen*

Por la cual se derogan las resoluciones 0309 de 2022 y 186 del 27 de febrero de 2019 de la Política de Seguridad y Privacidad de la Información en el Instituto Nacional de Salud y se dictan otras disposiciones

lineamientos frente al uso y manejo de la información y se deroga la Resolución 448 de 2022., fortalece la resiliencia institucional frente a amenazas digitales y garantiza la continuidad de los servicios públicos.

Que el Instituto Nacional de Salud (INS), como entidad científica y técnica del orden nacional, tiene la responsabilidad de garantizar la seguridad y privacidad de la información que gestiona, en especial aquella relacionada con datos personales, sensibles y de niños, niñas y adolescentes, en cumplimiento de su misión institucional y en concordancia con los avances normativos, tecnológicos y de gestión pública.

Que mediante las Resoluciones 186 de 2019 y 309 de 2022, el INS adoptó y actualizó su política de seguridad de la información; sin embargo, ante la evolución del marco normativo y los nuevos desafíos en materia de ciberseguridad y protección de datos, se hace necesario derogar dichas resoluciones y adoptar una nueva política integral, moderna y alineada con los estándares nacionales e internacionales vigentes.

Que, dado lo anterior, se hace necesario adoptar la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación del Instituto Nacional de Salud (INS), así como las Políticas Generales de Manejo de la Información, definiendo los lineamientos para su uso, gestión y protección. Y en consecuencia, se debe consolidar una política institucional integral, actualizada y alineada con el marco normativo vigente.

Que, en mérito de lo expuesto este despacho,

RESUELVE

CAPÍTULO I

DISPOSICIONES GENERALES

ARTÍCULO PRIMERO. Objeto.

La presente Resolución tiene por objeto adoptar la Política de Seguridad y Privacidad de la Información, Seguridad Digital, Protección de Datos Personales y Continuidad de la Operación del Instituto Nacional de Salud – INS, así como las Políticas Generales de Manejo y los lineamientos frente a su uso y administración, con el fin de garantizar la protección de los activos de información, la prestación continua de los servicios institucionales, la seguridad de los datos de terceros obtenidos bajo el desarrollo de las actividades misionales y el cumplimiento de los principios de confidencialidad, integridad y disponibilidad de la información.

ARTÍCULO SEGUNDO. Política General de Seguridad y Privacidad de la Información, Seguridad Digital, Protección de Datos Personales y Continuidad de la Operación.

El Instituto Nacional de Salud – INS protege, preserva y administra la confidencialidad, integridad y disponibilidad de la información institucional, así como la seguridad digital, la protección de los datos personales y la gestión de la continuidad de la operación, en concordancia con su mapa de procesos, funciones misionales y el marco normativo vigente. La entidad garantiza el tratamiento adecuado de los datos personales conforme a lo establecido en la Ley 1581 de 2012, el Decreto 1074 de 2015 y demás normas concordantes, asegurando el respeto por los derechos de los titulares y la implementación de medidas técnicas, jurídicas y organizacionales para su protección.

Por la cual se derogan las resoluciones 0309 de 2022 y 186 del 27 de febrero de 2019 de la Política de Seguridad y Privacidad de la Información en el Instituto Nacional de Salud y se dictan otras disposiciones

Asimismo, el INS previene incidentes mediante la gestión integral de riesgos en seguridad y privacidad de la información, seguridad digital y continuidad del negocio, implementando controles físicos, lógicos y administrativos orientados a la mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI). Esta política tiene como finalidad garantizar la prestación ininterrumpida de los servicios científicos, técnicos y de salud pública del INS, con calidad, transparencia y responsabilidad, en beneficio de la ciudadanía, el sistema de salud y las instituciones que conforman el Sistema Nacional de Ciencia, Tecnología e Innovación.

ARTÍCULO TERCERO. Principios orientadores.

La implementación de esta política se regirá por los siguientes principios:

1. **Confidencialidad:** se refiere a la privacidad de los elementos de información almacenados y procesados en un sistema informático, basándose en este principio, las herramientas de seguridad informática deben proteger el sistema de invasiones y accesos por parte de personas o programas no autorizados. Este precepto es particularmente importante en sistemas distribuidos, es decir, aquellos en los que los usuarios, computadores y datos residen en dispositivos diferentes, pero están física y lógicamente interconectados.

2. **Integridad:** se refiere a la validez y consistencia de los elementos de información almacenados y procesados en un sistema informático. Basándose en este principio, las herramientas de seguridad informática deben asegurar que los procesos de actualización estén bien sincronizados y no se dupliquen, de forma que todos los elementos del sistema manipulen adecuadamente los mismos datos. Este postulado es importante en sistemas descentralizados, es decir, aquellos en los que diferentes usuarios, computadores y procesos comparten la misma información.

3. **Disponibilidad:** se refiere a la continuidad del acceso a los elementos de información almacenados u procesados en un sistema informático. Apoyándose en este principio, las herramientas de seguridad informática deben reforzar la permanencia del sistema informático, en condiciones de actividad adecuadas para que los usuarios accedan a los datos con la frecuencia y dedicación que requieran, este fundamento es importante en sistemas informáticos cuyos compromisos con el usuario, es prestar servicio permanente.

4. **Legalidad:** Cumplimiento de la normativa vigente en materia de protección de datos personales, transparencia, acceso a la información pública y seguridad digital.

5. **Responsabilidad compartida:** Es la implementación de medidas por parte de la entidad encargada del tratamiento de datos que le permitan dar el debido cumplimiento a los principios establecidos en el régimen jurídico de la protección de datos de carácter personal.

6. **Mejora continua:** Aplicación del ciclo PHVA (Planear, Hacer, Verificar, Actuar) para fortalecer el sistema de gestión de seguridad de la información.

ARTÍCULO CUARTO. Objetivos.

La Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación del Instituto Nacional de Salud – INS tiene como objetivo general

establecer un marco estratégico y operativo que permita proteger los activos de información de la entidad, asegurar la prestación continua de los servicios institucionales y fortalecer la confianza de los ciudadanos y partes interesadas. Para ello, se establecen los siguientes objetivos específicos:

1. Proteger, preservar y administrar los activos de información, las bases de datos personales y los sistemas tecnológicos utilizados para su procesamiento, frente a amenazas internas o externas, asegurando su confidencialidad, integridad y disponibilidad.

2. Gestionar los riesgos asociados a la seguridad y privacidad de la información, la seguridad digital y la continuidad de la operación, mediante la identificación, análisis, evaluación, tratamiento y monitoreo de estos.

3. Prevenir y mitigar incidentes de seguridad de la información y ciberseguridad, mediante la implementación de controles técnicos, administrativos y físicos, así como mecanismos de respuesta y recuperación.

4. Establecer lineamientos claros para el uso adecuado de los recursos tecnológicos, la gestión de accesos, el tratamiento de datos personales y la protección de la infraestructura tecnológica institucional.

5. Fortalecer la cultura organizacional en materia de seguridad de la información, mediante procesos de sensibilización, formación, comunicación y apropiación de buenas prácticas por parte de funcionarios, contratistas y terceros.

6. Establecer las acciones necesarias para asegurar la mejora continua del sistema de seguridad y privacidad de la información y protección de datos personales.

7. Fortalecer la continuidad del negocio y la recuperación ante desastres, mediante la implementación de planes de continuidad de la operación y recuperación tecnológica, alineados con los objetivos estratégicos del INS.

CAPÍTULO II
POLÍTICAS GENERALES DE MANEJO DE INFORMACIÓN

ARTÍCULO QUINTO. Política de Privacidad y Tratamiento de la Información.

El Instituto Nacional de Salud – INS garantiza el tratamiento adecuado de los datos personales y la información institucional, conforme a lo establecido en la Ley 1581 de 2012, el Decreto 1074 de 2015, la Ley 1712 de 2014 y demás normas concordantes. La entidad cuenta con una Política de Tratamiento de Datos Personales bajo la Resolución 0457 del 3 de junio 2020 que regula la recolección, almacenamiento, uso, circulación y supresión de datos, asegurando el respeto por los derechos de los titulares y la implementación de medidas técnicas, jurídicas y organizacionales para su protección.

ARTÍCULO SEXTO. Política de Seguridad del Talento Humano.

El INS promoverá la apropiación de la cultura de seguridad de la información entre sus funcionarios, contratistas, colaboradores y demás Talento Humano de la Entidad, mediante procesos de inducción, capacitación, sensibilización y compromisos de confidencialidad. El Grupo de Gestión del Talento Humano en coordinación con la Oficina de Tecnologías de la Información y las Comunicaciones, será responsable de

implementar controles para prevenir el uso indebido de la información y los recursos tecnológicos.

PARÁGRAFO. El Grupo de Gestión Contractual deberá incluir en las minutas contractuales, cualquiera que sea su modalidad, cláusulas u obligaciones relacionadas con la Seguridad de la Información, con el fin de reducir el riesgo de pérdida, robo, fraude, uso indebido o suplantación de identidad en el manejo de los medios tecnológicos de la Entidad, asegurando la confidencialidad, disponibilidad e integridad de la información institucional.

ARTÍCULO SÉPTIMO. Política de Gestión de Activos de Información.

El INS identificará, clasificará, protegerá y gestionará sus activos de información, incluyendo documentos, bases de datos, sistemas, aplicaciones, infraestructura tecnológica y recursos humanos asociados. Cada dependencia será responsable de mantener actualizado el inventario de activos de información bajo su custodia, conforme a las guías institucionales de clasificación y etiquetado de la información. Así mismo, cada dependencia será responsable de remitir a la Oficina de Tecnologías de la Información y las Comunicaciones de forma periódica, el inventario de activos de información.

ARTÍCULO OCTAVO. Política de Uso Aceptable de Recursos Tecnológicos.

Todos los usuarios de los sistemas y recursos tecnológicos del Instituto Nacional de Salud – INS deberán hacer uso responsable, ético y conforme a los fines institucionales. Se prohíbe expresamente el uso de los recursos para fines personales, comerciales, políticos o contrarios a la ley. El uso del correo electrónico, internet, dispositivos móviles, medios removibles, software y sistemas de información estará regulado por las políticas internas de seguridad y será monitoreado por la Oficina de Tecnologías de la Información y las Comunicaciones.

Los colaboradores, contratistas, proveedores y operadores que accedan a los activos de información del INS son responsables de cumplir con las políticas establecidas para su uso apropiado. El uso inadecuado de estos recursos puede comprometer la continuidad de la operación y el cumplimiento de la misión institucional. Cada usuario es custodio de sus credenciales de acceso y debe proteger la información institucional bajo su responsabilidad, evitando su pérdida, alteración, destrucción o divulgación no autorizada.

Se deberán observar las siguientes directrices:

1. El correo electrónico institucional debe utilizarse exclusivamente para fines laborales. Está prohibido su uso para actividades personales, comerciales o no autorizadas.

2. El acceso a internet debe realizarse conforme a las categorías y restricciones definidas por la Oficina de Tecnologías de la Información y las Comunicaciones.

3. El uso de software debe limitarse a aquel licenciado o autorizado por el INS. Está prohibida la instalación de programas no aprobados.

4. El uso de dispositivos personales a través de la tendencia "trae tu propio dispositivo" (Bring Your Own Device BYOD), deberá cumplir con los lineamientos técnicos y de seguridad definidos por el INS.

5. Está prohibido almacenar información personal en equipos institucionales o en repositorios oficiales del INS.

6. Todo incidente de seguridad relacionado con el uso de recursos tecnológicos deberá ser reportado de inmediato a través de los canales establecidos.

7. El acceso a la red institucional mediante dispositivos no autorizados deberá ser previamente aprobado y controlado por la Oficina de Tecnologías de la Información y las Comunicaciones.

8. El uso de medios de almacenamiento externo está restringido y solo será autorizado en casos excepcionales, previa evaluación de riesgos, aval del supervisor o jefe inmediato y aprobación por parte de Dirección General.

9. Todo equipo personal que requiera conectarse a la red institucional del INS deberá contar con software licenciado y un sistema antivirus actualizado. Además, deberá ser validado y autorizado por la Oficina de Tecnologías de la Información y las Comunicaciones, mediante la creación de un caso en la herramienta de gestión Aranda.

10. Las credenciales de acceso (usuario y contraseña) a los sistemas, redes y servicios tecnológicos del INS son de carácter estrictamente personal e intransferible. Ningún colaborador, contratista, proveedor u operador está autorizado a compartir sus credenciales con terceros ni a utilizar credenciales ajenas. El incumplimiento de esta disposición será considerado una falta grave y podrá dar lugar a sanciones disciplinarias, contractuales o legales, según corresponda.

11. Todo colaborador es responsable de los registros y modificaciones de información que se hagan a nombre de su cuenta de usuario.

ARTÍCULO NOVENO. Política de Control de Acceso.

El acceso a la información y a los sistemas del INS estará basado en el principio de mínimo privilegio y necesidad de conocer. Se implementarán mecanismos de autenticación, autorización y trazabilidad para garantizar que solo el personal autorizado acceda a los recursos según su rol y funciones. La gestión de usuarios será responsabilidad compartida entre las áreas funcionales y la Oficina de Tecnologías de la Información y las Comunicaciones.

ARTÍCULO DÉCIMO. Política de Seguridad Física y del Entorno.

El Instituto Nacional de Salud – INS establecerá controles para la protección del perímetro de seguridad de sus instalaciones físicas, el control de acceso del personal, la permanencia en las oficinas, y el ingreso a áreas seguras destinadas al procesamiento o almacenamiento de información sensible, así como aquellas que alberguen equipos e infraestructura crítica de soporte a los sistemas de información y comunicaciones. Estos controles estarán orientados a mitigar riesgos y amenazas externas o ambientales que

puedan afectar la confidencialidad, integridad y disponibilidad de la información institucional.

PARÁGRAFO 1. Todos los colaboradores y visitantes que se encuentren en las instalaciones físicas del INS deberán estar debidamente identificados con un documento oficial, el cual deberá portarse en un lugar visible durante su permanencia en la entidad.

PARÁGRAFO 2. Los visitantes del INS deberán estar siempre acompañados por un funcionario autorizado, quien será responsable de su permanencia y desplazamiento dentro de las instalaciones.

PARÁGRAFO 3. El personal de empresas contratistas que desempeñe funciones de forma permanente en las instalaciones del INS deberá portar un carné institucional o distintivo visible que lo identifique como contratista, así como el carné de la ARL correspondiente.

PARÁGRAFO 4. El INS, a través del Grupo Gestión Administrativa o quien haga sus veces, será responsable de contratar y supervisar los servicios de seguridad física, incluyendo el manejo de bitácoras de ingreso y salida, sistemas de control de acceso, y sistemas de videovigilancia (CCTV), con el fin de garantizar el monitoreo y la protección de las instalaciones.

ARTÍCULO DÉCIMO PRIMERO. Política de Seguridad en las Comunicaciones.

La entidad garantizará la integridad, confidencialidad y disponibilidad de la información transmitida a través de redes institucionales. Se implementarán mecanismos de cifrado, segmentación de redes, monitoreo de tráfico y control de accesos remotos. Toda comunicación oficial deberá realizarse a través de canales autorizados y bajo las condiciones de seguridad definidas.

ARTÍCULO DÉCIMO SEGUNDO. Política de Seguridad de las Operaciones.

El INS, a través de la Oficina de Tecnologías de la Información y las Comunicaciones, será responsable de la operación y administración de la infraestructura tecnológica que soporta los servicios institucionales. Se deberán implementar controles para garantizar la eficiencia operativa, la protección de la información y la gestión de cambios de forma controlada.

PARÁGRAFO. Se deberán realizar copias de seguridad periódicas de la información crítica, conforme a los procedimientos establecidos, para asegurar su recuperación ante fallas o incidentes.

ARTÍCULO DÉCIMO TERCERO. Política de Seguridad para Relación con Proveedores.

El INS establecerá mecanismos de control en las relaciones con proveedores y contratistas que accedan a información o infraestructura tecnológica institucional. Se deberán incluir cláusulas contractuales de seguridad de la información y realizar seguimiento al cumplimiento de estas.

PARÁGRAFO. Los proveedores deberán firmar acuerdos de confidencialidad y cumplir con los lineamientos de seguridad definidos por el INS. Toda activación o desactivación de usuarios deberá ser gestionada oportunamente por los supervisores de contrato.

ARTÍCULO DÉCIMO CUARTO. Política de Gestión de Incidentes de Seguridad de la Información.

El INS promoverá el reporte oportuno de incidentes relacionados con la seguridad de la información. Se establecerán procedimientos para su identificación, análisis, tratamiento y documentación, con el fin de mitigar impactos y prevenir recurrencias.

PARÁGRAFO: La Oficina de Tecnologías de la Información y las Comunicaciones será responsable de coordinar la respuesta a incidentes de seguridad de la información y, de acuerdo con la criticidad de cada caso, podrá escalar los incidentes a instancias superiores o a las autoridades competentes, conforme a los procedimientos internos establecidos para la gestión de incidentes.

ARTÍCULO DÉCIMO QUINTO. Política de la Continuidad de la Operación.

El INS implementará planes de continuidad de la operación tecnológica y de recuperación ante desastres, con el fin de garantizar la prestación ininterrumpida de los servicios institucionales. Estos planes deberán ser actualizados y probados periódicamente.

PARÁGRAFO. La Oficina de Tecnologías de la Información y las Comunicaciones, en coordinación con las áreas responsables, liderará la elaboración y activación de los planes de continuidad y recuperación.

ARTÍCULO DÉCIMO SEXTO. Política de Cumplimiento.

El INS velará por el cumplimiento de los requisitos legales, normativos y contractuales relacionados con la seguridad de la información, protección de datos personales, derechos de autor, transparencia y acceso a la información pública.

PARÁGRAFO. La Oficina Asesora Jurídica y la Oficina de Tecnologías de la Información y las Comunicaciones serán responsables de mantener actualizada la matriz de requisitos legales y de verificar su cumplimiento en los procesos institucionales.

ARTÍCULO DÉCIMO SÉPTIMO. Política para el Uso Responsable de la Inteligencia Artificial.

El Instituto Nacional de Salud – INS promoverá el uso responsable, ético, transparente y seguro de tecnologías basadas en Inteligencia Artificial (IA) en el desarrollo de sus funciones misionales, científicas, técnicas y administrativas exclusivamente como fuente de consulta y no como gestor de la actividad misional. Esta política busca garantizar que la implementación de soluciones de IA respete los derechos fundamentales, la protección de datos personales, la seguridad de la información y los principios de equidad, no discriminación y explicabilidad.

PARÁGRAFO 1. Toda iniciativa, proyecto o sistema que utilice algoritmos de IA deberá ser evaluado previamente por la Oficina de Tecnologías de la Información y las Comunicaciones, en coordinación con la Oficina Asesora Jurídica y las áreas funcionales involucradas, para verificar su alineación con los principios institucionales, la normativa vigente y los estándares internacionales en ética digital.

Por la cual se derogan las resoluciones 0309 de 2022 y 186 del 27 de febrero de 2019 de la Política de Seguridad y Privacidad de la Información en el Instituto Nacional de Salud y se dictan otras disposiciones

PARÁGRAFO 2. El INS deberá asegurar que los sistemas de IA utilizados o desarrollados por la entidad cuenten con mecanismos de trazabilidad, supervisión humana, gestión de riesgos y documentación técnica que permita explicar sus decisiones y resultados.

PARÁGRAFO 3. Se prohíbe el uso de herramientas de IA que comprometan la confidencialidad, integridad o disponibilidad de la información institucional, que generen sesgos injustificados, o que no cuenten con licenciamiento, validación técnica o respaldo legal.

PARÁGRAFO 4. La capacitación del talento humano en el uso ético y seguro de la IA será promovida como parte de la cultura institucional de innovación y transformación digital.

CAPÍTULO III
REVISIÓN, VIGENCIA Y DEROGATORIAS
ARTÍCULO DÉCIMO OCTAVO. Revisión.

La Política de Seguridad y Privacidad de la Información, Seguridad Digital, Protección de Datos Personales y Continuidad de la Operación del Instituto Nacional de Salud – INS será revisada anualmente o cuando se presenten cambios normativos, tecnológicos, organizacionales o de riesgo que así lo requieran. La revisión será liderada por la Oficina de Tecnologías de la Información y las Comunicaciones, en coordinación con la Oficina Asesora Jurídica y el Comité Institucional de Gestión y Desempeño.

ARTÍCULO DÉCIMO NOVENO. Vigencia y Derogatoria.

La presente resolución rige a partir de la fecha de su publicación y deroga en su totalidad las Resoluciones No. 186 de 2019 y No. 309 de 2022, así como todas aquellas disposiciones que le sean contrarias.

Dada en Bogotá DC, a los (21) días del mes de julio de 2025.

COMUNÍQUESE Y CÚMPLASE

DIANA MARCELA PAVA GARZÓN
Directora General

Revisó: Henry Alfredo Cruz Rincón Asesor Dirección General
Revisó: Ingrit Lineth Vásquez Cely Jefe Oficina Asesora Jurídica
Revisó: Carlos Andrés López Fernández Jefe de Oficina de Tecnología de Información y Comunicaciones
Proyectó: José Gregorio Rodríguez Duarte Contratista Oficina de Tecnología de Información y Comunicaciones