TABLA DE CONTENIDO

1. OBJETIVO

Establecer políticas y directrices que regulen la seguridad de la información en el Instituto Nacional de Metrología, tendientes a asegurar la confidencialidad, integridad y disponibilidad de los activos de información que soportan el cumplimiento de la misionalidad.

2. ALCANCE

Este manual se desarrolla con el propósito de dar cumplimiento de los requisitos y controles de la Norma NTC-ISO/IEC ISO 27001:2013 y los

lineamientos de la Política de Gobierno Digital que cubre todos los procesos del INM. Las políticas aquí descritas son aplicables a todos los aspectos administrativos y de control que deben ser cumplidos por los colaboradores de la entidad para conseguir un adecuado nivel de protección de las características de calidad, privacidad y seguridad de la información.

3. ABREVIATURAS O SÍMBOLOS

CIGD: Comité Institucional de Gestión y Desempeño

GSIR: Grupo Sistemas de Información y Redes

INM: Instituto Nacional de Metrología

MinTIC: Ministerio de Tecnologías de la Información y Comunicaciones

MinCIT Ministerio de Comercio, Industria y Turismo

MSPI: Modelo de Seguridad y Privacidad de Información.

PQRSD: Peticiones, quejas, reclamos, solicitudes y denuncias.

PSPI. Política de Seguridad y Privacidad de la Información.

SGSI: Sistema de Gestión de Seguridad de la Información

SIG: Sistema Integrado de Gestión.

TI o TIC: Tecnologías de la Información y Comunicaciones.

TRD. Tablas de Retención Documental.

4. DEFINICIONES

Son aplicables los términos y referencias de las leyes o normas que se relacionan:

- Decreto Único Reglamentario del Sector TIC, Decreto 1078 de 2015 Artículo 2.2.17.1.3. Definiciones Generales
- Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional (Ley 1712 de 2014, Artículo 6° Definiciones).
- NTC-ISO /IEC 27000:2018. Capitulo No. 3 Términos y Definiciones.
- Régimen General de Protección de Datos Personales (Ley 1581 de 2012, Artículo 3° - Definiciones)
- Seguridad y Privacidad de la Información MinTIC, Guía Nro. 2 - Numeral 5 Glosario.
- Activo de Información. Elemento relevante y que tiene valor significativo para la organización relacionado con el tratamiento de la información como: sistemas, información en cualquier medio que se encuentre, instalaciones, personas, entre otros. (adaptado de la NTC-ISO /IEC 27001).

5. MARCO NORMATIVO

Ver: [Matriz de requisitos legales]

- Disposiciones Generales para la Protección de Datos Personales (Ley estatutaria 1581 de 2012 y Decreto 1377 de 2013)
- Ley de transparencia y del derecho al acceso a la información pública (Ley 1712 de 2014).
- Lineamientos generales de la Política de Gobierno Digital (Decreto 1008 de 2018)
- Modelo Integrado de Planeación y Gestión - MIPG (Decreto 1499 de 2017)
- Tecnología de la Información. Técnicas de Seguridad. Código de prácticas para el control de seguridad de la información. (GTC ISO/IEC 27002:2015)
- Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos. (NTC ISO/IEC 27001:2013.)
- Tecnología de la Información. Técnicas de Seguridad. Gestión del Riesgo en la Seguridad de la Información (NTC ISO/IEC 27005:2008.).

6. CONTEXTO DE LA ORGANIZACIÓN

6. 1. CONOCIMIENTO DE LA ORGANIZACIÓN Y SU CONTEXTO

La organización y su contexto puede ser consultado en el capítulo 6 del Manual Integrado de Gestión. Adicionalmente a los factores mencionados en el manual citado, se han identificado los siguientes factores que pueden afectar el desempeño u objetivos del SGSI:

De carácter interno:

- Liderazgo y gestión por parte del CIGD
- Asignación de recursos humanos y financieros para la seguridad de la información.
- Capacidad técnica y administrativa debido al tamaño de la entidad.
- Resistencia a la adopción de estándares y nuevos esquemas de trabajo.
- Motivación y compromiso con esquemas de mejoramiento continuo.

De carácter externo:

- Disminución de presupuesto para el INM, por efecto de la situación fiscal.
- Ciberataques cada vez más audaces y preparados.
- Emergencia sanitaria, social, económica y ambiental.

6. 2. COMPRENSIÓN DE LAS NECESIDADES Y EXPECTATIVAS DE LAS PARTES INTERESADAS

La siguiente tabla resume las necesidades y expectativas de las partes interesadas en el SGSI de la entidad

Parte interesada	Tipo	Necesidad o expectativa de seguridad	Fundamento
Entes de certificación, Sistema Interamericano de Metrología (SIM) y Oficina Internacional de Pesas y Medidas (BIPM)	Externo	Cumplimiento de requerimientos de confidencialidad y confiabilidad.	Normas: ISO17025, ISO17034 e ISO17043
Clientes de los servicios ofrecidos por la entidad	Externo	Confidencialidad, disponibilidad e integridad. Protección de datos personales.	Característica inherente al servicio. Acuerdos contractuales.
Personas naturales y jurídicas usuarios de la hora legal	Externo	Disponibilidad	Decreto 4175 de 2011
Ministerio de Comercio, Industria y Turismo	Externo	Integridad y Disponibilidad	Decreto 4175 de 2011
Colaboradores	Interno	Confidencialidad, integridad y disponibilidad. Protección de datos personales.	Ley de protección de datos personales. Cláusulas contractuales.
Subdirección de Metrología Física.	Interno	• Confidencialidad • Control de datos y gestión de la información. • Pruebas (validación) de funcionalidad. • Control de acceso. • Integridad de datos y disponibilidad.	ISO/IEC 17025:2017 Requisitos generales para la competencia de los laboratorios de ensayo y calibración.
Subdirección de Metrología Química y Biomedicina	Interno	• Confidencialidad. • Integridad de datos. (control de acceso e integridad) • Control de registros de la calidad y técnicos. (integridad, confiabilidad, procedimientos de seguridad).	ISO 17034:2016 Requisitos generales para la competencia de los productores de materiales de referencia.
Subdirección de Innovación y Servicios Metrológicos.	Interno	• Pruebas del software y todo equipo que intervenga en el procesamiento de datos. • Acuerdo y manejo de la confidencialidad. • Control de registros (disponibilidad, conservación segura y confidencialidad, procedimientos documentados para asegurar disponibilidad (backups), confidencialidad e integridad. • Rastreabilidad de errores y modificaciones (auditoría).	NTC-ISO/IEC 17043:2010 Evaluación de la conformidad. requisitos generales para los ensayos de aptitud.
Entidades y autoridades de control, gobierno y gestión (MinTIC, DAFP, DNP, Procuraduría General de la Nación, Contraloría General de la Nación, SIC, Etc)	Externo	Integridad y Disponibilidad	Decreto 1008 de 2018, Decreto 620 de 2020, Decreto 612 de 2018, Ley 1581 de 2015, Decreto 1377 de 2013, Ley 1712 de 2014
Proveedores	Externo	Confidencialidad	Cláusulas contractuales.

Tabla # 1. Partes Interesadas en el SGSI

El SGSI propende por el cumplimiento de estos requisitos mediante la implementación y gestión de controles administrativos y técnicos contemplados en la norma NTC-ISO-IEC 27001:2013, como se describe en este documento y documentos relacionados.

6. 3. ALCANCE DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN.

El alcance del SGSI incluye las actividades de: investigación en metrología, prestación de servicios de calibración y medición metrológica, asistencia técnica, capacitación en metrología, ensayos de aptitud, producción de materiales de referencia, control metrológico, coordinación y articulación de la Red Colombiana de Metrología, producción de documentos normativos y diseminación de las mediciones trazables al Sistema Internacional de Unidades, así como las actividades administrativas.

6. 4. SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN.

La estructura del SGSI en el INM es la siguiente:

—La base del sistema lo constituye la NTC-ISO-IEC 27001:2013 conformada por un conjunto de requisitos y controles, los cuales se desarrollan en este manual o en otros documentos del SIG.
—La base del sistema se fortalece por medio de las políticas de Seguridad Digital, el Modelo de Seguridad y Privacidad de MinTIC, cuyos lineamientos parte de la citada norma.
—Uno de los componentes del SGSI es el proceso de análisis y gestión de riesgos ya que, por medio de éste la seguridad se puede anticipar a las situaciones no deseadas.

Estos tres elementos, permiten que los criterios de seguridad (los principales son: confidencialidad, disponibilidad e integridad) se manejen en un ciclo de mejora continua para servir de soporte a los procesos misionales y de apoyo, que incorporan la seguridad como se describió en la tabla Nro. 1.

7. LIDERAZGO

7. 1. LIDERAZGO Y COMPROMISO

Como componente del SIG, al SGSI le aplican el liderazgo y compromiso declarados en el manual integrado de gestión (Ítem 7.1).

7. 2. POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

PSPI 1. La política general se encuentra establecida en el Manual Integrado de Gestión en los ítems 7.2 y 8.1.3.

7. 3. POLÍTICAS ESPECÍFICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La entidad rige sus actividades con la aplicación de las políticas aquí descritas las cuales serán revisadas cada 2 años o cuando existan cambios significativos que lo ameriten.

PSPI 2. Objetivos Específicos de las Políticas de Seguridad y Privacidad de la Información.

1. Administrar los riesgos de seguridad dando cumplimiento a los controles y actividades establecidas.
2. Desarrollar actividades de comunicación, sensibilización y capacitación en lo referente a seguridad y privacidad de la información.
3. Lograr la actualización y publicación anualmente de los Activos de Información del INM.

La siguiente tabla recoge los objetivos e indicadores asociados a las políticas enunciadas.

Compromiso	Objetivo	Forma de medición	Meta	Horizonte
Apalancar la Gestión de Riesgos de Seguridad Digital, como componente relevante y pilar de la seguridad para minimizar la materialización de incidentes y su impacto en activos de información.	Administrar los riesgos de seguridad, dando cumplimiento a los controles y actividades establecidas.	[(Número de actividades asociadas a controles ejecutada) / (Total de actividades programadas en la vigencia) x 100%]	100%	2021
			100%	2022
Establecer las bases para propiciar la toma conciencia y adopción de una cultura para la apropiación y aplicación de los conceptos y controles de seguridad	Desarrollar actividades de comunicación, sensibilización y capacitación en lo referente a seguridad y privacidad de la información	[(Número de actividades ejecutada) / (Total de actividades programadas en la vigencia) x 100%]	95%	2021
			95%	2022
Fortalecer la gestión de los activos por medio de su identificación y actualización del inventario.	Lograr la actualización y publicación periódica de los Activos de Información del INM	Inventario de Activos de Información actualizado	Inventario actualizado	2021
			Inventario actualizado	2022

Tabla # 2. Metas Asociadas a Objetivos

Para el cumplimiento de estos objetivos el INM adopta procedimientos y actividades, algunos de los cuales se describen en la sección 10. Operación de este documento, o mediante documentos que abordan temas específicos, por medio de los cuales la entidad lleva a la práctica su compromiso de mejora continua del sistema de gestión de seguridad de la información. Complementa lo anterior el proceso de análisis, gestión y seguimiento a los riesgos en seguridad y privacidad. 1. Apalancar la Gestión de Riesgos de Seguridad Digital, como componente relevante y pilar de la seguridad para minimizar la materialización de incidentes y su impacto en activos de información.

PSPI 3. Organización de la Seguridad. Las siguientes son las políticas específicas relacionadas con la estructura y responsabilidades sobre seguridad de la información:

1. Dirección Estratégica de Seguridad y Privacidad de la Información. El Comité Institucional de Gestión y Desempeño, es el órgano responsable de avalar y retroalimentar el direccionamiento estratégico de la Seguridad y Privacidad, así como de monitorear la implementación y cumplimiento de las políticas y demás elementos que la componen, conforme a las políticas establecidas por el MIPG.

2. Responsable de Seguridad y Privacidad de la Información. El INM asigna este rol a un(a) funcionario(a) de planta de la entidad que es el(la) encargado(a) de liderar proyectos, procesos y actividades relacionadas con seguridad y privacidad, y actúa como enlace entre los líderes de proceso y el Comité Institucional de Gestión y Desempeño.

3. Dispositivos Móviles. La entidad acorde a las necesidades de movilidad del personal y necesidades de los procesos suministra herramientas tales como: tablets, teléfonos móviles y computadores portátiles y su uso se realiza bajo las siguientes premisas:

- La adquisición de estos dispositivos requiere la aprobación de la alta dirección.
- Estos dispositivos no deben ser usados para reenvío de mensajes (tipo cadena) y en la medida de lo posible evitar que se conviertan en repositorios permanentes de información catalogada como Pública Reservada, Pública Clasificada o de Uso Interno. Por lo anterior corresponde al funcionario realizar revisiones periódicas para migrar la información a los repositorios de tipo corporativos.
- En caso de extravío del dispositivo adicional a las gestiones con el área de Servicios Administrativos, el funcionario informará por escrito vía mail a la mesa de servicios y al responsable de seguridad de la información.

4. Teletrabajo. La entidad adopta el trabajo en casa, conforme a las necesidades y normas que lo regulan, el cual se desarrolla bajo las premisas y lineamientos que se describen en la sección 10.1.2

PSPI 4. Seguridad del Talento Humano. El grupo de gestión del talento humano liderado por su coordinador(a) realiza esfuerzos y aplica controles durante el ciclo laboral de los servidores públicos, esto es; selección, vinculación, permanencia y desvinculación (procedimientos: A-04-P-005 Selección, Vinculación y Permanencia de Personal, A-04-P-006 Desvinculación Laboral y Plan Institucional de Capacitación), con el fin de

asegurar que los servidores conozcan y apliquen las políticas de seguridad y privacidad y que los activos de información no se vean afectados por el cambio de etapa en el ciclo citado. Las responsabilidades de colaboradores y demás partes interesadas en cuanto a seguridad y privacidad se pueden apreciar en el ítem 7.5. Roles, Responsabilidades Y Autoridad En Seguridad De La Información de este manual.

PSPI 5. Gestión de Activos de Información. El responsable de seguridad de la información en coordinación con los dueños de los activos, aplican controles durante el ciclo de vida de los activos, descritos en el Procedimiento de Gestión de Activos de Información (E-05-P-01), para minimizar el riesgo que éstos se vean comprometidos en incidentes, estos controles incluyen, pero no se limitan a los siguientes;

1. Inventario. Los dueños de los activos velan por la actualización permanente del inventario de activos con el apoyo del responsable de seguridad de la información, así como por su adecuada documentación, conforme al formato que hace parte del Procedimiento de Gestión de Activos de Información (E-05-F-03).
2. Dueño del Activo. Todo activo que apoye la misionalidad o la operación del INM tendrá designado un dueño, que es el responsable de definir las medidas de protección y velar por su implementación y adecuada protección.
3. Uso aceptable. Es el uso que se ciñe y cumple alguno de los siguientes criterios:

a) Indicaciones incorporadas en los manuales técnicos o de usuario, del producto en el que se apoyan los procesos misionales o de apoyo del INM.
b) Las establecidas por la ley o políticas, procedimientos y demás documentos del SIG.
c) Las establecidas en este manual. (cobija tanto a funcionarios, contratistas y proveedores).
d) El personal externo (contratistas y proveedores), hace uso de la información y los activos, conforme a las obligaciones contractuales y acuerdos de confidencialidad.

Por otra parte, las actividades que se relacionan a continuación se consideran contrarias al uso apropiado de los recursos o servicios de la entidad:

a) Cualquier actividad orientada a entorpecer, obstruir, bloquear o interferir los servicios de procesamiento de información.
b) Hacer uso de herramientas que evaden los controles de las redes y que comprometan la seguridad de la información o acceder por canales diferentes a los provistos por el GSIR a servidores, bases de datos y sistemas de información.
c) Intervenir o impedir el funcionamiento de controles y medidas de protección y seguridad de la plataforma de la entidad.

4. Clasificación de Información. Cuando se trate de información, ésta deberá estar clasificada conforme a lo establecido en el procedimiento; Gestión de Activos de Información y su formato asociado.

5. Personal Autorizado para la Manipulación de Activos. Los activos sólo podrán ser manipulados o intervenidos por el personal autorizado por el dueño del activo, una vez verificada o asegurada la competencia para esta labor (sea mediante manual de funciones o por autorización vía mail) y en el caso de equipos de cómputo, la intervención y mantenimiento sólo podrá realizarse por el personal autorizado por el coordinador del GSIR o quien haga sus veces. (La autorización para intervención y mantenimiento puede estar implícita como una obligación contractual o explícitamente mediante mail).

6. Devolución de Activos. Al finalizar la labor contractual o laboral con el INM, se aplican controles que permitan asegurar la devolución de los activos que son propiedad de la entidad.

PSPI 6. Control de Acceso a Información y Servicios. El dueño del activo define los niveles de acceso (roles o perfiles) y medidas de seguridad a

sus activos, bajo las siguientes reglas;

1. Todo usuario de los sistemas de información deberá tener una identificación única (código de usuario) que permita identificar de manera inequívoca a la persona que lo utiliza y en ninguna circunstancia será posible el uso de identificadores genéricos o compartidos. Cuando los sistemas de información para compartir información requieran de una sesión autenticada, harán uso de códigos de usuario de servicio y sus credenciales de acceso serán manejadas como información confidencial.
2. Manejo de mecanismos de autenticación. Los mecanismos de autenticación como; contraseñas (passwords), tarjetas inteligentes y carné son de uso personal e intransferible.
3. Necesidad de conocer. Para el desempeño de la función asignada o contratada es requerido el acceso (ej. información).
4. Menor privilegio. Los privilegios de acceso son de 3 niveles; consultar, modificar y eliminar, siendo el de menor nivel la consulta. Se aplicará el menor privilegio posible en la medida que esto permita cumplir la función asignada o contratada.
5. Apoyo tecnológico. El grupo de sistemas de información y redes brindará apoyo técnico cuando el dueño requiera la implementación de tecnologías especializadas para la protección de un activo (Ej. autenticación biométrica).
6. Procedimiento de Control de Acceso a Sistemas de Información y Servicios de Red. El INM utiliza un modelo de gestión de roles, perfiles y usuarios mixto, en el cual algunos accesos son otorgados por el grupo de Sistemas de Información y Redes y en las áreas donde internamente se administran aplicaciones los accesos son gestionados por ellas mismas, el acceso, registro y cancelación de permisos de acceso se realiza conforme a lo establecido en el Procedimiento de Control de Acceso.
7. Autenticación integrada. El INM establece que la autenticación de sus sistemas de información se realizará en forma preferencial de manera integrada con el Directorio Activo, como mecanismo de simplificación operativa y de gestión, sin embargo, en aquellos casos en los cuales este esquema técnicamente no sea el más apropiado o represente riesgo significativo, el líder del proceso puede tomar la decisión de que el sistema de información no se adhiera a este esquema.
8. Sólo se compartirá información a nivel interno a través de la aplicación del Instructivo Configuraciòn de Recursos Compartidos. E-O5-I-010, documento que precisa en detalle las actividades para su control y desempeño.
PSPI 7. Ciframiento y Firma Digital. Para los procesos misionales y de apoyo, en los cuales interviene información pública clasificada o reservada o en transacciones que se realizan bajo el marco de la Ley de Comercio Electrónico (ley 527 de 1999) en los cuales se hace necesario asegurar confidencialidad, integridad y no repudio (desconocimiento de la participación en una transacción) serán aplicadas técnicas de ciframiento y firma digital bajo los estándares de mercado vigentes y operativos; el grupo de sistemas de información y redes dará el apoyo para su implementación y mejora. La gestión y administración de estas herramientas se realiza conforme a los procedimientos, instructivos o guías que se adopten en el INM.

Los elementos que intervienen en la seguridad de estos esquemas, tales como llaves criptográficas, son custodiados con esquemas que protegen su confidencialidad y la máxima restricción posible de acceso, su uso es personal e intransferible y su pérdida o revelación serán tratados como incidentes de alta criticidad. En la eliminación de las llaves (claves asociadas a las firmas digitales) que pierdan su vigencia, ésta se realiza por medio de un mecanismo que evite su recuperación (borrado seguro). El tiempo de vigencia de las claves oscila entre uno y dos años.

PSPI 8. Seguridad Física. El INM establece como áreas de acceso restringido: los laboratorios, data center, áreas y muebles de archivo central y centros de cableado, el acceso a estas áreas es controlado y/o se mantienen bajo llave cuando aplique. (Las características y manejo de estas áreas se encuentran establecidas en la circular 013 de 2016).

PSPI 9. Escritorio Limpio. Debido a que la información que se obtiene y procesa en la misionalidad del instituto, se rige por normas en las cuales se da especial relevancia a los aspectos de confidencialidad, la entidad establece que sobre escritorios y áreas de trabajo no deben permanecer documentos con información catalogada como: Pública Reservada o Pública Reservada o medios removibles que la contenga, con mayor énfasis

en horas no laborales o periodos de ausencia de los servidores.

PSPI 10. Gestión y Operación de las TIC. El grupo de sistemas de información y redes es el responsable de gestionar y operar las TIC que soportan los procesos y servicios del instituto y en cumplimiento de esta responsabilidad, realiza las siguientes actividades, sin estar limitadas a:

1. Documenta la operación de las TIC, mediante manuales, procedimientos, guías e instructivos que hacen parte del SIG. (los cuales aparecen en la sección 11 Documentos Relacionados).
2. Aplica el procedimiento Gestión del Cambio (E-02-P-08) en el despliegue de nuevas herramientas, mantenimiento y mejora de las existentes.
3. Implementa, administra y opera herramientas para la protección de la infraestructura tecnológica para asegurar disponibilidad de los servicios y la protección de la información que fluye interna y externamente al instituto. (Ej. antivirus).
4. Realiza copias de respaldo de la información de los servidores de aplicación, bases de datos y carpetas compartidas (backups), conforme a los acuerdos con los dueños de la información por medio de la aplicación del procedimiento; Backups y Restauración de Información en Equipos de Cómputo y Servidores.
5. Genera y almacena registros de la actividad de los usuarios (logs) conforme las necesidades del proceso operativo que lo requiera.
6. Propende por la identificación y solución de las vulnerabilidades que puedan estar latentes en la infraestructura (incluye hardware y software).
7. Realiza monitoreo, previa autorización del responsable de seguridad de la información del uso de los recursos tecnológicos, con el fin de identificar situaciones que originen riesgo para los activos de información.

Las siguientes políticas aplican de manera específica a servicios o canales de comunicación y a la transferencia de información que fluye por éstos.

8. Gestión de redes y acceso remoto. Las herramientas utilizadas para el acceso remoto y la gestión de las redes serán exclusivamente las autorizadas por el GSIR y en el acceso remoto se aplican controles en cuanto a días y horas de acceso, conforme a las necesidades de la entidad.
9. Servicios como el correo electrónico e internet, son provistos para ser usados acorde a las actividades laborales y profesionales y no deben ser usados con fines: comerciales, políticos, religiosos y cualquier otro que no esté ligado al cumplimiento de sus deberes.
Con respecto a la transferencia y flujo de información por los diversos medios de comunicación, la entidad establece las siguientes políticas:
● Los documentos físicos que contengan información catalogada como: pública reservada, pública clasificada o de uso interno, serán enviados con medidas que protejan su confidencialidad por ejemplo sobres cerrados.
● La información de la entidad catalogada como pública clasificada o reservada no debe ser enviada por medios de comunicación o redes públicas (ej. correo electrónico o internet), cuando éstos no cuenten con medidas que garanticen la confidencialidad, como por ejemplo protocolos y técnicas de encripción, los mecanismos de seguridad a aplicar en cada caso será el resultante de realizar una revisión de los riesgos y las técnicos disponibles y aplicables a cada medio en particular.
● Las opiniones y expresiones que los colaboradores del INM, realicen por medio de canales, medios de comunicación y redes sociales, se entenderán como puntos de vista personales que no necesariamente reflejan la posición del INM y por consiguiente la entidad descarga la responsabilidad de estás comunicaciones en su emisor.
● Los medios de comunicación auspiciados por el INM o que hagan uso de su nombre no podrán ser usados por los colaboradores para actividades de difamación, acoso, suplantación o similares.
● El personal de la entidad que tiene acceso o participa en la producción o tratamiento de información sobre la cual aplican requisitos de confidencialidad contemplados en las normas: NTC-ISO/IEC 17025, NTC ISO 17034 o NTC-ISO/IEC 17043, se abstendrán de sostener conversaciones que versen sobre esta información en: lugares públicos, ascensores, lugares de reunión y demás espacios donde se pueda comprometer la confidencialidad, conforme a los acuerdos de confidencialidad.

PSPI 11. Seguridad de los Sistemas de Información. La adquisición o desarrollo de herramientas de software se rige por las siguientes directrices, las cuales son lideradas y aplicadas por el grupo de sistemas de información y redes;

1. La confidencialidad, disponibilidad e integridad de la información se incorporan en todo el ciclo de vida del software, esto es; desde su especificación y diseño, hasta el mantenimiento.
2. El grupo de sistemas de información y redes es la única área habilitada para la adquisición, mejora, desarrollo, instalación e implementación de TIC y prestará su apoyo para la adquisición de herramientas de metrología que hacen uso de las TIC, con el fin de garantizar estandarización y economías de escala en mantenimiento y soporte. De la misma manera es el área responsable de la custodia y administración de las licencias de software.
3. El mantenimiento o desarrollo de software para la entidad; se realiza bajo el procedimiento de Atención de Requerimientos de Mantenimiento de Software (E-05-P-001) o los que a futuro lo complementen o sustituyan, tiene derechos de autor reservados y se registra como tal ante la autoridad competente.
4. El software adquirido por el INM es exclusivo para su servicio y se rige por los acuerdos de las licencias de uso, quedando expresamente prohibido el uso de software comercial que no haya sido gestionado por conducto del grupo de sistemas de información y redes o que no cumpla con las cláusulas de licenciamiento establecidas por su autor.

PSPI 12. Relación con proveedores. El Grupo de Gestión Jurídica Contractual y de Investigaciones de Carácter Disciplinario y los supervisores establecen controles por medio de cláusulas contractuales, que cubre en lo posible, desde la etapa precontractual hasta la liquidación, los cuales pueden incluir, pero sin estar limitados a;

1. Los contratos de prestación de servicios contienen cláusulas de compromiso con las políticas y normas de seguridad y privacidad de la información, así como la autorización para el tratamiento de sus datos personales.
2. Devolución de activos que le hayan sido entregados para el desarrollo del objeto contractual (si aplica).
3. Existencia y aplicación de un proceso propio de gestión de riesgos, asociado al producto o servicios provisto al INM. (para contratistas o proveedores que son personas jurídicas).
4. Autonomía por parte del INM para la realización de actividades de auditoría al servicio o proceso contratado, liderado por el responsable de seguridad con el apoyo de las áreas involucradas.

PSPI 13. Gestión de Incidentes de Seguridad de la Información. La gestión de incidentes que comprometa un activo de información se adelantará bajo las siguientes premisas;

1. Es responsabilidad del personal que actúa como administrador de la plataforma que resulte afectada o del responsable de seguridad de la información, la investigación y atención de los incidentes relacionados con seguridad de la información, conforme al procedimiento de Gestión de Incidentes de Seguridad de la Información.
2. El cargo que desempeñe el rol de responsable de seguridad de la información (También conocido como Oficial de Seguridad de la Información) es el encargado de la atención de visitas y diligencias de inspección o investigación que adelanten las autoridades.
3. Es responsabilidad de todos los colaboradores reportar a la mesa de servicios, su superior inmediato (supervisor en el caso de contratistas) o a los líderes de proceso, los incidentes que perciban o de los que tengan noticia y que comprometa algún activo de información del INM. La entidad velará por ofrecer canales y mecanismos para que los usuarios de los servicios de la entidad, informen sobre anomalías en pro de la mejora de los servicios de la entidad.
4. El (la) secretario(a) general o el(la) director(a) son los únicos canales de comunicación autorizados para reportar posibles conductas delictivas en cuanto a seguridad de la información a las autoridades; así como para hacer pronunciamientos oficiales en representación del instituto.

PSPI 14. Continuidad de Servicios. El instituto propende por la existencia, prueba y mejora continua de planes y procedimientos que permitan afrontar situaciones de contingencia como:

1. Plan de continuidad de servicios de TIC (conocido como Disaster Recovery Plan, por sus siglas en inglés), liderado por el grupo de sistemas de información y redes.
2. Plan de continuidad de negocios (conocido como Business Continuity Plan, por sus siglas en inglés). Liderado por los responsables de las áreas misionales y de apoyo.

PSPI 15. Cumplimiento de Requisitos Legales. Por medio del normograma el instituto identifica las normas establecidas por las autoridades, éstas se referencian desde procedimientos, guías e instructivos como mecanismo que permite controlar su cumplimiento.

En cuanto a seguridad de la información la entidad vela por el cumplimiento de las leyes de protección de derechos de autor, protección de datos personales, así como las obligaciones contractuales con terceros. Por lo anterior todo software adquirido por el INM se rige por los requisitos de ley y condiciones contractuales.

7. 4. POLÍTICAS DE PROTECCIÓN DE DATOS PERSONALES EN EL INM

Las siguientes son las políticas que el INM aplica para la protección de datos personales que son gestionados en sus procesos de apoyo y están enmarcadas en leyes, en especial: Constitución Nacional, artículos 15 y 20, Ley 1266 de 2008, Ley 734 de 2002, Ley estatutaria 1581 de 2012, decretos reglamentarios 1727 de 2009 , 2952 de 2010 y 1377 de 2013, Ley 1273 de 2009, Resoluciones de la Superintendencia de Industria y Comercio, Sentencias de la Corte Constitucional C-1011 de 2008, C748 de 2011, Ley 1712 de 2014, Ley 599 de 2000, Reglamento Europeo de Protección de Datos Personales 2016/679 y demás normas concordantes.

El objetivo de las políticas que se enuncia a continuación es proteger el derecho de las personas a conocer, actualizar y rectificar la información que sobre ellas se maneja en el INM y aplican sobre las bases de datos que contienen información personal como: información de funcionarios, contratistas, proveedores, usuarios y contactos internacionales.

PSPI 16.Finalidad del Tratamiento Datos Personales.

El tratamiento de datos personales se realiza en la entidad para:

1. Apoyo y soporte a la prestación de servicios misionales entre los que se encuentran los siguientes, sin estar limitados a:
a. Establecer, custodiar y conservar los patrones nacionales de medida correspondientes a cada magnitud.
b. Establecer y operar los laboratorios de referencia de metrología científica e industrial que requiera el país.
c. Establecer, coordinar y articular, la Red Colombiana de Metrología (RCM).
d. Proporcionar servicios de calibración a los patrones de medición de los laboratorios, centros de investigación, a la industria u otros interesados.
e. Realizar las calibraciones de patrones para metrología legal y los ensayos para la aprobación de modelo o prototipo de los instrumentos de medida.
f. Asesorar y prestar servicios, de asistencia técnica a las entidades que lo soliciten.
g. Promover y participar de las comparaciones interlaboratorios y desarrollos de la metrología científica e industrial a nivel nacional e internacional.
h. Realizar estudios sobre las necesidades de medición de los diferentes sectores de la economía que se requieran y publicar documentos de

consulta.

2. Gestión del Talento Humano. El propósito es coordinar, programar, dirigir y supervisar las actividades de: administración del personal, bienestar laboral, seguridad industrial y relaciones laborales, de acuerdo con las políticas de la entidad y las normas legales vigentes.

3. Gestión de Proveedores y Contratistas. El propósito es la contratación y adquisición de bienes y servicios apoyado en el sistema de información diseñado para ello, que incluye: suministrar información a los organismos de control, autoridades administrativas o jurisdiccionales, en especial lo relacionado con el diario único de contratación y entidades como: Cámara de Comercio, Procuraduría General de la Nación y Contraloría General de la República.

4. Atención al ciudadano. El propósito es atender las peticiones, quejas, reclamos, solicitudes y denuncias de los clientes y ciudadanos (PQRSD) por medio del procedimiento; Atención al Ciudadano.

5. Control de visitantes. El propósito es el control, vigilancia y seguridad de las personas, los bienes y las instalaciones del INM, por medio de procedimientos documentados por el área de Gestión Administrativa.

PSPI 17. Principio General.

El INM vela por la protección de derechos como: habeas data, privacidad, intimidad, buen nombre e imagen, con tal propósito sus actuaciones se rigen por principios de buena fe y responsabilidad.

PSPI 18. Principios Específicos.

El INM aplica los siguientes principios específicos para el tratamiento de datos personales, desde su recolección hasta el borrado;

1. Principio de legalidad: En el tratamiento de datos personales se da aplicación a las disposiciones vigentes y aplicables sobre el asunto, así como a los demás derechos fundamentales conexos.

2. Principio de libertad: El tratamiento de datos personales sólo se lleva a cabo con el consentimiento, previo, expreso e informado del titular. Los datos personales no podrán ser tratados sin previa autorización, o sin que exista mandato legal, estatutario o judicial que releve el consentimiento.

3. Principio de finalidad: El tratamiento de datos personales en el INM están subordinados y atienden una finalidad legítima, la cual le es informada a su titular.

4. Principio de veracidad y calidad: El tratamiento de datos personales es veraz, completa, exacta, actualizada, comprobable y comprensible. Se prohíbe el tratamiento de datos parciales, incompletos o fraccionados que puedan inducir a error.

5. Principio de transparencia: En todo momento y sin restricciones se garantiza al titular, obtener información acerca de la existencia de cualquier dato personal que sea de su interés o del cual sea titular.

6. Principio de acceso y circulación restringida: El Tratamiento sólo podrá hacerse por personas autorizadas por el Titular y/o por las personas previstas en la ley. Los datos personales, salvo que sea información pública, no podrán estar disponibles en internet u otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los titulares o terceros autorizados, para este propósito la responsabilidad del INM es de medio.

7. Principio de seguridad. El tratamiento de datos personales se realiza aplicando medidas técnicas y administrativas enfocadas a la confidencialidad, entre las que cabe mencionar el procedimiento de Gestión de Activos de Información, las cláusulas contractuales de confidencialidad, el control de acceso (solicitud de
recurso compartido) entre otros.

8. Principio de confidencialidad: Todas las personas que intervengan en el Tratamiento de datos personales que no tengan la naturaleza de públicos están obligadas a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende el Tratamiento.

PSPI 19. Derechos de los Titulares

Los titulares de los datos personales por medio de peticiones o solicitudes pueden ejercer entre otros, los siguientes derechos;

1. Conocer, actualizar y rectificar sus datos personales frente al INM o terceros encargados por el INM para el tratamiento. Este derecho se puede ejercer, entre otros frente a datos parciales, inexactos o incompletos o que sean contrarios a lo definido en esta política.
2. Solicitar prueba de la autorización otorgada al INM salvo cuando expresamente se exceptúa como requisito para el tratamiento, de conformidad a lo previsto en el artículo 10 de la ley 1581 de 2012.
3. Ser informado respecto del uso, tratamiento y finalidad que se ha dado a sus datos personales.
4. Presentar consultas y reclamos como se describe en la PSPI 25.
5. Revocar la autorización o solicitar la supresión del dato cuando en el tratamiento no se respeten los principios, derechos y garantías constitucionales y legales.
6. Acceder en forma gratuita a sus datos personales que hayan sido objetivo de tratamiento.

PSPI 20. Derechos de menores de edad.

El INM vela por el respecto a los derechos prevalentes de niños, niñas y adolescentes y realizará el tratamiento bajo los siguientes requisitos:

1. Que el tratamiento responda y respete el interés superior del menor.
2. Que esté asegurado el respeto de sus derechos fundamentales.
3. Que se cuente con la autorización del representante legal del menor.

PSPI 21. Deberes del INM como responsable del tratamiento de datos personales:

Las siguientes son las responsabilidades del INM por el tratamiento de datos personales:
1. Garantizar al titular, en todo tiempo, el pleno y efectivo derecho de habeas data.
2. Solicitar y conservar copia de la respectiva autorización otorgada por el titular.
3. Informar debidamente al titular sobre la finalidad de la recolección y los derechos que le asisten por virtud de la autorización otorgada.
4. Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
5. Tramitar las consultas y reclamos formulados en los términos señalados por la ley.
6. Informar a solicitud del titular sobre el uso dado a sus datos.
7. Informar a la autoridad de protección de datos personales cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los titulares.
8. Adoptar procedimientos para garantizar el adecuado cumplimiento de la ley sobre la materia.
9. Cumplir las instrucciones y requerimientos que imparta la autoridad competente.
10. Informar al titular acerca de la entrega de datos a autoridades. Se informará al titular sobre la entrega, cuando esto corresponda a una obligación legal para el INM.

Cuando sean contratados terceros que realicen tratamiento por cuenta del INM (encargado del tratamiento) las responsabilidades son las siguientes:

11. Velar por que la información entregada al encargado sea veraz, completa, exacta, actualizada, comprobable y comprensible.

12. Actualizar o rectificar la información, comunicando de manera oportuna las novedades respecto de los datos que previamente le haya suministrado y adoptar las demás medidas necesarias para que la información, suministrada a este se mantenga actualizada y sea veraz.
13. Suministrar al encargado únicamente datos cuyo tratamiento esté previamente autorizado o no requiera autorización conforme lo establecido por la ley.
14. Exigir al encargado en todo momento, el respeto y cumplimiento de las condiciones y políticas de seguridad y privacidad.
15. Informar al encargado de tratamiento cuando existan datos que se encuentren en discusión por parte del titular, mientras la reclamación se encuentre en trámite.

PSPI 22. Tratamiento Datos Sensibles:

El INM hará tratamiento de datos personales sensibles cuando:

1. El titular haya dado su autorización explícita para dicho tratamiento, salvo en los casos que por ley no sea requerido.
2. El tratamiento tiene una finalidad histórica, estadística o científica. En este evento deben adoptarse las medidas conducentes a la supresión de identidad del titular.

PSPI 23. Autorización:

Cuando el INM actúe como responsable del tratamiento, solicitará autorización previa al titular, la cual se puede obtener con apoyo de medios técnicos que permitan conservar la prueba de la autorización otorgada. La autorización debe ser realizada de manera libre, expresa, voluntaria e inequívoca sobre el tratamiento de los datos conforme a lo establecido en la presente política y en el aviso de privacidad.
La autorización podrá ser dada por un tercero legitimado para actuar, quien debe acreditar su identidad en forma suficiente, adicionalmente puede recibirse por causahabientes, quienes deben acreditar tal calidad o por el representante o apoderado del titular previa acreditación de la representación o apoderamiento.
Se entenderá que la autorización cumple con los requisitos cuando se manifieste por escrito, de forma oral o mediante conductas inequívocas del titular, que permitan concluir de forma razonable que otorgó la autorización. El silencio no se asimila a una conducta inequívoca.
El INM no solicitará la autorización cuando se trate de:
● Información que requiera en ejercicio de sus funciones legales o por orden judicial.
● Datos de naturaleza pública.
● Casos de urgencia médica o sanitaria.
● Tratamiento de información autorizado por ley para fines históricos, estadísticos o científicos.
● Datos relacionados con el Registro Civil de las personas.

PSPI 24. Aviso de Privacidad:

Por medio de este aviso el INM comunica al titular la información relativa a la existencia de políticas de seguridad y privacidad que le son aplicables, la forma de acceder a éstas y las características del tratamiento de los datos. El aviso de privacidad contiene como mínimo la siguiente información:

● Identificación, domicilio y datos de contacto del INM.
● Tratamiento al cual serán sometidos sus datos y la finalidad de este.

● Los derechos que le asisten como titular.

● Mecanismos de acceso a estas políticas. (página web)

PSPI 25. Atención de PQRSD por tratamiento de datos personales.

Las solicitudes de los titulares serán gestionadas por medio del procedimiento de peticiones, quejas, reclamos, sugerencias y denuncias (E-04-P-01), una vez el titular ha radicado la solicitud por alguno de los canales establecidos que aparecen en la siguiente tabla y en su atención se aplican los términos y plazos establecidos por la ley 1581 de 2012, o la que a futuro la complemente o sustituya.

CANAL	DESCRIPCIÓN
Presencial	Av carrera 50 no 26 - 55 Int. 2. Bogotá, D.C. Colombia Ventanilla de recepción de equipos lunes a viernes de 08:00 a 17:00
Línea telefónica	Teléfono: +57 (1) 254222 extensión 1218
Correo electrónico	contacto@inm.gov.co
Redes sociales	Twitter: @inmcolombia - Facebook: INM de Colombia
Página web	https://www.inm.gov.co/contactenos/

Tabla # 3. Canales de Atención

PSPI 26. Cumplimiento de las políticas.

En caso de incidentes que se constituyan en violación a las políticas y que puedan tener incidencia en materia fiscal, penal o administrativa, el responsable de seguridad de la información las pondrá en conocimiento del(la) Secretario(a) General y del CIGD conforme al manejo de incidentes de seguridad de la información.

7. 5. ROLES, RESPONSABILIDADES Y AUTORIDAD EN SEGURIDAD DE LA INFORMACIÓN

Como componente del SIG, al SGSI le aplican los roles y responsabilidades descritas en el anexo 2 del manual integrado de gestión, sin embargo y para facilitar su asimilación por parte del lector se describen otros cargos y roles que juegan un papel importante en el SGSI, partiendo de la base que la seguridad de la información compete a todos y cada uno de los colaboradores de la entidad.

CARGO / ROL	AUTORIDAD	RESPONSABILIDAD
COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO	— Máxima autoridad del S GS I	— Las establecidas en el Anexo 2 del manual del SIG.
COORDINADORES DE GRUPOS Y LÍDERES DE PROCESO	— Exigir el cumplimiento de normas, políticas y actividades asociadas a la seguridad.	— Velar por la ejecución de las actividades propias a sus procesos por medio de las cuales se aplican los controles establecidos en la norma NTC-ISO-IEC 27001:21 y en particular los siguientes: — Revisión del cumplimiento en su área. Este control establece que: "Los directores deben revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas y cualquier otro requisito de seguridad" (Control A.18.2.2). — Revisión de los derechos de acceso de usuario: Este control establece que: "Los propietarios de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares" Control (A.9.2.5)
PROFESIONAL DE LA SECRETARIA GENERAL RESPONSABLE DEL SGSI Y DE SEGURIDAD DIGITAL [1]	— Solicitar el cumplimiento legal, de directrices y políticas de Seguridad y Privacidad en las áreas. — Concertar con las partes interesadas los requisitos y cambios que puedan llegar a afectar el SGSI. — Hacer seguimiento, direccionar y coordinar los recursos relacionados con el SGSI y la Política de Seguridad Digital. — Exigir y velar por el cumplimiento por parte de proveedores, contratistas y demás personal, de los requisitos y procedimientos del SGSI. — Exigir el cumplimiento de los requisitos legales, reglamentarios y/o contractuales relacionados con los derechos de propiedad intelectual y el cumplimiento de los términos de las licencias de software.	— Liderar la implementación de Planes de Mejoramiento. — Liderar el proceso de análisis y gestión de riesgos de seguridad de la información y velar por que estos se mantengan en niveles aceptables. — Reportar cuando aplique y tan pronto como sea posible los eventos o incidentes de seguridad de la información detectados. — Velar por que se establezcan, implementen y mantengan: procedimientos, documentación y actividades del SGSI. — Promocionar programas de sensibilización y toma de conciencia frente a la seguridad de la información. — Asegurarse de la aplicación de los lineamientos y guías de las autoridades en la materia, adaptándolas a los requerimientos y necesidades del INM. — Presentación de informes al CIGD. — Propender por la adopción de una arquitectura de seguridad. — Apoyar el establecimiento de los planes de recuperación de desastres (DRP). — Participar en los proyectos de implementación de servicios o herramientas, que tengan un componente asociado a seguridad digital.

Tabla # 4. Roles y Responsabilidades asociadas al SGSI (primera parte)

Coordinador del GSIR (CIO)	Exigir el cumplimiento de normas, políticas y actividades asociadas a la seguridad.	— Velar por la ejecución de las actividades propias a sus procesos por medio de las cuales se aplican los controles técnicos establecidos en la norma NTC-ISO-IEC 27001:2013,también conocidos como Seguridad Lógica ϸ Seguridad Informática.(En particular los siguientes objetivos de control: Seguridad de las Operaciones- A.12, Seguridad de las Comunicaciones A.13, Adquisición, desarrollo y mantenimiento de sistemas - A.14)
Colaboradores.	— Exigir el cumplimiento de normas, políticas y actividades asociadas a la seguridad.	– Cumplir los lineamientos, políticas y procedimientos de seguridad y privacidad de la información.

Tabla # 5. Roles y Responsabilidades asociadas al SGSI (segunda parte)

8. PLANIFICACIÓN.

8. 1. ACCIONES PARA TRATAR RIESGOS Y OPORTUNIDADES.

El INM determina, valora y define el tratamiento de los riesgos de seguridad digital o de seguridad y privacidad, aplicando la metodología que se describe en el documento; Gestión del Riesgo (E-02-D-001) incluido en el SIG.

Con respecto al tratamiento y conforme a lo establecido por el Departamento Administrativo de la Función Pública la entidad en cada vigencia establece y ejecuta el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, el cual se publica al inicio de cada vigencia en la página web de la entidad.

Debido a que la forma de mitigar los riesgos es la adopción de controles y conforme a lo establecido como requisito por parte de la NTC-ISO-IEC 27001:2013 la siguiente tabla resume la justificación de la necesidad de implementar los controles de la norma y se constituye en la declaración de aplicabilidad. En el Anexo 1 se presenta la justificación detallada de cada uno de los 114 controles de la citada versión de la norma.

ID.	DESCRIPCIÓN	NRO. CONTROLES	JUSTIFICACIÓN
A5	Políticas de la Seguridad de la Información	2	Son requeridos estos controles para que la entidad dé a conocer a las partes interesadas su posición frente a requerimientos legales, normativos y de gestión y de esta manera minimizar el riesgo de incumplimiento por desconocimiento o falta de claridad en su formulación.
A6	Organización de la Seguridad de la Información	7	La entidad requiere establecer la responsabilidad de cada colaborador en cuanto a seguridad de la información, establecer canales para recibir apoyo externo cuando sea requerido, así como evitar el conflicto de intereses y riesgos en el diseño de las funciones de los cargos. En forma similar evitar riesgos por la implementación de nuevos productos o servicios o por el uso de tecnologías y esquemas en auge como el uso de dispositivos móviles o el trabajo remoto, lo que hacen que los controles de este dominio sean necesarios.
A7	Seguridad de los Recursos Humanos	6	Aplica a la entidad los controles establecidos en el ciclo de vida del personal que labora en la entidad desde la selección hasta la terminación de la relación laboral. Estos controles se hacen operativos por medio de los procedimientos del GTH.
A8	Gestión de Activos	10	Es una necesidad para el INM la protección de los activos, por lo que aplican todos los controles de este dominio.
A9	Control de Acceso	14	El alto componente digital que demandan las actividades empresariales y la interacción entre usuarios y sistemas de información, requiere la identificación y autenticación apropiada de los mismos.
A10	Criptografía	2	La entidad provee certificados a sus clientes y realiza operaciones de tesorería que hacen uso de la firma digital por lo que tienen aplicabilidad estos controles en dichos procesos.
A11	Seguridad Física y del Entorno	15	En nuestro entorno la seguridad física es una necesidad no sólo para los equipos de cómputo sino para las áreas de trabajo por lo que estos controles son requeridos en la entidad.
A12	Seguridad de las Operaciones	14	En la entidad son requeridos estos controles para mantener adecuados niveles de servicio, disponibilidad y auditoría y proteger de amenazas como los virus por lo que los controles de este dominio son requeridos.

Tabla # 6. Declaración de Aplicabilidad de Controles – Resumen Conforme al Anexo A de la NTC-ISO-IEC 27001:2013

ID.	DESCRIPCIÓN	NRO. CONTROLES	JUSTIFICACIÓN
A13	Seguridad de las Comunicaciones	7	El alto grado de interconexión y la consiguiente transferencia de información entre los diferentes actores de los procesos, requiere que estos controles brinden seguridad a las comunicaciones para evitar riesgos de pérdida de confidencialidad, integridad, disponibilidad y minimizar su impacto en caso de materialización.
A14	Seguridad en los Procesos de Desarrollo y Soporte	13	En la entidad se realiza desarrollo y mantenimiento del software al igual que se adquiere e implementa software desarrollado por terceros, razón por la cual tienen aplicabilidad los controles relacionados con el ciclo de vida del software, así como los que propenden por mantener la seguridad en canales y redes no controladas por la entidad.
A15	Relaciones con los proveedores	5	El tamaño y capacidad de la entidad da origen a la contratación de servicios profesionales y de apoyo técnico que deben ser supervisados y controlados, asegurando que los riesgos inherentes a estos servicios sean tratados y gestionados de manera adecuada, por lo que son requeridos estos controles.
A16	Gestión de Incidentes de Seguridad de la Información	7	Es una necesidad para toda organización minimizar el impacto de los incidentes y dar un tratamiento adecuado ya que permiten mejorar y medir el desempeño del SGSI, por lo que estos controles son necesarios.
A17	Aspectos de Seguridad de la Información de la Gestión de Continuidad de Negocio	4	Ante una contingencia es necesario que la seguridad mantenga niveles apropiados de seguridad y que la tecnología brinde soporte a los procesos de negocio y de apoyo, razón por la que estos controles tienen aplicabilidad en la entidad.
A18	Cumplimiento	8	Para evitar que la entidad se afecte negativamente por incumplimiento de normas u obligaciones contractuales son requeridos estos controles al igual que los que propenden por la efectividad y mejora continua por medio de la revisión y auditoría.
Total controles aplicables		114	

Tabla # 7. Declaración de Aplicabilidad de Controles – Resumen Conforme al Anexo A de la NTC-ISO-IEC 27001:2013

8. 2. OBJETIVOS DEL SGSI Y PLANES PARA LOGRARLOS.

El objetivo del SGSI es gestionar y mitigar los riesgos de seguridad digital por medio de la implementación de requisitos y controles de la norma NTC-ISO-IEC 27001:2013 y para el logro de este objetivo, en cada vigencia se planea y se ejecuta el Plan Operativo de Seguridad y Privacidad, así como el Plan de Tratamiento de Riesgos, lo cuales se establecen y publican al inicio de cada vigencia conforme a las normas vigentes.

9. SOPORTE DEL SGSI.

9. 1. RECURSOS.

Los siguientes son los recursos humanos que la entidad determina para la gestión del SGSI:

• Responsable de Seguridad de la Información: Profesional de la entidad que coordina y monitorea la seguridad de la información en la entidad, sus responsabilidades aparecen en la sección 7.4 de este documento.

• Administradores de herramientas y plataformas: Profesionales del GSIR, encargados de la administración y gestión de herramientas de seguridad. (seguridad informática).

• Apoyo para la gestión del sistema: Contratista experto o especializado en Sistema de Gestión de Seguridad de la Información o Riesgos, requerido para la gestión y operación del sistema.

Complementa a los recursos humanos las herramientas de hardware o software que usa la entidad para proteger la infraestructura, las cuales son

adquiridas o licenciadas conforme a los presupuestos anuales.

9. 2. COMUNICACIÓN.

La siguiente tabla esquematiza a manera de guía las comunicaciones y las responsabilidades relacionadas con éstas, por medio de las cuales se dan a conocer los eventos y aspectos relacionados con la seguridad de la información y sus riesgos. El modelo descrito en la tabla es referencial, para permitir que la entidad pueda comunicar situaciones excepcionales o de urgencia manifiesta por los medios que resulten apropiados a la situación que se presenta.

TIPO DE COMUNICACIÓN	DIRIGIDA A	CUANDO COMUNICAR	RESPONSABLE DE LA COMUNICACIÓN
Campañas de divulgación y concientización	Todo el personal	Conforme al plan de seguridad de cada vigencia.	Responsable de seguridad de la información o el recurso profesional de apoyo.
Mensajes de prevención y alerta por el descubrimiento o detección de amenazas y riesgos.	Administradores de plataformas o servicios potencialmente expuestos o que puedan ser objeto de la amenaza.	Una vez validada la información y confirmada su veracidad	
Reporte de incidentes	Autoridad competente y grupos de interés en Seguridad.	Una vez que el incidente ha sido presentado y analizado por el CIGD	

Tabla # 8. Comunicaciones del SGSI.

10. OPERACIÓN.

Este capítulo describe algunas de las actividades que permiten el cumplimiento de los controles del Anexo A de la norma NTC-ISO-IEC 27001:2013, otras actividades se detallan en documentos diseñados para abordar temas específicos.

10. 1. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN.

10. 1. 1. Contacto con Autoridades y Grupos de Interés

El objetivo de esta actividad es mantener identificados y actualizados los canales de comunicación con autoridades y grupos de interés que pueden representar un apoyo importante ante casos de incidentes, obtener información sobre vulnerabilidades, compartir experiencias o recibir apoyo cuando esto sea requerido.

Esta actividad permite el cumplimiento de dos controles, identificados como A.6.1.3 y A.6.1.4 del Anexo A de la ISO 27001:2013 y se detalla en el Anexo 2 de este documento.

10. 1. 2. Lineamientos y Consideraciones para Trabajo Remoto. (A.6.2.2)

Los lineamientos aplicables por la entidad para el trabajo remoto son las siguientes:

- Los colaboradores que realicen funciones bajo esta modalidad serán autorizados por el superior inmediato o las autoridades cuando aplique.
- Al colaborador que se encuentra bajo esta modalidad también le aplican las políticas, normas, controles y condiciones que rigen a los colaboradores de la modalidad presencial.
- El colaborador que se encuentre bajo esta modalidad facilitará, en el momento que sea requerido y apropiado, el acceso a los recursos suministrados por la entidad para fines de mantenimiento, reemplazo, actualización o auditoría.
- Las herramientas suministradas por la entidad solo deben ser usadas por el colaborador, quien al finalizar esta modalidad deberá restituirlos en buen estado, salvo el deterioro causado por el uso normal y cotidiano de los elementos. Cuando los equipos a devolver no se encuentren en buen estado, el colaborador debe informar a la entidad con anticipación mediante mail a su superior inmediato o supervisor, informando el estado y las condiciones de funcionalidad en las que se encuentra el equipo.
- Los mecanismos y técnicas de seguridad mínimos que aplican al trabajo remoto se relacionan a continuación, los cuales pueden ser

mejorados o fortalecidos, conforme a los riesgos de las actividades a realizar, caso en el cual éstos, deben serán avalados por el responsable de seguridad de la información o quien haga sus veces:

o Autenticación por medio de usuario y contraseña.

o Generación y entrega segura de contraseña.

o Uso de técnicas de encapsulamiento y protocolo de ciframiento para la conexión usuario-INM, por ejemplo, mediante VPN. (Red Privada Virtual).

o Si las herramientas para teletrabajo han sido dispuestas por el INM, éstas deben disponer y/o tener habilitadas mecanismos de prevención como antivirus y firewall, así como herramientas para diagnóstico y soporte remoto.

o Registros de auditoría de la actividad del usuario.

o La entidad se reserva el derecho de realizar visitas de inspección o auditoría al sitio y lugar donde se ubican sus recursos, aplicando el mismo procedimiento y técnicas de auditoría que se aplican a instalaciones y procesos cuando éstas se realizan en las dependencias del INM.

o Los privilegios de acceso a los recursos (aplicaciones y servicios) son restringidos, conforme a los roles y funciones del personal que hace uso de esta modalidad de trabajo.

o El personal de la mesa de servicios es el único autorizado al uso de herramientas de control remoto para funciones exclusivamente de soporte, como excepción, cuando un tercero requiere tener control remoto de la infraestructura del INM, esto deberá estar autorizado vía mail por el responsable de seguridad de la información.

10. 2. GESTIÓN DE ACTIVOS.

10.2.1 Responsabilidad por los Activos

La entidad aplica el procedimiento de Gestión de Activos de Información (E-05-P-04) por medio del cual se aplican los controles establecidos en el objetivo de control (A.8) de la NTC-ISO-IEC 27001:2013, los registros que se generan por este procedimiento se consignan en el formato E-05-F-005 del SIG.

10.2.2. Disposición de Medios (A.8.3.2)

Cuando sea requerido por la entidad eliminar o dar de baja medios magnéticos que contengan información catalogada como: pública clasificada, pública reservada o de uso interno (acorde a la clasificación establecida en el procedimiento de Gestión de Activos de Información), el GSIR procederá a destinar una partida presupuestal que permita la contratación de esta actividad con un tercero que ofrezca este tipo de servicio bajo protocolos y procedimientos certificados o conformes con los estándares de seguridad vigentes. A continuación, se describen las técnicas aplicables para la fecha de elaboración de este documento, las cuales pueden ser complementadas o sustituidas por otras que sean desarrolladas posteriormente

MÉTODO	TIPO DE MEDIO AL QUE APLICA Y EJEMPLOS	OBSERVACIONES
Desmagnetización (exposición de los medios a un potente campo magnético)	Medios magnéticos (discos duros, cintas magnéticas)	• Válido sólo para medios magnéticos. • El procedimiento inhabilita el medio, al cual se le debe dar una eliminación posterior. • Elimina de una manera segura la información
Sobre escritura (escritura de un patrón de datos sobre toda la superficie de almacenamiento)	Medios magnéticos y electrónicos (USB, discos duros SSD).	• No es aplicable a medios que no sean regrabables. • Implica tener acceso al medio tecnológico que permita sobreescribir. • Después del procedimiento el medio es reutilizable.
Destrucción física	Aplica a cualquier medio y es el adecuado para medios ópticos como CD y DVD.	Inhabilita el medio y se dificulta el reciclaje de materiales

Tabla # 9. Disposición Segura de Medios

10. 3. SEGURIDAD FÍSICA Y DEL ENTORNO

Esta sección describe las actividades relacionadas con la prevención de riesgo de daño, acceso no autorizado o uso indebido de instalaciones y

equipos de procesamiento de datos.

10.3.1 Disposición o reutilización segura de equipos.

Para la reutilización de computadores propios o devolución de equipos en arrendamiento, se aplicarán las actividades descritas en la siguiente tabla, cuando el equipo contenga información catalogada como pública reservada o pública clasificada, conforme al procedimiento de Gestión de Activos de Información. (no aplica cuando contenga información catalogada como pública).

Destino del equipo	Actividad a realizar	
	Si tienen software licenciado o desarrollado por el INM	Si contiene información reservada o clasificada
Reutilización en el INM	No aplica	Borrado mediante software libre que realice como mínimo 3 pasadas.
Enajenación de bienes a título gratuito entre entidades estatales o transferencia del derecho de dominio o devolución de equipos en arriendo	Des-instalación de licencias de software	

Tabla # 10. Disposición o Reutilización de Equipos

En el caso de equipos que vayan a ser destinados a chatarrización o reciclaje de materiales, los medios de almacenamiento con que cuentan estos equipos deben ser sometidos a lo descrito en el ítem 10.2.2 de este documento.

10. 4. SEGURIDAD DE LAS OPERACIONES

En esta sección se establecen las actividades y controles tendientes a asegurar una adecuada gestión de la plataforma tecnológica.

10. 4. 1. Gestión de Cambios

Los cambios que se realizan en las instalaciones de TI, infraestructura de TI, así como en el ciclo de vida del software, sea que estos se lleven a cabo por personal interno o proveedores se gestionan por medio del procedimiento Gestión del Cambio (E-02-P-08).

Lo anterior permite cumplir con los controles: Gestión de Cambios, Procedimiento de Control de Cambios en Sistemas y Gestión de Cambios en los Servicios de los Proveedores (identificados como A.12.1.2, A.14.2.2 y A.15.2.2 respectivamente, del Anexo A de la NTC-ISO-IEC 27001:2013).

10. 5. SEGURIDAD EN REDES DE COMUNICACIÓN.

Esta sección establece las políticas o actividades relacionadas con la mitigación de riesgos por el flujo de información a través de canales y servicios tanto internos como externos:

10. 5. 1. Seguridad de Servicios de Red. (A.13.1.2)

La entidad dispone de herramienta y mecanismos para proteger su información y servicios, las cuales son administradas por personal del INM y se genera informe estadístico acorde a las necesidades de seguimiento y control de los dispositivos de seguridad perimetral mediante la plataforma Analyzer, la cual permite tener un consolidado de la actividad de las herramientas de seguridad perimetral (Firewall, Anti DDoS y WAF o las que a futuro las sustituyan o complementen). El objetivo de estos reportes es conocer el desempeño, niveles y volumen de tráfico bajo condiciones normales, que sirvan de referencia ante situaciones anómalas.

10. 5. 2. Transferencia de Información con Terceros.

Cuando la entidad requiera enviar a un tercero, información de la cual es responsable el INM, esta transferencia se realizará siguiendo los estándares de interoperabilidad definidos por MinTIC y bajo acuerdos o cláusulas de responsabilidad claramente establecidas. Así mismo serán aplicados protocolos para asegurar la confidencialidad (ej. encripción), cuando se trate de información catalogada como pública reservada o

pública clasificada.

10. 6. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS.

10. 6. 1. Restricciones en los cambios a los paquetes de software.

Los paquetes de software adquiridos a terceros no deben ser sometidos a cambios de programación o cambios en el código fuente. El mantenimiento a este tipo de programas se realizará priorizando esta labor por parte del proveedor. En casos excepcionales antes de proceder se requerirá análisis y control riguroso, considerando el impacto e implicaciones a futuro.

10. 6. 2. Pruebas de Seguridad de Sistemas.

Esta actividad tiene por objetivo evaluar la efectividad de los controles de seguridad de la información en sistemas de información desarrollados o adquiridos y su realización permite el cumplimiento del control que hace parte del dominio de adquisición, desarrollo y mantenimiento de sistemas (identificado como A.14.2.8 de la ISO 27001:2013), por lo anterior es importante que éstas pruebas se realicen durante el desarrollo o preparación y antes de la puesta en producción de un nuevo sistema de información o la mejora a uno existente, como lo refiere el control citado.

Las actividades relacionadas con las pruebas de seguridad pueden ser consultadas en el Documento: Metodología Ciclo de Vida del Software.

10. 6. 3. Pruebas de Aceptación de Sistemas.

Previo a la puesta en producción de software desarrollado o adquirido por la entidad se llevarán a cabo pruebas sobre la funcionalidad y parametrización de las aplicaciones, las cuales serán: planeadas, ejecutadas y documentadas, tal como lo establece la metodología que regula el ciclo de vida del software adoptada por el GSIR e incorporada al SIG.

11. DOCUMENTOS RELACIONADOS

- Procedimiento Gestión Activos de Información - E-05-P-004
- Atención de requerimientos de mantenimiento de software - E-05-P-001
- Back Ups y restauración de información en equipos de cómputo y servidores - E-05-P-002
- Código de Integridad del Servicio Público en el INM (Resolución 161 de 2020).
- Procedimiento Control de Cambios. -E-02-P-008.
- Gestión de Incidentes y Requerimientos de Servicios de TI. E-05-P-003
- Gestión de servicios de correo electrónico - E-05-I-002
- Instructivo de Copias de Respaldo y Restauración en Servidores - E-05-I-006
- Configuración de recursos compartidos - E-05-I-010

12. REFERENCIAS BIBLIOGRÁFICAS.

- Manual de Gobierno Digital V.7 - MinTIC.
- Modelo de Seguridad y Privacidad de la Información V.3.0.2 - MinTIC
- Elaboración de la Política General de Seguridad y Privacidad de la Información (Guía No. 2) - MinTIC
- Controles de Seguridad y Privacidad de la Información (Guía Nro. 8) - MinTIC
- Guía de Mejora Continua (Guía Nro. 17) - MinTIC
- Norma Técnica NTC-ISO-IEC 27001:2013
- Guía Técnica GTC-ISO-IEC 27002:2015

13. ANEXOS

Anexo 1 Declaración de Aplicabilidad de Controles – Detallada Conforme al Anexo A de la NTC-ISO-IEC 27001:2013

Anexo 2 Contacto con Autoridades y Grupos de Interés

CONTROL DE CAMBIOS

FECHA	DESCRIPCIÓN DEL CAMBIO	VERSIÓN
21/Dic/2020	Versión inicial. Inclusión dentro del SIG del INM	1
21/Dic/2020	Se incorporan: El requisito de comunicaciones del SGSI, identificado como 7.4 en la ISO 27001 en la sección 9.2. Se incorporan los siguientes controles: políticas de dispositivos móviles, teletrabajo, disposición de medios de soporte, disposición segura y reutilización de equipos, políticas de transferencia de información. Acciones de mejora derivadas de auditorías. Ajustes aclaraciones y precisiones de redacción. Se incluyen los siguientes temas: pruebas de funcionalidad a sistemas de información y declaración de aplicabilidad detallada como anexo.	2

ELABORÓ	REVISÓ	APROBÓ
Nombre: Edgar Franco Ruiz **Cargo:** Contratista Grupo Sistemas de Información y Redes **Fecha:** 12/Nov/2020	**Nombre:** Omar Enrique Mejia Vargas **Cargo:** Ninguno **Fecha:** 10/Dic/2020	**Nombre:** Comité Institucional de Gestión y Desempeño **Cargo:** Ninguno **Fecha:** 21/Dic/2020

"Si imprime o descarga este documento se considera una copia no controlada"