POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

CODIGO MNL-D04.0000-001

VERSION 01

INSTITUTO NACIONAL DE SALUD

INSTITUTO NACIONAL DE SALUD

Febrero de 2024

TABLA DE CONTENIDO

1. INTRODUCCION

El Instituto Nacional de Salud – (en adelante INS) mediante la Resolución 186 de 27 de 2019: "*Por la cual se adopta la política de seguridad de la información en el INS y se dictan otras disposiciones.*", formaliza su compromiso con la preservación del activo institucional más importante, es decir la Información, por tal motivo y para asegurar que se implementen de manera más eficiente los controles que garanticen la preservación de la información se crea éste documento el cual hace parte fundamental del Sistema de Gestión de Seguridad de la Información del INS y desarrolla las políticas establecidas en la Resolución ***mencionada, la cual fue modificada mediante Resolución 0309 de Abril de 2022.***

Para el INS la descripción de las políticas y las normas de seguridad de la información, se constituyen como parte fundamental del sistema de gestión de seguridad de la información el cual se integrará con el Sistema de Gestión del INS y se convierten en la base para la implantación de los controles, procedimientos y estándares definidos. Para la elaboración de este, se toman como base las leyes y demás regulaciones aplicables, la norma ISO 27001:2013 y las recomendaciones del estándar ISO 27002:2013.

El presente manual de Políticas de Seguridad de la Información establece las normas fundamentales que deben regir y los controles básicos a ser establecidos por el INS, para garantizar la seguridad de la información y el adecuado uso de los recursos informáticos suministrados por el INS y administrados por la Oficina de Tecnologías de la Información y Comunicaciones.

2. OBJETIVO

El INS, establece sus objetivos del Sistema de Gestión de Seguridad de la Información, realizando una alineación con la Planeación Estratégica de la entidad apoyando el cumplimiento de los objetivos estratégicos, y de esta manera expresar la intención articuladamente con el desempeño del resultado, ***de acuerdo a lo definido en la Resolución 0309 de Abril de 2022[1], así:***

a) Proteger, preservar y administrar los activos de información, las bases de datos personales y las tecnologías utilizadas para su procesamiento, frente a amenazas internas o externas, con el fin de asegurar la confidencialidad, la integridad y la disponibilidad de manera coordinada con las partes involucradas y previniendo ciber amenazas que potencialmente afectarán los activos de información del Instituto Nacional de Salud en cualquiera de sus estados.

b) Aplicar un proceso de gestión de riesgos de seguridad y privacidad de la información y bases de datos personales, mediante la ejecución de medidas apropiadas con el fin de identificar, analizar, evaluar, tratar y mitigar los riesgos y así reducir el impacto potencial a niveles aceptables sobre los riesgos asociados con la pérdida de confidencialidad, de integridad, y de disponibilidad.

---

[1] Resolución 0309 de 2022; Artículo Quinto "Objetivos de Seguridad y Privacidad de la Información: págs. 3 y 4; https://www.ins.gov.co/Normatividad/Resoluciones/Res.%200309%20de%202022.pdf

c) ***Implementar, operar y revisar periódicamente los controles establecidos en la declaración de aplicabilidad, para la prevención y mitigación de los riesgos de seguridad y privacidad de la información y la seguridad digital.***

d) ***Disponer de medidas para atender oportunamente eventos de seguridad y privacidad de la información y seguridad digital con el fin de disminuir los impactos negativos ocasionados por los incidentes de seguridad y privacidad de la información que se puedan llegar a presentar en la Entidad.***

e) ***Reducir la probabilidad de violación de la privacidad de los datos personales de la entidad.***

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

g) ***Fortalecer la cultura de seguridad y privacidad de la información en la entidad, a través de la gestión del conocimiento, las campañas de sensibilización, transferencias de conocimiento, capacitaciones y las necesarias definidas en el plan de comunicación de seguridad y privacidad de la información.***

h) ***Actualizarse en las distintas modalidades de ciberataques que potencialmente pudieran representar una amenaza para los activos de información del Instituto Nacional de Salud.***

3. ALCANCE

El sistema de seguridad y privacidad de la información, protección de datos personales y seguridad digital, abarca los activos de información, las Bases de Datos personales y los contenedores de información, gestionados en el desarrollo de las funciones, de todos los procesos definidos en el Instituto Nacional de Salud (INS), así como todo el personal, es decir: funcionarios, contratistas, proveedores, colaboradores, profesionales en entrenamiento o partes interesadas que generen, accedan o utilicen información de la entidad, con el fin de garantizar su confidencialidad integridad y disponibilidad en él INS[2]**.**

4. RESPONSABILIDAD

Las políticas contenidas en este documento aplican para la Alta Dirección, Directores, asesores de oficinas, jefes de oficina, Subdirectores, Coordinadores, Secretaria General y Oficinas Asesoras , funcionarios, contratistas, ***proveedores, colaboradores, profesionales en entrenamiento o partes interesadas y*** a todos los usuarios de la información que cumplan con los *propósitos* generales del INS; ***quienes son responsables de dar cumplimiento a la presente política; hoy el incumplimiento traerá consigo, las consecuencias administrativas y legales que apliquen a la normatividad vigente del INS, incluyendo lo establecido en las que competen al gobierno nacional en cuanto a la seguridad y privacidad de la información*****.**

La alta dirección del INS es la responsable de garantizar que la seguridad y privacidad de la información sean parte de la cultura organizacional.

---

[2] ***Resolución 0309 de 2022; Articulo Segundo "Alcance de la Política de Seguridad y Privacidad de la Información: pág 2; https://www.ins.gov.co/Normatividad/Resoluciones/Res.%200309%20de%202022.pdf***

5. DEFINICIONES Y ABREVIATURAS

Acceso a la Información Pública: Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceso a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4).

Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de ésta (sistemas, soportes, edificios, personas, etc.) que tenga valor para la organización. (ISO/IEC 27000).
Activo de Información y recursos: se refiere a elementos de hardware y de software de procesamiento, almacenamiento y comunicaciones, bases de datos y procesos, procedimientos y recursos humanos asociados con el manejo de los datos y la información misional, operativa y administrativa de cada entidad, órgano u organismo. (CONPES 3854 de 2016).

Amenazas: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).

Análisis de Riesgo: Proceso para comprender la naturaleza del riesgo y determinar el nivel de dicho riesgo. (ISO/IEC 27000).

Archivo: Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura. (Ley 594 de 2000, art 3)

Apetito de riesgo: Cantidad y tipo de riesgo que una organización está preparada para buscar o retener. (ISO/IEC 22300).

Auditoría: Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y obviamente para determinar el grado en el que se cumplen los criterios de auditoría. (ISO/IEC 27000).

Autorización: Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3)

Aviso de privacidad: Comunicación verbal o escrita generada por el responsable, dirigida al Titular para el Tratamiento de sus datos personales, mediante la cual se le informa acerca de la existencia de las políticas de Tratamiento de información que le serán aplicables, la forma de acceder a las mismas y las finalidades del Tratamiento que se pretende dar a los datos personales. (Decreto 1377, art 3).

Bases de Datos Personales: Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3)

Ciberseguridad: Protección de activos de información, mediante el tratamiento de las amenazas que ponen en riesgo la información que se procesa, almacena y transporta mediante los sistemas de información que se encuentran interconectados.

Ciberespacio: Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).

Ciclo PHVA (Planificar-Hacer- Verificar-Actuar): Este ciclo permite a una organización asegurarse de que sus procesos cuenten con recursos y se gestionen adecuadamente, y que las oportunidades de mejora se determinen y se actúe en consecuencia. (ISO/IEC 9001).

Confidencialidad: Propiedad por la que la información no se pone a disposición o se divulga a personas, entidades o procesos no autorizados. (ISO/IEC 27000).

Control: Medida por la que se modifica el riesgo. Los controles incluyen procesos, políticas, dispositivos, prácticas, entre otras acciones que modifican el riesgo. Es posible que los controles no siempre ejerzan el efecto de modificación previsto o supuesto. (ISO Guide 73:2009)

Control de acceso: Significa garantizar que el acceso a los activos esté autorizado y restringido según los requisitos comerciales y de seguridad. (ISO/IEC 27000).

Control correctivo: Control que corrige un riesgo, error, omisión o acto deliberado antes de que produzca pérdidas relevantes. Supone que la amenaza ya se ha materializado pero que se corrige. (ISO/IEC 27000).

Control detectivo: Control que detecta la aparición de un riesgo, error, omisión o acto deliberado. Supone que la amenaza ya se ha materializado, pero por sí mismo no la corrige. (ISO/IEC 27000).

Control disuasorio: Control que reduce la posibilidad de materialización de una amenaza, p.ej., por medio de avisos o de medidas que llevan al atacante a desistir de su intención. (ISO/IEC 27000).

Control preventivo: Control que evita que se produzca un riesgo, error, omisión o acto deliberado. Impide que una amenaza llegue siquiera a materializarse. (ISO/IEC 27000).

Custodio: Es una parte designada de la entidad, un cargo, proceso, o grupo de trabajo encargado de administrar y hacer efectivos los controles de seguridad que el propietario de la información haya definido, tales como copias de seguridad, asignación privilegios de acceso, modificación y borrado. (Guía # 5 para la Gestión y Clasificación de Activos de Información, MINTIC)

Datos Personales: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).

Datos Personales Privados: Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3 literal h)

Datos Personales Públicos: Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, art 3)

Datos Personales Sensibles: Para los propósitos de la presente ley, se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos. (Ley 1581 de 2012, art 5)

Declaración de aplicabilidad: Documento que enumera los controles aplicados por el SGSI de la organización -tras el resultado de los procesos de evaluación y tratamiento de riesgos- y su justificación, así como la justificación de las exclusiones de controles del anexo A de la norma ISO 27001.

Disponibilidad: Propiedad de la información de ser accesible y utilizable a solicitud de una entidad autorizada. (ISO/IEC 27000).

Encargado del Tratamiento de Datos: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del responsable del Tratamiento. (Ley 1581 de 2012, art 3)

Gestión de incidentes de seguridad de la información: Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).

Información Pública Clasificada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)

Información Pública Reservada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)

INS: Instituto Nacional de Salud

Integridad: Propiedad de la información relativa a su exactitud y completitud. (ISO/IEC 27000).

Ley de Habeas Data: Se refiere a la Ley Estatutaria 1581 de 20212. La presente ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma.

Ley de Transparencia y Acceso a la Información Pública: Se refiere a la Ley Estatutaria 1712 de 2014. El objeto de la presente ley es regular el derecho de acceso a la información pública, los procedimientos para el ejercicio y garantía del derecho y las excepciones a la publicidad de información.

MSPI (Instructivo para el Diligenciamiento de la Herramienta de Diagnostico de Seguridad y Privacidad de la Información de MinTIC): El Modelo de Seguridad y Privacidad de la Información - MSPI, conceptualizado y presentado por MINTIC imparte lineamientos a las entidades públicas en materia de implementación y adopción de buenas prácticas, tomando como referencia estándares internacionales, con el objetivo de orientar la gestión e implementación adecuada del ciclo de vida de la seguridad de la información (Planeación, Implementación, Evaluación, Mejora Continua), permitiendo habilitar la implementación de la Política de Gobierno Digital.

No repudio: Capacidad de probar la ocurrencia de un evento o acción reclamada y sus entidades de origen. (ISO/IEC 27000).

Partes interesadas: Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad. (ISO/IEC 27000).

Propietario de la Información: Es una parte designada de la entidad, un cargo, proceso, o grupo de trabajo que tiene la responsabilidad de garantizar que la información y los activos asociados con los servicios de procesamiento de información se clasifican adecuadamente, y de definir y revisar periódicamente las restricciones y clasificaciones del acceso, teniendo en cuenta las políticas aplicables sobre el control del acceso. (Guía # 5 para la Gestión y Clasificación de Activos de Información, MINTIC).

Plan de continuidad del negocio: Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000).

Plan de tratamiento de riesgos: Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).

Propiedad intelectual: Se refiere a la protección del producto del intelecto humano, sea en los campos científicos, literarios, artísticos o industriales. Esa protección concede a los creadores, autores e inventores un derecho temporal para excluir a los terceros de la apropiación de conocimiento por ellos generados.

Teletrabajo (teletrabajo.gov.co): De acuerdo con la Ley 1221 de 2008 es "una forma de organización laboral, que consiste en el desempeño de actividades remuneradas o prestación de servicios a terceros utilizando como soporte las tecnologías de la información y comunicación - TIC - para el contacto entre el trabajador y la empresa, sin requerirse la presencia física del trabajador en un sitio específico de trabajo".(Dirección Nacional de Derechos de Autor, Unidad Administrativa Especial Ministerio del Interior.

Responsable del Tratamiento de Datos: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos. (Ley 1581 de 2012, art. 3).

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

Seguridad de la información: Preservación de la confidencialidad, integridad y disponibilidad de la información en cualquier medio: impreso o digital. (ISO/IEC 27000).

Sistema de Gestión de Seguridad de la Información (en adelante SGSI): Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión del riesgo y de mejora continua.

Tolerancia al riesgo: Disponibilidad de una organización o de las partes interesadas para soportar el riesgo después del tratamiento del riesgo con objeto de conseguir sus objetivos. (ISO/IEC 22300).

Titulares de la información: Personas naturales cuyos datos personales sean objeto de Tratamiento. (Ley 1581 de 2012, art 3)

Tratamiento de Datos Personales: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. (Ley 1581 de 2012, art 3).

Tratamiento de riesgos: Proceso para modificar el riesgo. El tratamiento del riesgo puede involucrar lo siguiente; evitar el riesgo al decidir no comenzar o continuar con la actividad, tomar o aumentar el riesgo buscando una oportunidad, eliminar el riesgo, cambiar la probabilidad, cambiar las consecuencias, compartir el riesgo o retener el riesgo. (ISO/IEC 27000).

Trazabilidad: Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad. (ISO/IEC 27000).

Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).

6. CONDICIONES GENERALES

N/A

7. CONTENIDO

7.1 POLITICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

La Alta Dirección del INS, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un sistema de gestión de seguridad de la información buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la entidad.

Para el INS, la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad ***de esta***, acorde con las necesidades de los diferentes grupos de interés identificados.
De acuerdo con lo anterior, esta política se aplica en el INS según como se defina en el alcance, sus funcionarios, terceros, aprendices, practicantes, proveedores y la ciudadanía en general, teniendo en

cuenta que los principios sobre los que se basa el desarrollo de las acciones o toma de decisiones alrededor del SGSI estarán determinadas por las siguientes premisas:

a) Gestionar el riesgo de los procesos estratégicos, misionales, de apoyo y de evaluación de la entidad.
b) Cumplir con los principios de seguridad de la información: Confidencialidad, Integridad y Disponibilidad.

- CONFIDENCIALIDAD: la información debe ser accesible sólo a aquellas personas autorizadas.
- INTEGRIDAD: la información y sus métodos de procesamiento deben ser completos y exactos.
- DISPONIBILIDAD: la información y los servicios deben estar disponibles cuando se le requiera.

c) Mantener la confianza de los funcionarios, contratistas y terceros.

d) Mantener y Mejorar el sistema de gestión de seguridad de la información, cumpliendo con el ciclo PHVA.

e) Proteger los activos de información.

f) Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.

g) Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes del INS.

h) Garantizar la continuidad del negocio frente a incidentes.

Nivel de cumplimiento. Todas las personas cubiertas por el alcance y aplicabilidad deberán cumplir de manera obligatoria, en su totalidad, sin perjuicio de las sanciones a que haya lugar.

7.2 COMPROMISO DE LA ALTA DIRECCIÓN

La alta Dirección del INS aprueba esta Política de Seguridad de la Información mediante la Resolución 186 de 27 de febrero de 2019: "*Por la cual se adopta la política de seguridad de la información en el INS y se dictan otras disposiciones.*", y así formaliza su compromiso y apoyo en el diseño e implementación de políticas eficientes que garanticen la seguridad de la información de la entidad, a través de:

- La revisión y aprobación de las políticas de Seguridad de la Información contenidas en este documento.
- Facilitar la divulgación de este manual a todos los funcionarios del INS.
- El aseguramiento de los recursos adecuados para implementar y mantener las políticas de seguridad de la Información
- La verificación del cumplimiento de las políticas aquí mencionadas
- Compromiso permanente de una cultura de seguridad.

La resolución 186 de febrero de 2019 fue modificada y adiciona por medio de la Resolución 0309 de 2022[3] que el Instituto Nacional de Salud, mediante la Política de Seguridad y Privacidad de la Información da cumplimiento a los lineamientos de la Planeación estratégica de la entidad, en concordancia con su misión, visión, objetivos estratégicos, que establecen la función de seguridad y privacidad de la información de la Entidad.

7.2.1 PLANIFICACIÓN

La Oficina de Tecnologías de la Información y las Comunicaciones deberá formular el plan de tratamiento de riesgos de seguridad de la información y registrarlos en el formato FOR -D04.000-011.

7.2.2 SOPORTE

La Oficina de Tecnologías de la Información y las Comunicaciones gestionará el apoyo de los recursos necesarios para la implementación de los controles y el plan de tratamiento requerido para la operación de Seguridad de la Información.

7.2.3 OPERACIÓN

La Oficina de Tecnologías de la Información y las comunicaciones deberá formular anualmente el Plan de Seguridad y Privacidad de la Información del INS y publicarlo en el portal web institucional, de acuerdo con los lineamientos de la normatividad vigente.

7.2.4 EVALUACIÓN DEL DESEMPEÑO

Se debe evaluar el desempeño y la eficacia del SGSI, a través de instrumentos que permitan determinar el avance del ciclo de operación PHVA, la efectividad de la implementación de controles, por lo que en el INS se adoptan los indicados por la normatividad vigente y el Modelo de seguridad de privacidad de la información, como apoyo en el seguimiento y medición se deben tener en cuenta los resultados de las auditorías internas e indicadores del SGSI.

7.2.5 MEJORA

El SGSI adopta el modelo PHVA (Planear, Hacer, Verificar, Actuar) de mejora continua, el cual se aplica para estructurar los procesos del sistema como parte del ciclo de mejora continua, en una secuencia lógica de cuatro pasos, los cuales son repetidos y ejecutados sucesivamente.

Como resultado de las revisiones efectuadas, se establecen las decisiones relacionadas con las oportunidades de mejora continua y cualquier necesidad del cambio del SGSI.

7.2.6 APROBACIÓN Y REVISIONES DE LA POLITICA

Las políticas de Seguridad de la información se deben revisar anualmente o si ocurre cambios significativos, para asegurar su conveniencia, adecuación y eficacia continuas. Teniendo en cuenta las siguientes variables:

---

[3] ***Resolución 0309 de 2022; Artículo Quinto "Fines de la política; pág. 4; https://www.ins.gov.co/Normatividad/Resoluciones/Res.%200309%20de%202022.pdf***

a) Se debe verificar que se definan, implementen, revisen y actualicen las políticas de seguridad de la información como efectos de mejora continua.

b) Todos los usuarios de los sistemas de información y telecomunicaciones del INS tienen la responsabilidad y obligación de cumplir con las políticas, normas, procedimientos y buenas prácticas de seguridad de la información establecidas en el presente documento de la política de seguridad de la información.

c) El INS cuenta con seguridad perimetral y demás herramientas que protejan todas las transacciones que se realicen en el INS.

d) La conexión remota a la red de área local del INS debe realizarse conforme a la justificación del usuario y se realizara a través de una conexión VPN segura suministrada por la entidad, la cual debe ser aprobada, registrada y auditada, por la Oficina Tecnología Información y Comunicaciones.

e) Los directores, asesores de oficinas, jefes de oficina, Subdirectores, Coordinadores, Secretaria General y Oficinas Asesoras, funcionarios, contratistas del INS, deben asegurarse ***que*** todos los procedimientos de seguridad de la información se cumplan.

7.3 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (ROLES Y RESPONSABILIDADES)

El INS, define los roles y responsabilidades para la implementación del MSPI y el cumplimiento de los lineamientos de seguridad descritos en esta política y los demás documentos derivados (Manuales, Procedimientos, Formatos etc.…), siendo formalizada en ***Resolución 0186 de 2019[4], así***:

ROL / INSTANCIA / DEPENDENCIA	*RESPONSABILIDADES*
Jefe de la Oficina de Tecnologías de Información y Comunicaciones, o quien haga sus veces.	*Responsable de Seguridad de la Información, encargado de establecer, implementar, mantener y mejorar continuamente el Sistema de Gestión de Seguridad de la Información y demás actividades derivadas para la estandarización de la presente Política.*
Jefe de la Oficina Asesora Jurídica	*Responsable de Protección de Datos Personales, encargado de implementar, mantener y mejorar continuamente, así como apoyar y coordinar con las demás áreas del Instituto Nacional de Salud (INS) el tratamiento de los datos personales, para asegurar una implementación transversal del cumplimiento de la Ley 1581 de 2012.*
	• *Planear, participar y realizar actividades de Seguridad de la información que involucren a todo el personal.* • *Ejercer seguimiento y control del SGSI, aplicando los correctivos y ajustes necesarios para el logro de los objetivos, informando a la alta dirección sobre el desempeño del sistema.* • *Emplear la información, los procedimientos, el talento humano y*

[4] *Resolución 0186 de 2019; Articulo Septimo "Responsables del Sistema de Seguridad de la Informacion y Proteccion de Datos personales; pág 2; https://www.ins.gov.co/Normatividad/Resoluciones/RESOLUCION%200186%20DE%202019.pdf*

ROL / INSTANCIA / DEPENDENCIA	RESPONSABILIDADES
Oficial de Seguridad de la Información - Jefe de la Oficina de Tecnologías de la Información y las comunicaciones.	los recursos materiales y financieros para el desarrollo de las actividades del SGSI adecuadamente. • Establecer y realizar la revisión y actualización de las políticas y los objetivos de Seguridad de la información de la organización. • Analizar los datos arrojados por el SGSI y tomar las decisiones necesarias para garantizar el mantenimiento y mejoramiento del sistema. • Coordinar el levantamiento de activos de información de la entidad para su clasificación de acuerdo con la metodología establecida. • Coordinar la realización de un análisis de riesgos de seguridad de la información en cada uno de los Procesos del Instituto Nacional de Salud (INS), y para cada una de las actividades subcontratadas, el cual debe llevarse a cabo como mínimo una vez al año, para determinar el grado de exposición a las amenazas relacionadas con los activos de información. • Definir y ejecutar los planes de entrenamiento y sensibilización y capacitación para los funcionarios y partes interesadas del Instituto Nacional de Salud (INS) en lo referente a seguridad de la información. • Respetar y cumplir los principios básicos de seguridad de la información (Confidencialidad, Integridad y Disponibilidad). • Identificar todos los cambios significativos de amenazas y exposición de la información. • Evaluar la adecuación e implantación de los controles de Seguridad de la información. • Realizar el escaneo de vulnerabilidades a fin de identificar huecos de seguridad en los activos de información. • Evaluar la información de seguridad recibida a la hora de monitorear y revisar los incidentes de Seguridad de la información, además de recomendar todas las acciones apropiadas en respuesta para identificar incidentes de Seguridad de la información. • Definir las metodologías y los procesos para seguridad de la información.
Oficial de Protección de Datos Personales - Jefe de la Oficina Asesora Jurídica	• Asesorar y constatar que los responsables de la protección de los datos personales realicen el trámite a las solicitudes de los Titulares de los datos personales para el ejercicio de los derechos que se consagran en la Ley 1581 de 2012. • Realizar la revisión y actualización anual en conjunto con el Oficial de Seguridad de la información, respecto de los riesgos jurídicos que se identifiquen frente a la protección de datos personales del INS. • Mantener un inventario de las bases de datos personales en poder del INS y clasificarlas según su contenido. • Coordinar con la Oficina de Tecnología de información y comunicación la actualización anual de las Bases de Datos en la plataforma de la Superintendencia de Industria y Comercio (SIC). • Realizar un Plan de Sensibilización anual, en conjunto con el

ROL / INSTANCIA / DEPENDENCIA	RESPONSABILIDADES
	área de Comunicaciones en materia de protección de Datos Personales para el INS. • Servir de coordinador con las demás áreas de la organización para asegurar una implementación transversal del cumplimiento de la Ley 1581 de 2012.
Oficina de tecnologías de la información y las comunicaciones	• Implantar, mantener y divulgar las políticas y procedimientos de tecnología, incluida esta política de seguridad de información, el uso de los servicios tecnológicos en toda la institución de acuerdo a las mejores prácticas y lineamientos de la Dirección General del Instituto y directrices del Gobierno. • Salvaguardar la información que reposa en los diferentes sistemas de información, bases de datos y aplicativos de la institución. • Informar de los eventos que estén en contra de la seguridad de la información y de la infraestructura tecnológica de la Institución a la Dirección General, las diferentes Direcciones e Informar de los eventos que estén en contra de la seguridad de la información y de la infraestructura tecnológica de la Institución a la Dirección General, las diferentes Direcciones y Jefaturas del Instituto Nacional de Salud, así como a los entes de control e investigación que tienen injerencia sobre la institución. • Informar a la alta dirección, al Centro Cibernético Policial (CCP), COLSERT – Grupo de Respuesta a Emergencias Cibernéticas en Colombia, CSIRT-CCIT – Centro de Coordinación Seguridad Informática Colombia, y demás relacionados en el numeral A.6.1.3 Contacto con las autoridades. • Proporcionar medidas de seguridad físicas, lógicas y procedimentales para la protección de la información digital del Instituto. • Aplicar y hacer cumplir la Política de Seguridad de la Información y sus componentes. • Administrar las reglas y atributos de acceso a los equipos de compute, sistemas de información, aplicativos y demás fuentes de información al servicio del Instituto Nacional de Salud. • Implementar los mecanismo de controles necesarios y pertinentes para verificar el cumplimiento de la presente política.
Oficina de control interno	• Coordinar las auditorías internas para verificar el cumplimiento de las Políticas y Procedimientos en materia de Protección de Datos Personales y Seguridad de la Información, e informar el resultado de estas. • Realizar los planes de auditoría de los sistemas de Protección de Datos Personales, Seguridad de la Información. • La Oficina de Control Interno diseñara y ejecutara los programas de auditoría de Seguridad de Información y Protección de datos con el fin de verificar el cumplimiento de las políticas establecidas en el artículo 60, de acuerdo con sus funciones, a partir de la firma y divulgación de este documento y realizara el seguimiento correspondiente al Sistema de Seguridad de la

ROL / INSTANCIA / DEPENDENCIA	RESPONSABILIDADES
	Información y Protección de datos.
Oficina de Tecnologías de Información y Comunicaciones – Mesa de Ayuda	• Atender las solicitudes de mantenimiento que puedan afectar la normal prestación de los servicios; así como gestionar su acceso de acuerdo a las solicitudes recibidas de las diferentes Direcciones, Jefaturas o Coordinaciones siguiendo el procedimiento establecido, y así mismo programar e informar a todos los usuarios. • Determinar las estrategias para el mejoramiento de la prestación del soporte tecnológico y la optimización de los recursos tecnológicos. • Brindar el soporte necesario a los usuarios a través del apoyo del recurso humano y los diversos canales de ayuda que se han implementado en el INS.
Propietarios de la información	• Son propietarios de la información cada uno de los directores, así como los jefes de las oficinas donde se genera, procesa y mantiene información, en cualquier medio, propio del desarrollo de sus actividades. • Valorar y clasificar la información que está bajo su administración y/o generación. • Autorizar, restringir y delimitar a los demás usuarios de la institución el acceso a la información de acuerdo a los roles y responsabilidades de los diferentes funcionarios, contratistas o practicantes, que por sus actividades requieran acceder a consultar, crear o modificar parte o la totalidad de la información. • Reportar a la Oficina Asesora Jurídica las Bases de Datos Personales en el momento que surja una actualización para que se tenga actualizado el inventario de las Bases de Datos Personales ante la SIC. • Determinar los tiempos de retención de la información en conjunto con el Grupo de Gestión Documental y las áreas que se encarguen de su protección y almacenamiento de acuerdo a las políticas de la Entidad como de los entes externos y las normas vigentes. • Determinar y evaluar de forma permanente los riesgos asociados a la información, así como los controles implementados para el acceso y gestión de la administración comunicando cualquier anomalía o mejora tanto a los usuarios como a los custodios de esta. • Tienen la responsabilidad y obligación de cumplir con las políticas, normas, procedimientos, buenas prácticas y responsabilidades asignadas en el Sistema de Gestión de Seguridad de la Información y protección de datos personales.
Funcionarios, contratistas,	• Conocer, divulgar, aplicar y cumplir la Política de Seguridad de la Información vigente. • Utilizar solamente la información necesaria para llevar a cabo las funciones que le fueron asignadas, de acuerdo con los permisos establecidos o aprobados en el Manual de Funciones, Código Disciplinario Único o Contrato. • Manejar la Información del INS y rendir cuentas por el uso y

ROL / INSTANCIA / DEPENDENCIA	RESPONSABILIDADES
practicantes y usuarios de la información	protección de tal información, mientras que este bajo su custodia. Esta puede estar almacenada física o electrónicamente. • Proteger la información a la cual accedan y procesen, para evitar su perdida, alteración, destrucción o uso indebido. • Evitar la divulgación no autorizada o el uso indebido de la información. • Cumplir con todos los controles establecidos por los propietarios de la información y los custodios de esta. • Informar a directores, jefes de las oficinas y Supervisores sobre la violación de estas políticas o si conocen de alguna falta a alguna de ellas. • Proteger los datos almacenados en los equipos de cómputo y sistemas de información a su disposición de la destrucción o alteración intencional o no justificada y de la divulgación no autorizada. • Reportar los Incidentes de seguridad, eventos sospechosos y el mal uso de los recursos que identifique. • Proteger los equipos de cómputo y demás dispositivos tecnológicos o técnico científicos asignados para el desarrollo de sus funciones o actividades. • No está permitida la conexión de equipos de cómputo y de comunicaciones ajenos al Instituto a la red Institucional ni el uso de dispositivos de acceso externo a Internet o de difusión de señales de red que no hayan sido previamente autorizadas por la Oficina de Tecnologías de la Información y las Comunicaciones. • Usar software autorizado que haya sido adquirido legalmente por la institución. No está permitido la instalación ni uso de software diferente al Institucional sin el consentimiento de sus superiores y visto bueno de la Oficina de Tecnologías de la información y las Comunicaciones • Aceptar y reconocer que en cualquier momento y sin previo aviso, la Dirección General del Instituto puede solicitar una inspección de la información a su cargo sin importar su ubicación o medio de almacenamiento. Esto incluye todos los datos y archivos de los correos electrónicos institucionales, sitios web institucionales y redes sociales propiedad del Instituto, al igual que las unidades de red institucionales, computadoras, servidores u otros medios de almacenamiento propios de la institución: lo anterior de llegar a ser el caso, con el acompañamiento del Grupo de Gestión del Talento Humano o de la Oficina Asesora Jurídica. • Proteger y resguardar su información personal que no esté relacionada con sus funciones o actividades en la institución. El Instituto Nacional de Salud no es responsable por la pérdida de información, desfalco o daño que pueda tener un usuario al brindar información personal como identificación de usuarios, claves, números de cuentas o números de tarjetas debito/crédito etc. • Tienen la responsabilidad y obligación de cumplir con las

ROL / INSTANCIA / DEPENDENCIA	RESPONSABILIDADES
	políticas, normas, procedimientos, buenas prácticas y responsabilidades asignadas en el Sistema de Gestión de Seguridad de la información y protección de datos personales.

Para la asignación de los roles se cuenta con el formato “Notificaciones de Responsabilidades Roles FOR-R01.0000.036”, el cual se implementará para la asignación cada uno de los roles con los cuales debe contar el sistema de seguridad de la Información.

7.4 MARCO LEGAL

Constitución Política de Colombia. Artículo 15. 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 bancos de datos y en archivos de entidades públicas y privadas.

Ley 44 de 1993. Por la cual se modifica y adiciona la Ley 23 de 1982 y se modifica la Ley 29 de 1944 y Decisión Andina 351 de 2015 (Derechos de autor).

Ley 527 de 1999. Por la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales y se establecen las entidades de certificación y se dictan otras disposiciones.

Ley 1266 de 2008. Por la cual se dictan las disposiciones generales del Hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.

Ley 1273 de 2009. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

CONPES 3701 de 2011. Lineamientos de Política para Ciberseguridad y Ciberdefensa.

Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales.

Ley 1712 de 2014. Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.

Decreto 886 de 2014. Por el cual se reglamenta el Registro Nacional de Bases de Datos.

Decreto 1074 de 2015. Por medio del cual se expide el Decreto Reglamentario del Sector Comercio, Industria y Turismo. Reglamenta parcialmente la Ley 1581 de 2012 e imparten instrucciones sobre el Registro Nacional de Bases de Datos. Artículos 25 y 26.

Decreto 1078 de 2015. Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.

CONPES 3854 de 2016. Política Nacional de Seguridad digital.

Ley 1915 de 2018. Por la cual se modifica la Ley 23 de 1982 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos.

Decreto 1008 del 2018. Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.

Resolución 186 de 27 de 2019. Por la cual se adopta la política de seguridad de la información en el INS y se dictan otras disposiciones.

Resolución 457 de 2020. Por medio de la cual se adiciona el anexo No. 02 de la Resolución 1607 de 2014 y se actualiza la Política de Tratamiento de Datos Personales del instituto Nacional de Salud.

Resolución 0309 de Abril de 2022. Por la cual se actualiza la política de seguridad y privacidad de la información en el INS hoy y se dictan otras disposiciones.

Resolución 1400 de 2022. Por medio de la cual se actualiza el Reglamento de Propiedad Intelectual del Instituto Nacional de Salud - INS, y se dictan otras disposiciones.

Lineamientos del 05 de agosto de 2022 para dar cumplimento a la ley Habeas Data, el cual se encuentra publicado en el portal web del INS, como parte de las políticas institucionales; la cual es obligatorio cumplimiento por parte de todo el Talento Humano del Instituto Nacional de Salud que tenga acceso a los datos tratados y deberá aplicarse a todos los datos de carácter personal registrados en soportes físicos o digitales que sean susceptibles de ser tratados por el Instituto Nacional de Salud como responsable de dichos datos, recolectados en virtud del desarrollo de su objeto misional. Con el objetivo de dar cumplimiento al presente documento, todo el Talento Humano del Instituto Nacional de Salud deberá suscribir y consecuentemente dar cumplimiento al Acuerdo de Confidencialidad FOR-A07.0000-014.

Resolución 0447 de 2023. Por medio de la cual se fija el reglamento interno del equipo de implementación y seguimiento del teletrabajo y se establecen las causales de incumplimiento de las responsabilidades del teletrabajador.

Resolución 214 de 2023.Por medio de la cual se reglamenta el teletrabajo en el Instituto Nacional de Salud.

7.5 DESARROLLO DEL ANEXO A ISO/IEC 27001:2013

DOMINIO: A.6.1 ORGANIZACIÓN INTERNA

Control A.6.1.3 Contacto con las autoridades

Las autoridades que se contemplan en los cuadros corresponden a las entidades competentes, en caso de que se presentara un incidente de cualquier índole, que pusiera en riesgo la confidencialidad, integridad y disponibilidad de la información; en caso de requerirse el llamado a las autoridades mencionadas, sólo podrán hacerlo los funcionarios encargados de la OTIC y que sean los responsables de la notificación.

Descripción	Organización	Contacto
Notificación de Incidentes	Alta Dirección del INS	Alta Dirección
	Comité Institucional de Gestión y Desarrollo INS	Secretario General y/o secretario técnico (planeación)

En primera Instancia al Interior del INS se notifica el incidente que se encontró y el procedimiento a seguir a la Alta Dirección, y posteriormente al Comité Institucional de Gestión y Desarrollo.

Descripción	Organización	Contacto
Acceso abusivo a sistemas informáticos	Centro Cibernético Policial (CCP)	http://www.ccp.gov.co/
Violación de Datos personales		
Uso de Software malicioso		
Suplantación de Sitios Web		
Transferencia no consentida de activos		
Hurto por medios informáticos		
Phishing		
Ingeniería Social		
Respuesta a Emergencias Cibernéticas de Colombia	COLSERT – Grupo de Respuesta a Emergencias Cibernéticas en Colombia	www.colcert.gov.co/
Atención a incidentes de seguridad informática colombiano	CSIRT-CCIT – Centro de Coordinación Seguridad Informática Colombia	https://cc-csirt.policia.gov.co
Emergencia por Incendio	Bomberos	119
Robo	Policía Nacional	112
Antisecuestro y Antiextorsión	GAULA	165
Siniestros ambientales	Defensa Civil	144
Incidentes Laborales	Cruz Roja	132
Incidentes laborales	Centro Toxicológico	136
Robo	DIJIN	157

Control A.6.1.4 Contactos con grupos de Interés Especial

El Contratista *responsable* de Seguridad de la Información, será el encargado de coordinar los conocimientos disponibles en INS, a fin de brindar ayuda en la toma de decisiones en materia de seguridad, éste podrá obtener asesoramiento de otros Organismos.

Se debe mantener contacto permanente con las Universidades, los grupos de investigación, entidades del gobierno, proveedores de tecnología que trabajan en pro de mantener actualizado a las personas que se desarrollan dentro del ámbito de la tecnología, para de esta manera mantenerse al tanto en amenazas, incidentes y soluciones.

Control A.6.1.5 Seguridad de la Información en la gestión de proyectos

1. Los proyectos, convenios, contratos desarrollados por el INS deberán incorporar dentro de la planeación y desarrollo, el cumplimiento de la política de seguridad de la información, valoración de riesgos y los controles a estos.

2. Para la elaboración de los proyectos deben tener en cuenta los lineamientos y directrices del Oficial de seguridad y de la Oficina de Tecnología de la Información y Comunicaciones en referencia de adquisición, desarrollo, transferencia etc.

DOMINIO A.6.2 USO DE DISPOSITIVOS MÓVILES Y TELETRABAJO

Control A.6.2.1 Uso de dispositivos móviles

1. ***Los funcionarios, contratistas y/o terceros*** que haga uso de dispositivo móviles (***Dispositivos USB, Discos Duros externos, PC y/o portátiles personales, tabletas o similares***) de uso personal, para almacenar o acceder a la información del INS deberán, mediante caso a la mesa de ayuda a través de su referente del proceso y la debida ***autorización del jefe de área, indicando el tipo de equipo, procedencia del equipo, justificación y tiempo del permiso***, solicitando la autorización de uso al referente de seguridad de la información, ***quién realizará el estudio del caso y las condiciones a las que haya lugar.***

2. Mesa de Ayuda ***revisara que el software y antivirus instalado estén debidamente licenciados***; adicionalmente realiza la validación y configuraciones de seguridad necesarias en el dispositivo, las cuales, no podrán modificarse mientras este acceda o almacene información del INS.

3. El ***referente*** de Seguridad de la Información debe definir y dar seguimiento al cumplimiento de la Política de dispositivos móviles del INS.

4. Los funcionarios deben proteger física y lógicamente los dispositivos móviles asignados y que son propiedad del INS, para prevenir el hurto y/o acceso o divulgación no autorizada de la información institucional.

5. En caso de pérdida o hurto de un dispositivo móvil de propiedad del INS el funcionario(a), contratista o tercero a quien se le haya asignado el dispositivo, será el responsable de informar con carácter urgente a su jefe inmediato del INS y a la Oficina de Tecnologías de Información y Comunicación – OTIC a través de los canales de comunicación autorizados.

6. La Oficina de Tecnologías de Información y Comunicación (OTIC), está autorizada para realizar la desactivación, eliminación y/o retiro de los permisos de acceso de las aplicaciones y/o cuentas del INS (Correo institucional, One Drive), cuando el dispositivo móvil haya sido extraviado, hurtado o haya sido comprometida su seguridad.

7. El funcionario deberá emplear una aplicación para el borrado remoto de la información cuando este haya sido extraviado, hurtado o haya sido comprometida su seguridad. (*Buscar mi Iphone* en dispositivos Apple, *Android.com/find* en dispositivos Android)

8. La Oficina de Tecnologías de Información y Comunicación – OTIC, adopta e implementa los mecanismos de seguridad, necesarios para salvaguardar la información contenida y transmitida mediante el uso de dispositivos móviles de los funcionarios(as), contratistas y terceros del INS a través de los cuales se les autoriza el acceso a los recursos tecnológicos de la entidad.

Control A.6.2.2 Teletrabajo

Teniendo en cuenta la resolución 0214 del 28 de febrero de 2023 "por medio de la cual se reglamenta la implementación del teletrabajo en el Instituto Nacional de Salud (INS)" y la Resolución 0447 de 14 de abril de 2023 "Por la cual se fija el reglamento interno del equipo de trabajo de implementación y seguimiento del teletrabajo y se establecen las causales de incumplimiento de las responsabilidades del teletrabajador"

1. ***La realización de la visita domiciliaria, para certificar que las instalaciones donde va a laborar el servidor público que se postula a teletrabajar, sean las adecuadas en cuanto a iluminación, ruido, ventilación, puesto de trabajo, ergonomía y ubicación de los elementos del lugar donde realizaría el teletrabajo, es responsabilidad del Grupo de Gestión de Talento Humano, esto según el Art 13 y Art 20 parágrafo 3 de la Resolución 214 del 28 de febrero de 2023.***

2. ***El grupo de Gestión de Talento Humano deberá suministrar oportunamente, la información del retiro o traslado del teletrabajador a su residencia, a la Oficina de Tecnologías de la Información y las Comunicaciones, la cual deberá realizar visita domiciliaria para certificar que las instalaciones donde va a laborar el servidor público que se postula a teletrabajar sean las adecuadas en cuanto a equipo de cómputo, software asignado y antivirus instalado, el cual debe estar debidamente licenciado; esto según el Art 10 resolución 214 del 28 de febrero de 2023.***

3. ***La evaluación de las pruebas de ofimática es responsabilidad de la Oficina de Tecnologías de la Información y las Comunicaciones; esto de acuerdo con el Art 11 de la Resolución 214 del 28 de febrero de 2023.***

4. ***El líder del proceso al cual pertenece el funcionario o teletrabajador debe solicitar a la Oficina de las Tecnologías de Información y las comunicaciones (OTIC), por medio de la generación de un caso en mesa de servicio, la creación de una VPN, indicando el tiempo por el cual se requiere la conexión, sistemas de información y los servicios a los cuales se requiere acceder.***

5. ***La Oficina de TIC´s deberá proporcionar al teletrabajador conexión a través de la Red Privada Virtual del Instituto ó VPN (Virtual Private Network por sus siglas en inglés) del equipo de cómputo para uso en esta modalidad de trabajo y el acceso a la información que requiera y corresponda a la red del INS, con el fin de no ver interrumpido el cumplimiento de sus funciones. Lo anterior regido bajo la política de confidencialidad de la información.***

6. ***Así mismo se debe asegurar la operación en los equipos de trabajo de presencialidad todos los días de jornada habitual, para que, en caso de una solicitud presencial, se asegure la capacidad resolutiva en comunicación con los responsables de estas actividades, como tener disponibilidad de correo electrónico, teléfono, entre otras.***

7. ***Es responsabilidad de Oficina de Tecnologías de la Información y las Comunicaciones, monitorear el uso dado por los teletrabajadores a la conectividad informática proporcionada por el INS para el desarrollo de sus funciones.***

8. ***En caso de que el INS, suministre los equipos y conexión a internet, la Entidad tendrá las siguientes obligaciones:***

- ***Garantizar el mantenimiento de los equipos del teletrabajador, conexiones, programas y valor de la energía, necesarios para desempeñar sus funciones, para lo anterior el Instituto expedirá el respectivo lineamiento de asignación de recursos de acuerdo con la disponibilidad presupuestal de cada vigencia.***
- ***Suministrar al teletrabajador, de acuerdo con la necesidad y la disponibilidad presupuestal y tecnológica, las herramientas tecnológicas que le permitan mantener conectividad con la Entidad.***

9. ***Es responsabilidad del teletrabajador (servidor público) cumplir con los controles técnicos que defina la Oficina de las Tecnologías de Información y las comunicaciones (OTIC) para garantizar la seguridad de la información, en las actividades de teletrabajo incluidas:***

- ***Contar con un espacio y equipo de trabajo que deberá cumplir con las especificaciones técnicas mínimas establecidas por la Oficina de Tecnologías de la Información y las Comunicaciones, en cuanto a software y hardware.***
- ***El Teletrabajador deberá realizar curso presencial o virtual sobre Teletrabajo el cual consta de los siguientes módulos: inducción al teletrabajo, seguridad de la información, competencias digitales y laborales, el cual está diseñado para capacitar a los aspirantes en temas de teletrabajo y demás aspectos relevantes desde las funciones propias de la OTIC***
- ***Presentar y superar la prueba o evaluación de acreditación de competencias y habilidades Tecnológicas: Esta prueba tiene como fin medir, frente a un estándar definido, las habilidades requeridas en el manejo de las herramientas tecnológicas de la información y las comunicaciones para el desempeño efectivo de las funciones en el teletrabajo, si las aprueba, sigue adelante en el proceso***
- ***Utilizar únicamente los equipos de cómputo autorizados por la Entidad para tener acceso a los sistemas de información e infraestructura tecnológica institucional, el cual será ingresado en un inventario donde se tendrá en cuenta la marca, modelo, serial y características (procesador, memoria RAM, almacenamiento, tipo de almacenamiento); este será diligenciado por mesa de ayuda en el momento de la visita domiciliaria.***
- ***Mantener el desarrollo de sus actividades, el debido proceso y la reserva guardando total confidencialidad de la información, claves de acceso a la red o los aplicativos institucionales habilitados para el cumplimiento de sus funciones y no utilizar ningún documento institucional para otro fin distinto al de su labor.***
- ***Tomar las medidas y precauciones necesarias para mitigar cualquier riesgo que puedan correr los equipos o bienes del INS, en caso de que le sean asignados, asi como la información a su cargo.***
- ***Garantizar que los elementos y medios no sean usados ni manipulados por personas distintas al teletrabajador, en caso de ser suministrado por el INS***
- ***Cumplir todos los parámetros de seguridad laboral e informática que le señale el INS durante el desarrollo del teletrabajo.***
- ***Cumplir las reglas relativas al uso de los equipos y programas informáticos, protección de datos personales, propiedad intelectual y seguridad de la información que se encuentren en la ley o que lleguen a señalarse mediante disposiciones internas.***
- ***Entregar a la oficina OTIC de manera trimestral una copia de seguridad de la información recolectada en el ejercicio de las funciones del teletrabajador.***
- ***Reportar a la mesa de servicio, cualquier comportamiento sospechoso o inusual que se detecte cuando se realicen actividades de teletrabajo.***
- ***Conocer y estar alerta a los tipos de amenazas informáticas socializadas por la Entidad para evitar ser víctima de estafas o software malicioso.***

- ***Es responsabilidad del teletrabajador, actualizar el antivirus periódicamente, activar mecanismos de autenticación, habilitar bloqueo de sesiones por inactividad y realizar copias de seguridad para el respaldo de la información, en caso de que el equipo de cómputo sea de propiedad del funcionario.***
- ***En caso de utilizar equipos de propiedad personal para las actividades de teletrabajo, cumplir con los lineamientos de seguridad que determine la Oficina de las tecnologías de información y las comunicaciones para este tipo de dispositivos.***
- ***En caso de tener problemas técnicos con el computador, la VPN, el correo o las aplicaciones propias para las labores desarrolladas en el INS, el teletrabajador debe ingresar un caso en mesa de ayuda para su análisis y resolución; si de acuerdo con la valoración se debiera revisar el equipo de cómputo, el teletrabajador deberá desplazarse con el computador a las instalaciones del INS.***
- ***Devolver en buen estado de conservación y funcionamiento, salvo el deterioro natural, y en observancia del procedimiento establecido para el reintegro de bienes, los equipos asignados y elementos suministrados por la Entidad en caso de suspensión, finalización o retiro del teletrabajo.***
- ***Garantizar que el acceso autorizado a los diferentes sistemas y aplicaciones de la Entidad sea efectuado siempre y en todo momento bajo condiciones de seguridad, de acuerdo con lo establecido en la política de seguridad de información frente al teletrabajo, como aquellas normas adicionales que establezcan lineamientos frente a la seguridad de la información y demás normas que las modifiquen o adicionen.***
- ***Cumplir con las medidas de seguridad que la Entidad ha implementado para asegurar la confidencialidad, privacidad, integridad y disponibilidad de los datos de carácter personal, privados o sensibles a los que tenga acceso en su domicilio, exclusivamente para el cumplimiento de sus obligaciones y funciones propias del cargo.***
- ***Utilizar, para efectos del manejo de información propia del trabajo y producto de las funciones desempeñadas, únicamente el drive y los medios suministrados por el INS para salvaguardar y/o almacenar la información.***

DOMINIO A.7 SEGURIDAD DE LOS RECURSOS HUMANOS
Control A.7.1 Antes de asumir la Vinculación de Funcionarios

Está política aplica para todos los aspectos administrativos y de control que se deben cumplir por parte de los funcionarios, contratistas y quienes tengan algún tipo de relación contractual con el INS dentro del cumplimiento de sus funciones, actividades y demás tareas asignadas, y para conseguir un adecuado nivel de protección de la información, aportando medidas preventivas y correctivas.

Control A.7.1.1 Selección y verificación de antecedentes

1. Se deben realizar las actividades de verificación de las Hojas de vida ***en cuanto a:*** certificaciones ***académicas, experiencia*** y antecedentes (***procuraduría, Contraloría, policía, etc.***) de los candidatos a ser funcionarios y/o contratistas o usuarios de terceras partes, de acuerdo con los reglamentos la ética, las leyes pertinentes y ***reglamentos del INS; los cuales*** deben ser proporcionales a los requisitos del negocio, la clasificación de la información a la cual se va a tener acceso y los riesgos percibidos.

2. Los candidatos, aspirantes, contratistas y proveedores deben dar aprobación al INS para el tratamiento de sus datos personales de acuerdo con la Ley 1032 de 2006, por el cual se dictan disposiciones generales del Habeas Data y se regula el manejo de la información contenida en

base de datos personales; ***alineándose a la política institucional de Habeas Data, publicada en portal institucional. Es obligación del Talento Humano dar estricto cumplimiento al Acuerdo de Confidencialidad suscrito con el Instituto Nacional de Salud, el cual se encuentra en el SIG y fue elaborado por el área jurídica*****.**

3. Se debe dar cumplimiento a la normatividad vigente que regula el empleo público, y al Manual de Funciones, Competencias Laborales y Requisitos de los empleos de la Planta de Personal del INS, ***los cuales se encuentran publicados en el portal web institucional del INS*****.**

4. ***La entidad establece directrices para asegurar que los servidores públicos y contratistas tengan conocimiento sobre los derechos, deberes y responsabilidades en relación de la información establecida en la entidad*****.**

5. ***Los acuerdos contractuales entre la entidad y los servidores públicos o Contratistas especifican el cumplimiento a los lineamientos de seguridad de la información establecidos por la entidad*****.**

6. ***La entidad debe incorporar los roles y responsabilidades en seguridad de la información dentro de las funciones y obligaciones contractuales de los colaboradores y terceros***.

7. ***El incumplimiento o la violación de las políticas de seguridad de la información de la entidad, por parte del o colaboradores o terceros, se les aplicara lo establecido en el proceso de investigaciones disciplinarias***.

Control: A.7.1.2 Términos y condiciones del Empleo

1. A la firma del contrato laboral o posesión del cargo el funcionario, contratista o terceras partes, que van a tener un vínculo con el INS, deben hacer firmar el Acuerdo y/o Cláusula de Confidencialidad y un Anexo de Aceptación de Políticas de Seguridad de la Información; estos documentos deben ser anexados a los demás documentos relacionados con la ocupación del cargo.

2. ***Es obligación del Talento Humano dar estricto cumplimiento a la firma del Acuerdo de Confidencialidad suscrito con el Instituto Nacional de Salud, el cual se encuentra en el SIG y fue elaborado por el área jurídica, siendo este*** parte integral de la carpeta de Talento humano y del contrato si es contratista o proveedor para con el INS.

3. Directores, coordinadores y supervisores de contrato, ***deben*** verificar la existencia de acuerdos y/o cláusulas de confidencialidad y de la documentación de aceptación de políticas para el personal provisto por terceras partes, antes de otorgar acceso a la información del INS.

4. El personal contratista y provisto por terceras partes con el grupo de contractual, deben garantizar el cumplimiento de los acuerdos y/o cláusulas de confidencialidad y aceptación de las Políticas de seguridad de la Información del INS.

5. Se debe asegurar que los funcionarios, contratistas y demás colaboradores del INS, adopten sus responsabilidades en relación con las políticas de seguridad de la información del INS y actúen de manera consistente frente a las mismas, con el fin de reducir el riesgo de hurto, fraude, filtraciones o uso inadecuado de la información o los equipos empleados para el tratamiento de la información.

6. ***En cumplimiento de los requisitos del código único disciplinario los servidores públicos, contratistas y terceras partes, aceptan la obligación legal de mantener la reserva de la información bajo su responsabilidad.***

7. ***Es responsabilidad del jefe Inmediato o Supervisor del contrato, informar las responsabilidades, actividades y tareas asignadas al nuevo personal antes de dar acceso a la información de propiedad del INS.***

8. ***Los funcionarios, contratistas y terceras partes, tienen prohibida la divulgación de información confidencial a la cual tengan acceso, en cumplimiento de sus obligaciones y actividades, en cualquier contexto y sin autorización expresa y documentada de los responsables de los activos de información.***

DOMINIO A.7.2 DURANTE LA EJECUCIÓN DEL EMPLEO

Control: A.7.2.1 Responsabilidades de la Alta Dirección

1. El INS en su interés por proteger su información y los recursos de procesamiento de ***esta***, demostrará el compromiso de la Alta Dirección en este esfuerzo, promoviendo que el personal cuente con el nivel deseado de conciencia en seguridad de la información para la correcta gestión de los activos de información y ejecutando el proceso disciplinario necesario cuando se incumplan las Políticas de seguridad de la información del INS.

2. Cada Supervisor de Contrato, directores, coordinadores, jefes de oficina y la secretaria general debe apoyar la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos del INS.

Control A.7.2.2 Toma de Conciencia, educación y formación en la seguridad de la información

1. Se debe capacitar y sensibilizar a los funcionarios durante la inducción, sobre las políticas de seguridad de la información.

2. Todo funcionario, contratistas y terceras partes deben cumplir a cabalidad con los lineamientos del Sistema de Gestión de Calidad y dar un tratamiento y respeto y aplicabilidad a los procesos, procedimientos, formatos que en el espacio de Intranet se alojan no solo en el área que se encuentran laborando sino a nivel del INS.

3. Los funcionarios del INS deben cumplir con el manual de Ética y buen gobierno junto con la capacitación o inducción.

Control: A.7.2.3 Proceso disciplinario

Las Políticas de Seguridad de la Información pretenden instituir y afianzar la cultura de seguridad de la información entre los que cubren todos los procesos, funcionarios, pasantes, profesionales en entrenamiento, investigadores visitantes o externos ad honorem, o su equivalente, contratistas, colaboradores, y en general, el talento humano temporal o transitorio que se encuentre vinculado o prestando sus servicios al INS mediante relación legal y reglamentaria, contrato, convenio o acto jurídico de cualquier naturaleza del INS.

Por tal razón, las violaciones a las Políticas Seguridad de la Información son clasificadas, con el objetivo de aplicar medidas correctivas conforme con los niveles de clasificación definidos y mitigar posibles afectaciones contra la seguridad de la información. Las medidas correctivas pueden considerar desde acciones administrativas emitidas por la oficina de control interno disciplinario del INS para ejecutar las acciones de orden disciplinario o penal, de acuerdo con las circunstancias***, infracciones y contravenciones a las leyes pertinentes y a lo verificado por entes de control,*** si así lo ameritan.

1. En situaciones de incumplimiento y/o violaciones a las políticas de seguridad de la información.

2. se deberá tramitar el cumplimiento de la ley 1952 de 2019, ley 200 de 1995 y demás normas que reglamenten los procesos disciplinarios para los empleados del estado.

3. Cada supervisor de contrato, directores, o coordinadores, debe comunicar algún incumplimiento ***con el acervo de pruebas que aplique a la brecha detectada que pueda considerarse*** una violación de la seguridad de la información ***al referente de Seguridad de la Información bajo la dirección de la OTIC,*** de acuerdo con las políticas y procedimientos del INS.

4. ***Tras su comprobación,*** La ***Secretaría General*** debe aplicar el proceso disciplinario del Instituto cuando se identifiquen violaciones o incumplimientos a las políticas de seguridad de la información.

5. Los funcionarios y contratistas que, por sus funciones, hagan uso de la información del INS deben dar cumplimiento a las políticas, actividades y procedimientos de seguridad de la información; como también, asistir a las capacitaciones que sean referentes a la seguridad de la información.

DOMINIO A.7.3 POLÍTICA DE TERMINACIÓN O CAMBIO DE EMPLEO, LICENCIAS, VACACIONES O CAMBIO DE LABORES DE LOS FUNCIONARIOS Y PERSONAL PROVISTO POR TERCEROS

Control: A.7.3.1 Terminación o cambio de responsabilidades del empleo

1. Cada Director, coordinador, jefes de oficina, Secretaria General y Supervisor de Contrato debe monitorear y reportar de manera inmediata la desvinculación o cambio de labores de los funcionarios al grupo de Talento Humano y contractual y estas a su vez a la Oficina de Tecnología de Información y Comunicaciones para realizar los trámites correspondientes.

2. ***El proceso de talento humano y/o contratación realiza el proceso de desvinculación, licencias, vacaciones o cambio de labores de los servidores públicos y contratistas llevando a cabo los procedimientos y ejecutando los controles establecidos para tal fin, así mismo los directores, jefes, supervisores de contrato o lideres deben informar la desvinculación o cambio de labores de acuerdo con los procedimientos, esta información debe ser entregada oportunamente al proceso T.I.***

3. ***El Grupo de talento humano y/o contratación, es el encargado de solicitar por medio de la Herramienta de Mesa de Servicio la creación, actualización y eliminación de cuentas de usuario y asignación de equipos de cómputo para el cumplimiento de las actividades que le sean asignadas.***

4. ***En el caso de la Mesa de Ayuda ingresado por desvinculación, licencias, vacaciones o cambio de labores de los servidores públicos y contratistas, se debe especificar si se requiere suspensión, modificación, desactivación o configuración de respuesta automática o reenvío en el caso de correo electrónico.***

5. ***Es responsabilidad de los funcionarios, contratistas y terceras partes, realizar la entrega de la información generada durante el contrato con el INS, una vez finalice el vínculo con la Entidad, así mismo es responsabilidad del jefe Directo o Supervisor del Contrato verificar que esto se cumpla.***

6. ***La información del INS se debe proteger, no se puede reproducir, usar o divulgar, así se haya finalizado la relación contractual por parte de los funcionarios, contratistas y terceras partes con relación contractual.***

7. ***El jefe directo, el líder funcional o supervisor de contrato debe verificar que los accesos queden cerrados al finalizar el contrato. En caso de no ser así, es su responsabilidad afrontar las consecuencias derivadas de posibles casos de violación a la confidencialidad, integridad y disponibilidad de la información.***

DOMINIO 8 GESTIÓN DE ACTIVOS DE INFORMACIÓN

1. ***El INS establece los métodos de identificación y valoración de activos de información, así como la definición de la asignación de responsabilidades, manteniendo mecanismos acordes para el control de riesgos de la información.***

2. ***Es responsabilidad del referente de proceso, jefe de área o director, la identificación y reporte de nuevos activos de información así mismo mantener actualizada la valoración de estos.***

3. ***Los servidores públicos y Contratistas deben hacer devolución de los activos de información asignados a su cargo, una vez finalice la relación contractual con la entidad.***

4. ***Todos los activos de información deben contar con un responsable, que asegure la protección de la información y los datos que son almacenados en cada uno de ellos.***

Control A.8.1 Política de Responsabilidad por los Activos

1. ***No está permitido que áreas diferentes a la Oficina de Tecnologías de la Información y las Comunicaciones conecten a la red de la Entidad equipos de cómputo y servidores sin previa autorización de la Oficina de Tecnologías de la Información y las Comunicaciones.***

2. El INS es el propietario de la información física, así como de la información generada, procesada, almacenada y transmitida con su plataforma tecnológica***;*** cada área del Instituto debe ser responsable de sus activos de información, asegurando el cumplimiento de las directrices que regulen el uso adecuado de la misma.

3. ***Toda la información que genere procese, almacene, transfiera o transmita el INS en medios físicos o digitales, en su servicios tecnológicos, infraestructura tecnológica o activos de información es de su propiedad y solo puede ser utilizada para el cumplimiento de las funciones institucionales.***

4. El propietario de los activos de información es el INS, de la propiedad intelectual y de los avances tecnológicos e intelectuales desarrollados por los funcionarios del INS y los contratistas, derivadas del objeto del cumplimiento de funciones y/o tareas asignadas, como las necesarias para el cumplimiento del objeto del contrato.

5. El INS, como propietario de los activos de información, ***determina que*** los administradores de estos activos son los funcionarios, contratistas o demás colaboradores del INS (denominados "usuarios") que estén autorizados y sean responsables por la información de los procesos a su cargo, de los sistemas de información o aplicaciones informáticas, hardware o infraestructura de Tecnología y Sistemas de Información (TIC).

6. El inventario de activos de información, como lo indica la Resolución 0451 de 2016, mantendrá un inventario actualizado de sus activos de información, bajo la responsabilidad de cada garante de la información.

7. Los ***responsables*** de los activos de información son ***garantes*** de su uso y protección mientras estén en su custodia ya sea física o electrónica. Así mismo, son responsables de informar a los jefes inmediatos de cualquier incidente de seguridad que se pueda presentar, tales como: uso indebido, alteración y/o divulgación no autorizados.

8. Los ***responsables*** de los activos de información deben monitorear periódicamente la validez de los usuarios y sus perfiles de acceso a la información.

9. Los ***responsables*** **de los activos de información deben ser conscientes que los recursos de procesamiento de** información del Instituto.

10. ***Los responsables de los activos de información de cada dependencia deben promover la confidencialidad de la información contenida en los activos categorizada como clasificada y/o reservada, según lo previsto en la normatividad vigente.***

11. ***Los responsables de los activos de información de cada dependencia deben promover el manejo apropiado del activo cuando es eliminado o destruido, de acuerdo con la normatividad vigente, las políticas y procedimientos de gestión de bienes y las tablas de retención documental de la Entidad.***

12. ***Gestionar las copias de respaldo de los activos de información digitales y electrónicos.***

13. ***Gestionar con el Grupo de Gestión documental las copias de respaldo de los activos de información físicos.***

DOMINIO A.8.2 CLASIFICACIÓN DE LA INFORMACIÓN

El INS definirá los niveles más adecuados para clasificar su información de acuerdo con ***la*** sensibilidad, toda la información del INS debe ser identificada, clasificada y documentada de acuerdo a las directrices impartidas por la Oficina Asesora Jurídica para preservar la confidencialidad, integridad y disponibilidad de la misma, con el fin de promover el uso adecuado por parte de los funcionarios del INS y contratistas que se encuentre autorizado y requiera de ella para la ejecución de sus actividades.

Control A.8.2.1 Clasificación de la Información

La información se debe clasificar en función de los requisitos legales, valor de criticidad y susceptibilidad a divulgación o a modificación no autorizada, así:

1. Los propietarios de los activos de información deben clasificar su información de acuerdo a las categorías publica, publica reservada y pública clasificada y guías de clasificación de la Información.

2. Los propietarios de los activos de información son responsables de monitorear periódicamente la clasificación de sus activos de información y de ser necesario realizar su reclasificación.
3. Los usuarios deben acatar los lineamientos de clasificación de la Información para el acceso, divulgación, almacenamiento, copia, transmisión, etiquetado y eliminación de la información contenida en los recursos tecnológicos, así como de la información física del INS.
4. Los propietarios de los activos de información son responsables de monitorear periódicamente la clasificación adecuada de sus activos de información y de ser necesario realizar su reclasificación.
5. ***Cada activo de información de la entidad debe tener un responsable que debe velar por su seguridad. Los propietarios de la información deben garantizar que todos los activos de información reciban un apropiado nivel de protección basados en su valor de confidencialidad, integridad, disponibilidad, riesgos identificados y/o requerimientos legales de retención*.**

Control A.8.2.2 Etiquetado de la Información

1. Se debe tener en cuenta lo que el procedimiento nos indica para el adecuado etiquetado de la información, de acuerdo con el esquema de clasificación de la información que adopte el INS

2. El responsable de la producción de la información etiqueta la información que genera de acuerdo con los niveles de clasificación de la Ley 1712 de 2014.

3. La etiqueta es una marca en la esquina inferior izquierda del documento, que puede tener las siguientes palabras:

   - **Información Pública:** Su rotulo se encuentra en el formato definido para llevar el Inventario y Clasificación de Activos de la Información

   - **Información Pública Clasificada**. Su rotulado se encuentra en el formato de clasificación de la información

   - **Información Pública Reservada**.

     Físicos: Su rotulado se encuentra en el formato definido para llevar la clasificación de la información y su correspondiente en la Tabla de Retención Documental, se coloca un adhesivo de color azul.

     Electrónicos: Su rotulado se encuentra en el formato definido para llevar la clasificación de la información que corresponden a los permisos (controles) otorgados a través del aplicativo.

Control A.8.2.3 Manejo de Activos

El manejo de los activos se desarrolla con la clasificación, según se tiene, en el Inventario de la información de acuerdo con el esquema de clasificación de información y la adopción en el interior del INS.

Control A.8.3 Manejo de medios

Evitar la divulgación, la modificación, el retiro o la destrucción no autorizados de información almacenada en los medios.

Control A.8.3.1 Gestión de Medios

El INS mantiene la protección adecuada y uso de los activos de información en sus servidores y dispositivos de comunicación

Mediante la asignación a los usuarios finales el perfilamiento desde el Directorio activo para poder así brindar una clasificación de roles y funciones. Los usuarios no deben mantener almacenados en los discos duros de las estaciones cliente o discos virtuales de red, archivos de vídeo, música, y fotos y cualquier tipo de archivo que no sean de carácter institucional.

Para la eliminación de medios informáticos de almacenamiento La eliminación de medios informáticos de almacenamiento que contengan Información Confidencial, crítica, sensible o de Uso Interno del INS, debe ser llevada a cabo únicamente por personal autorizado, y en estricto cumplimiento con los documentados y aprobados que están normados en el SIG para tales efectos.

Indicaciones para aplicar

1. La Oficina de Tecnología de Información y Comunicaciones deben establecer las condiciones de uso de periféricos y medios de almacenamiento en la plataforma tecnológica del INS.

2. La Oficina de Tecnología de Información y Comunicaciones debe autorizar el uso de periféricos o medios de almacenamiento en la plataforma tecnológica del instituto de acuerdo con el perfil del cargo del funcionario solicitante.

3. El Grupo Administrativo de Soporte debe implantar los controles que regulen el uso de periféricos y medios de almacenamiento en la plataforma tecnológica del instituto, de acuerdo con los lineamientos y condiciones establecidas por la Oficina de Tecnología de Información y Comunicaciones.

4. ***Se debe coordinar con la Oficina de Tecnología de Información y Comunicaciones la disposición de medios de almacenamiento del instituto, con el fin de establecer si estos ameritan labores de borrado seguro por reasignación o disposición final.***

Control A.8.3.2 Disposición de los medios

El grupo de Mesa de Ayuda debe generar y aplicar lineamientos para la disposición segura de los medios de almacenamiento del instituto, ya sea cuando son dados de baja o reasignados a un nuevo usuario.

Eliminación segura de activos físicos

La Oficina de Tecnología de Información y Comunicaciones en apoyo con la mesa de ayuda brindan los conceptos técnicos para la disposición segura de la información, si existen equipos de cómputo la Mesa de ayuda emplea un método o métodos elegidos por el INS para la eliminación de sus activos físicos, debe elegirse con base en garantizar que aplica un borrado seguro de la información que nos permita evitar fuga de información confidencial o información sensible del INS.

Ningún funcionario y/o contratista o terceras partes podrá eliminar activos físicos ni electrónicos, toda eliminación de activos físicos corresponderá a personal autorizado debidamente capacitado. Toda omisión o violación a esta política que derive en consecuencias dañosas para el INS y/o los Administrados, será gravemente castigada y el infractor será hecho personalmente responsable por las mismas.

El INS tomará todas las medidas administrativas, laborales, civiles y/o penales que la ley le permite para sancionar a los responsables.

Para la reparación ***o*** eliminación de medios de almacenamiento de información ***sensible***, debe hacerse un análisis de riesgo previo a decidir si ***se debe*** reparar o eliminar equipos de almacenamiento de información confidencial o ***sensible***, que se hayan dañado.
En caso de eliminación de medios de almacenamiento que contengan información ***sensible*** previo a ser descartados, los medios de almacenamiento que contienen material sensitivo deben ser físicamente destruidos o sobrescritos de forma segura en vez de utilizar funciones de borrado estándar. La eliminación de los activos físicos debe hacerse conforme los procedimientos establecidos y aprobados y normalizados en el SIG y debe obedecer a criterios de necesidad. No deben eliminarse activos físicos, sin la debida autorización del dueño del activo de Información ya sea físico o electrónico, para tales efectos.

Control A.8.3.3 Transferencia de los medios

1. Los funcionarios y contratistas deben acoger las condiciones de uso de los periféricos y medios de almacenamiento establecidos por la Oficina de Tecnología de Información y Comunicaciones y grupo administrativo.

2. Los funcionarios del INS y contratistas no deben modificar la configuración de periféricos y medios de almacenamiento establecidos por la Oficina de Tecnología de Información y Comunicaciones.

3. Los funcionarios y contratistas son responsables por la custodia de los medios de almacenamiento institucionales asignados.

4. Los funcionarios y contratistas no deben utilizar medios de almacenamiento personales en la plataforma tecnológica del INS.

5. La reubicación de los activos físicos en centro de cómputo dentro del INS debe ser aprobada por la oficina de Tecnología de Información y comunicaciones.

DOMINIO 9: CONTROL DE ACCESO
Control A.9.1 Requisitos para el Control de Acceso

El acceso a la red del INS está controlado mediante un dispositivo de seguridad perimetral Firewall, que permite la segregación de redes y el manejo de políticas de acceso a cada una de ellas. La modificación de estas reglas establecidas en el Firewall debe ser aprobada por el personal responsable en la Oficina de Tecnologías de Información y Comunicación.

Los funcionarios y contratistas que tengan acceso a la información institucional no deben realizar modificaciones sobre ella, sin la debida autorización, y en todo caso, deberán guardar la confidencialidad de la información a la cual tiene acceso.

1. ***La entidad define los lineamientos para asegurar un acceso controlado, físico o lógico, a la información y plataforma tecnológica, considerándolas importantes para el sistema de gestión de seguridad de la información.***

2. ***La entidad establece procedimientos la creación de datos de acceso, suministro de acceso a la información revisión periódica de los accesos otorgados, y desactivación o eliminación de las cuentas de usuario una vez finalizada la relación contractual.***

3. ***Todos los servidores públicos y contratistas con acceso a un sistema de información o a la red informática institucional, dispondrán de una única autorización de acceso compuesta de identificador de usuario y contraseña y serán responsables de las acciones realizadas por el usuario que les ha sido asignado.***

4. ***Si una entidad, empresa o persona externa requiere acceso a la información sensible o critica, se debe suscribir acuerdos de confidencialidad o de no divulgación para salvaguardar la información, así como el cumplimiento de la normativa vigente para la entidad.***

5. ***Las claves son de uso personal e intransferible y es responsabilidad del usuario el uso de las credenciales asignadas.***

6. ***Se llevará a cabo seguimiento a los accesos realizados por los usuarios, con el fin de minimizar los riesgos de pérdida de integridad, disponibilidad y confidencialidad de la información.***

7. ***Todos los usuarios en su primer inicio de sesión deben cambiar las contraseñas suministradas de acceso a la red, sistemas de información, aplicación, entre otros***.

8. Está expresamente prohibido vulnerar los controles de seguridad establecidos por la Oficina de Tecnologías de Información y Comunicación; la violación de esta política podrá acarrear consecuencias disciplinarias, civiles y penales según el caso.

9. La Oficina de Tecnologías de Información y Comunicación, debe asegurar que las redes inalámbricas cuenten con mecanismos de autenticación que evite los accesos no autorizados.

Control A.9.1.2 Acceso a redes y a Servidores de Red

La Oficina de Tecnología de Información y Comunicaciones debe asegurar que la seguridad y los controles de autenticación estén implementadas para todo lo dispuesto por el INS como son el acceso de los usuarios a la red, y a los servicios del datacenter, las redes inalámbricas del Instituto cuenten con métodos de autenticación que evite accesos no autorizados.

Oficina de Tecnología de Información y Comunicaciones, debe establecer controles para la identificación y autenticación de los usuarios provistos por terceras partes en las redes o recursos de red del INS, así como velar por la aceptación de las responsabilidades de ***los terceros***. Además, se debe formalizar la aceptación de las Políticas de Seguridad de la Información por parte de estos, así:

1. Los funcionarios y contratistas deben acoger las condiciones de acceso a la red del INS.

2. Los funcionarios del INS y contratistas no deben configurar otros dispositivos de comunicación ***sin la debida autorización por parte de la OTIC***.

3. Los funcionarios y contratistas son responsables de no utilizar dispositivos personales y realizar malas acciones que ejecuten por acceder a páginas NO institucionales.

Control A.9.2 Gestión de acceso de usuarios

Todos los usuarios del INS tendrán un identificador de red único (ID del usuario) para su uso personal que les permita validar los accesos y verificar su buen uso.

Los responsables de los activos de información deberán realizar revisiones periódicas de los derechos de acceso de los usuarios autorizados a los sistemas de información a intervalos regulares con el fin de cancelar las cuentas redundantes o inactivas.

La Oficina de Tecnologías de Información y Comunicación debe asegurarse, que los usuarios o perfiles de usuario que tienen asignados por defecto los diferentes recursos y/o equipos de la plataforma tecnológica, sean inhabilitados o eliminados.

Control A.9.2.1 Registro y cancelación del usuario

El INS tiene estandarizados privilegios para el control de acceso lógico de cada usuario o grupo de usuarios a las redes de datos, los recursos tecnológicos y los sistemas de información del instituto. Así mismo, velará porque los funcionarios y contratistas que tengan acceso únicamente a la información necesaria para el desarrollo de sus labores y para la asignación de los derechos de acceso que esté regulada por normas y procedimientos establecidos para tal fin.

1. La oficina de tecnología de información y comunicaciones tiene establecido un procedimiento formal para la administración de los usuarios POE-D04-1400-001 sobre los accesos en las redes de datos, los recursos tecnológicos y sistemas de información del instituto, que contemple la creación, modificación, bloqueo o eliminación de las cuentas de usuario.

2. Para la creación del usuario se toma la primera letra del nombre y ***el primer*** apellido, ***para*** la unión del dominio del INS ***(@ins.gov.co) al perfil; se realiza*** con lo parametrizado en el Directorio Activo para acceso a la red, ***de existir usuarios*** con nombres ***y*** apellidos iguales se toma la inicial de segundo nombre o apellido (donde aplique). ***Para los casos donde el usuario solo cuente con un único nombre y apellido debe validarse la generación del usuario con el fin de evitar cuentas homónimas.***

3. La Oficina de Tecnología de Información y Comunicaciones, ***para*** la creación de cuentas de red, debe realizarlo con la notificación o creación de la solicitud o requerimiento por medio de la herramienta de service manager que se encuentra alojad***o*** en la Intranet, en la opción ***‘***cuentas de usuario***’*** y debe presentar la resolución para funcionarios o el contrato para los contratistas.

4. La Oficina de Tecnología de Información y Comunicaciones**,** por medio de una directiva que se parametriz***ó*** en el servidor del Directorio Activo para toda la familia INS**,** cada tres (3) meses le saldrá un aviso ***dónde*** deben oprimir las teclas (Ctrl + ALT Gr + Supr), ***seleccionar*** la opción ‘cambiar contraseña y realizar los pasos que se desplieguen.

5. La Oficina de Tecnología de Información y Comunicaciones previa solicitud de los jefes inmediatos de los solicitantes de las cuentas de usuario y aprobación de los propietarios de los sistemas de información, debe crear, modificar, bloquear o eliminar cuentas de usuarios sobre las redes de datos, los recursos tecnológicos y los sistemas de información administrados, acorde con el procedimiento establecido.

6. Para la creación ***de la*** contraseña, la Oficina de Tecnología de Información y Comunicaciones le socializa al funcionario/contratistas, ***los lineamientos*** que debe tener en cuenta para la construcción de las contraseñas, **las cuales deben cumplir con las siguientes** características:

- (1) Una letra Mayúscula
- (3) tres Dígitos de Número (no deben ser seguidos los números).
- (4) Cuatro Letras minúsculas
- (1) Un carácter especial debe definir lineamientos para la configuración de contraseñas

Control A.9.2.2 Suministro de acceso de usuarios

Se implementó el POE-D04-1400-001 donde se tiene contemplado el acceso formal de usuarios y la inactivación de usuario para los sistemas y servicios

1. Los usuarios deben de realizar la actividad de bloqueo de pantalla cada vez ***que se retiran*** del puesto de trabajo, con (Ctrl + Alt Gr + Supr) y de la misma forma para habilitar la sesión.

2. La oficina de tecnología de información y comunicaciones también contempla en el POE-D04-1400-001 la creación de usuarios ***e inicios de sesión*** en los sistemas de Información.

Control A.9.2.3 Gestión de Derechos de acceso privilegiado

Se debe restringir y controlar la asignación y uso de accesos privilegiados

La Oficina de Tecnología de Información y Comunicaciones del INS, velará porque los recursos de la plataforma tecnológica y los servicios de red del Instituto sean operados y administrados en condiciones controladas y de seguridad, que permitan un monitoreo posterior de la actividad de los usuarios administradores, poseedores de los más altos privilegios sobre la plataforma y servicios.

La Oficina de Tecnología de Información y Comunicaciones con Infraestructura de TI y deben proveer los mecanismos para brindar controles de seguridad a la red del INS, al igual que los funcionarios, contratistas y terceros deben acogerse a los controles de seguridad establecidos.

1. La Oficina de Tecnología de Información y Comunicaciones debe otorgar los privilegios para administración de recursos tecnológicos, servicios de red y sistemas de información sólo a aquellos funcionarios designados para dichas funciones.

2. La Oficina de Tecnología de Información y Comunicaciones debe restringir las conexiones remotas a los recursos de la plataforma tecnológica; únicamente se deben permitir estos accesos a personal autorizado, de acuerdo con las labores desempeñadas u tendientes a resolver requerimientos o solicitudes en relación con sistemas de información.

3. La Oficina de Tecnología de Información y Comunicaciones debe monitorear los recursos tecnológicos, los servicios de red y los sistemas de información que tengan instalados en sus equipos de cómputo utilitarios que permitan accesos privilegiados a dichos recursos, servicios o sistemas, y mesa de ayuda es responsable de su revisión.

4. La Oficina de Tecnología de Información y Comunicaciones, En relación con los administradores de los recursos tecnológicos y servicios de red, no deben hacer uso de los utilitarios que permiten

acceso a los sistemas operativos, firmware o conexión a las bases de datos para pasar por alto la seguridad de los sistemas de información alojados sobre la plataforma tecnológica del INS.

5. La Oficina de Tecnología de Información y Comunicaciones debe validar que las políticas de contraseñas establecidas sobre la plataforma tecnológica, los servicios de red y los sistemas de información son aplicables a los usuarios administradores; así mismo, debe verificar que el cambio de contraseña de los usuarios administradores

6. La Oficina de Tecnología de Información y Comunicaciones debe revisar periódicamente la actividad de los usuarios con altos privilegios en los registros de auditoría de la plataforma tecnológica y los sistemas de información.

Los recursos informáticos del INS no podrán ser utilizados, sin previa autorización escrita, para divulgar, propagar o almacenar contenido personal o comercial de publicidad, promociones, ofertas, programas destructivos (virus), propaganda política, material religioso o cualquier otro uso que no esté autorizado.

Los usuarios no deben realizar intencionalmente actos que impliquen un mal uso de los recursos tecnológicos o que vayan en contravía de las políticas de seguridad de la información entre ellos envíos o reenvíos masivos de correos electrónicos o spam, practica de juegos en línea, uso permanente de redes sociales personales, conexión de periféricos o equipos que causen molestia a compañeros de trabajo, etc.

Los usuarios no podrán efectuar ninguna de las siguientes labores sin previa autorización de la Oficina de Tecnología y Comunicaciones:

- Instalar software en cualquier equipo del INS;
- Bajar o descargar software de Internet u otro servicio en línea en cualquier equipo del INS;
- Modificar, revisar, transformar o adaptar cualquier software propiedad del INS;
- Descompilar o realizar ingeniería inversa en cualquier software de propiedad del INS.
- Copiar o distribuir cualquier software de propiedad del INS.
- Cambiar la configuración de hardware de propiedad del INS

El usuario deberá informar al jefe Inmediato de cualquier violación de las políticas de seguridad, uso indebido y debilidades de seguridad de la información del INS que tenga conocimiento y al Área de Tecnologías de la Tecnología.

Control A.9.2.5 Revisión de los derechos de acceso de usuarios

La Oficina de Tecnología de Información y Comunicaciones realiza periódicamente la revisión de los usuarios con la creación, bloqueo, desbloqueo y en la inactivación de se realiza aproximadamente cada tres (3) meses.

Control A.9.2.6 Retiro o ajuste de los derechos de acceso.

Se **implementó** el POE-D04-1400-001 donde se tiene contemplado el acceso formal de usuarios y la **desactivación** de usuario para los sistemas y servicios.

Control A 9.3 Responsabilidades de Acceso de los Usuarios

Los usuarios de los recursos tecnológicos y los sistemas de información del INS realizarán un uso adecuado y responsable de dichos recursos y sistemas, salvaguardando la información a la cual es permitido el acceso.

1. Los funcionarios y contratistas que utilicen la plataforma tecnológica, los servicios de red y los sistemas de información del INS deben hacerse responsables de las acciones realizadas en los mismos, así como del usuario y contraseña asignados para el acceso a estos.

2. Los funcionarios y contratistas no deben compartir sus cuentas de usuario y contraseñas con otros funcionarios o con personal provisto por terceras partes.

3. Los funcionarios y contratistas que posean acceso a la plataforma tecnológica, los servicios de red y los sistemas de información del Instituto deben acogerse a los lineamientos para la configuración de contraseñas implantados por el Instituto.

4. Ningún usuario deberá acceder a la red o a los servicios TIC del INS, utilizando una cuenta de usuario o clave de otro usuario.

5. Los usuarios no están autorizados para hacer uso de redes externas a través de dispositivos personales en las instalaciones de la entidad (modem USB, router, wifi público, etc.), esto compromete la seguridad de los recursos informáticos del INS.

6. El Oficina de Tecnología de la Información y Comunicaciones del INS, es el área responsable de realizar el aseguramiento de los accesos a internet, acceso a redes de terceros y a las redes de la entidad; esta responsabilidad incluye, pero no se limita a prevenir que intrusos tengan acceso a los recursos informáticos y a prevenir la introducción y propagación de virus.

7. Todo archivo o material descargado o recibido a través de diferentes medios, correo medio magnético/electrónico o descarga de Internet o de cualquier red externa, deberá ser revisado para detección de virus y otros programas maliciosos antes de ser instalados en la infraestructura TIC del INS.

8. Todos los archivos provenientes de equipos externos al INS deben ser revisados para detección de virus antes de su utilización dentro de la red del INS.

9. Todo cambio a la infraestructura informática deberá estar controlado y será realizado de acuerdo con los procedimientos de gestión de cambios de la Oficina de Tecnología de la Información y Comunicaciones del INS

10. Los funcionarios deberán realizar la devolución de todos los activos físicos y/o electrónicos asignados por el INS en el proceso de desvinculación, de igual manera deberán documentar y entregar al INS los conocimientos importantes que posee de la labor que ejecutan para obtener el paz y salvo.

Control A.9.3.1 Uso de información de autenticación secreta

La Oficina de Tecnología de Información y Comunicaciones debe realizar las actividades de control, seguimiento y verificación por medio de la herramienta de Firewall y del uso de los servicios que por medio de la red lógica se brindan y aplican a cada uno de los funcionarios y contratistas. Poder determinar si las consultas realizadas o a los sitios que ingresan son temas institucionales.

Control A.9.4 Control de Acceso a Sistemas y aplicaciones

Los directores, coordinadores, asesores de oficinas, jefes de oficina y la secretaria general como propietarias de los sistemas de información y aplicativos que apoyan los procesos y áreas que lideran, velarán por la asignación, modificación y revocación de privilegios de accesos a sus sistemas o aplicativos de manera controlada.

1. La Oficina de Tecnología de Información y Comunicaciones, como responsable de los sistemas de información y aplicativos en la parte operativa y dueño de la información. propenderá para que estos sean debidamente protegidos contra accesos no autorizados a través de mecanismos de control de acceso lógico. Así mismo, velará porque los desarrolladores, tanto internos como externos, acojan buenas prácticas de desarrollo en los productos generados para controlar el acceso lógico y evitar accesos no autorizados a los sistemas administrados.

2. La Oficina de Tecnología de Información y Comunicaciones debe establecer un procedimiento para la asignación de accesos a los sistemas y aplicativos del INS.

3. La Oficina de Tecnología de Información y Comunicaciones debe establecer ambientes separados a nivel físico y lógico para desarrollo, pruebas y producción, contando cada uno con su plataforma, servidores, aplicaciones, dispositivos y versiones independientes de los otros ambientes, evitando que las actividades de desarrollo y pruebas puedan poner en riesgo la integridad de la información de producción.

4. Los propietarios de los activos de información deben autorizar los accesos a sus sistemas de información o aplicativos, de acuerdo con los perfiles establecidos y las necesidades de uso, acogiendo los procedimientos establecidos.

5. Los propietarios de los activos de información deben monitorear periódicamente los perfiles definidos en los sistemas de información y los privilegios asignados a los usuarios que acceden a ellos.

6. Los desarrolladores deben asegurar que los sistemas de información construidos requieran autenticación para todos los recursos y páginas, excepto aquellas específicamente clasificadas como públicas.

7. Los desarrolladores deben garantizar la confiabilidad de los controles de autenticación, utilizando implementaciones centralizadas para dichos controles.

8. Los desarrolladores deben garantizar que no se almacenen contraseñas, cadenas de conexión u otra información sensible en TEXTO CLARO y que se implementen controles de integridad de dichas contraseñas.

9. Los desarrolladores deben establecer los controles de autenticación de tal manera que cuando fallen, lo hagan de una forma segura, evitando indicar específicamente cual fue la falla durante el proceso de autenticación y, en su lugar, generando mensajes generales de falla.

10. Los desarrolladores deben asegurar que no se despliegan en la pantalla las contraseñas ingresadas, así como deben deshabilitar la funcionalidad de recordar campos de contraseñas.

11. Los desarrolladores deben asegurar que se inhabilitan las cuentas luego de un número establecido de intentos fallidos de ingreso a los sistemas desarrollados.

12. Los desarrolladores deben asegurar que, si se utiliza la reasignación de contraseñas, únicamente se envíe un enlace o contraseñas temporales a cuentas de correo electrónico previamente registradas

en los aplicativos, los cuales deben tener un periodo de validez establecido; se deben forzar el cambio de las contraseñas temporales después de su utilización.

13. Los desarrolladores deben garantizar que el último acceso (fallido o exitoso) sea reportado al usuario en su siguiente acceso exitoso a los sistemas de información.

14. Los desarrolladores deben asegurar la Re-autenticación de los usuarios antes de la realización de operaciones críticas en los aplicativos.

15. Los desarrolladores deben establecer que periódicamente se revalide la autorización de los usuarios en los aplicativos y se asegure que sus privilegios no han sido modificados.

Control A.9.4.1 Restricción de acceso a la información

El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso.

Se implementó el POE-D04-1400-001 donde se tiene contemplado el acceso formal de usuarios y la inactivación de usuario para los sistemas y servicios.

La información personal que se recolecta de pacientes y que se guarde en las bases de datos debe ser anonimizada, para que no sea posible su identificación, pero si su posible análisis.

Control A.9.4.2 Ingreso Seguro

1. En el INS existen unos grupos como son Financiera con el sistema de Información SIIF y la administración de un sistema de Correspondencia, son aquellos sistemas para los cuales se utilizan los TOKEN y cada área son los responsables de administradores de estos sistemas serán los responsables de la generación, actualización y disposición de los Tokens en el INS.

2. Cada usuario que hace uso de los tokens debe tener su propio dispositivo, el cual es exclusivo, personal e intransferible, al igual que la cuenta de usuario y la contraseña de acceso.

3. El almacenamiento de los tokens debe efectuarse bajo estrictas medidas de seguridad, en la tula o sobre asignado para cada token, dentro de caja fuerte o escritorios con llave al interior de las áreas usuarias, de tal forma que se mantengan fuera del alcance de terceros no autorizados.

4. Los usuarios deben notificar al Administrador de los tokens en caso de robo, pérdida, mal funcionamiento o caducidad para que este a su vez, se comunique con las entidades emisoras de dichos tokens.

5. Los usuarios no deben permitir que terceras personas observen la clave que genera el token, así como no deben aceptar ayuda de terceros para la utilización del token.

6. Los usuarios deben responder por las transacciones electrónicas que se efectúen con la cuenta de usuario, clave y el token asignado, en el desarrollo de las actividades como funcionarios del INS. En caso de que suceda algún evento irregular con los tokens los usuarios deben asumir la responsabilidad administrativa, disciplinaria y económica.

7. Los usuarios deben mantener las siguientes indicaciones:

- los tokens asignados en un lugar seco y no introducirlos en agua u otros líquidos.

- Los usuarios deben evitar exponer los tokens a campos magnéticos y a temperaturas extremas.
- Los usuarios deben evitar que los tokens sean golpeados o sometidos a esfuerzo físico.
- Los usuarios no deben abrir los tokens, retirar la batería o placa de circuitos, ya que ocasionará su mal funcionamiento.
- Los usuarios no deben usar los tokens fuera de las instalaciones del INS para evitar pérdida o robo de estos.

Política de uso de Periféricos y medios de Almacenamiento

El uso de periféricos y medios de almacenamiento en los recursos de la plataforma tecnológica del INS será reglamentado por la Oficina de Tecnología de Información y Comunicaciones, considerando las labores realizadas por los funcionarios y su necesidad de uso.

DOMINIO 10 CRIPTOGRAFÍA

Control A.10.1.1 Política sobre el uso de controles criptográficos

La Oficina de Tecnologías de Información y Comunicaciones es la encargada de definir los mecanismos de cifrado de información más apropiados frente a las necesidades del INS con base en el análisis de riesgos y considerando los criterios de confidencialidad, integridad, autenticidad y no repudio en las comunicaciones o en el tratamiento de la información de la entidad, adopta los controles de cifrado de datos que reduzcan los riesgos de seguridad de la información. El uso de herramientas de cifrado será autorizado conforme a los roles o responsabilidades de los funcionarios(as) y contratistas del INS.

Control A.10.1.2 Gestión de Llaves Criptográficas

La Oficina de Tecnologías de Información y Comunicaciones, suministrará las herramientas necesarias para garantizar el cifrado y envío seguro de la información confidencial, sensible, o reservada que será almacenada y/o transmitida al interior o exterior de la entidad.

Toda información sensible, confidencial o reservada que se transmita al interior o fuera de la entidad debe ser encriptada y protegida con una contraseña segura, antes de enviarla al destinatario.

La contraseña de encriptación debe ser compartida con el destinatario por un medio diferente al del envío de la información.

DOMINIO 11 SEGURIDAD FÍSICA Y DEL ENTORNO

Control A.11.5 Áreas Seguras

Todas las áreas destinadas al procesamiento o almacenamiento de información sensible, así como aquellas en las que se encuentren los equipos de comunicaciones y seguridad perimetral y demás infraestructura de TI, serán consideradas como áreas seguras y de acceso restringido para personal no autorizado por la Oficina de Tecnologías de Información y Comunicaciones.

No se permite fumar, ni el ingreso o consumo de alimentos o bebidas en las instalaciones de centros de cómputo y/o de cableado.

En las dependencias donde se gestione, almacene y procesa información del INS deben implementarse controles de acceso seguro, con el fin de prevenir accesos no autorizados, adulteración, perdida, consulta, daños e interferencia en el funcionamiento de los aplicativos e información de la entidad.

Las puertas de acceso a las oficinas e instalaciones del INS deben permanecer cerradas y aseguradas, con el fin de prevenir el acceso de personal no autorizado.
La Oficina de Tecnologías de Información y las Comunicaciones, monitorea periódicamente la temperatura de los espacios destinados como centros de cómputo y/o centros de cableado.

Control A.11.2 Equipos

La administración de hardware conectado a la red y la atención de nuevos requerimientos y adecuaciones, debe realizarse de acuerdo con lo establecido en el procedimiento “Gestión de Sistemas de Información” código: POE-D04.0000-001”; en consecuencia, no pueden conectarse computadores, servidores, dispositivos de comunicaciones como concentradores, switches, enrutadores o cualquier otro hardware a la red, sin la participación y/o supervisión de personal autorizado por la Oficina de Tecnología de la Información y las Comunicaciones.

Todos los servidores y equipos de comunicaciones de voz y datos deben estar localizados en lugares seguros para prevenir el uso o acceso no autorizado. De igual forma, deberá contarse con protecciones físicas y ambientales para los activos críticos, incluyendo perímetros de seguridad, controles de acceso físicos, seguridad en el suministro eléctrico y cableado y sistemas de detección y extinción de incendios.

Se debe prevenir el daño de los equipos por interferencia eléctrica o magnética, riesgo de contaminación por alimentos, bebidas o golpes con objetos que perjudiquen o pongan en riesgo el funcionamiento de ***estos*** o deterioren la información almacenada en ellos. Se debe evitar colocar encima o cerca de los computadores ganchos, clips, bebidas y comidas que se pueden caer accidentalmente dentro del equipo.

El suministro de energía eléctrica deberá estar regulado a 110 voltios y con sistema de polo a tierra, salvo especificación en contrario del fabricante o proveedor de los equipos y se debe contar con sistema de energía ininterrumpida (UPS) y/o planta eléctrica para asegurar el apagado controlado y sistemático o la ejecución continua del parque tecnológico que sustenta las operaciones críticas de la entidad.

La Oficina de Tecnología de la Información y las Comunicaciones deberá elaborar el cronograma de mantenimiento preventivo, el cual será notificado a las dependencias con mínimo 3 días hábiles de antelación con el fin de asegurar la prestación del servicio a los usuarios. Adicionalmente, deberá informarse el nombre e identificación del personal autorizado para realizar las actividades de mantenimiento con el fin de evitar el riesgo de hurto y/o pérdida de equipos.

Ningún funcionario(a) y/o contratista diferente al personal autorizado por la Oficina de Tecnología de la Información y las Comunicaciones, está autorizado(a) para destapar, intervenir, efectuar reparaciones y/o modificaciones en los equipos de cómputo de la entidad. El mantenimiento preventivo y correctivo debe ser realizado exclusivamente por personal especializado y autorizado por la Oficina de Tecnología de la Información y las Comunicaciones.

Cualquier cambio que se realice en el centro de cómputo o centros de cableado, y que potencialmente afecte los sistemas de información de la entidad, debe estar previamente autorizado y registrarse en una bitácora de ingreso al centro de cómputo.

Toda persona que ingrese al centro de cómputo debe estar autorizada y acompañada por un funcionario(a) y/o contratista de la Oficina de Tecnología de la Información y las Comunicaciones. Los administradores del centro de cómputo mantendrán un registro de todas las visitas autorizadas a esta área, en el que se identifique nombre del visitante, documento de identificación, fecha, hora de entrada y salida de las instalaciones, actividad por la cual ingresaron y la persona que autorizó su ingreso. A su vez, todo equipo informático ingresado al centro de cómputo deberá ser registrado.

Constituyen áreas de acceso restringido el centro de cómputo, los cuartos de potencia (Plantas eléctricas, unidades de poder ininterrumpida UPS y cuartos de electricidad) y centros de cableado, por lo que solo el personal autorizado por la Oficina de Tecnología de la Información y las Comunicaciones puede acceder a él. Este personal debe portar el carnet de la entidad que lo acredita como funcionario(a) y/o contratista del área en mención.

Control A.12.2.9 Política de Escritorio y Pantalla Limpia

Toda vez que el personal se ausente de su lugar de trabajo, debe además de bloquear su estación de trabajo, guardar en un lugar seguro cualquier documento, medio magnético u óptico removible que contenga información confidencial.

Si la estación de trabajo del personal está ubicada cerca de zonas de atención de público, al ausentarse de su lugar de trabajo debe guardar también los documentos y medios que contengan información de uso interno.

Al finalizar la jornada de trabajo, el personal debe apagar su equipo de cómputo, guardar en un lugar seguro los documentos y medios que contengan información confidencial o de uso interno, además desconectarse de los sistemas de información y servidores.

Los usuarios deben mantener el puesto de trabajo y escritorio de los equipos de cómputo, organizado y libre de archivos o información institucional que pueda ser objeto de consulta, copiado, eliminación por personal no autorizado.

Las estaciones de trabajo y equipos portátiles de la entidad tendrán aplicado un protector de pantalla definido por la Oficina de Tecnología de la Información y las Comunicaciones, que se activará cuando el equipo permanezca inactivo durante un tiempo determinado. La pantalla de autenticación a la red de la entidad debe requerir solamente la identificación de la cuenta y una clave y no entregar otra información adicional y se configurará el ahorro de energía apagando la pantalla a los quince (15) minutos de inactividad

El papel tapiz se configura automáticamente en cada uno de los equipos conectados a la red LAN del INS.
Al imprimir información confidencial, reservada o pública clasificada, los documentos deberán ser retirados de forma inmediata de las impresoras para evitar divulgación no autorizada de la información.

DOMINIO 12 SEGURIDAD DE LAS OPERACIONES

Control A.12.1 Procedimientos Operacionales y Responsabilidades

La entidad establecerá procedimientos relacionados con la operación y administración de la información institucional, estarán documentados y serán puestos a disposición del personal que lo requiera.

La Oficina de Tecnología de la Información y las Comunicaciones deberá mantener y proveer a su personal, los manuales, guías y procedimientos de configuración de equipos, plataformas informáticas y demás servicios de TI.

Los ambientes de desarrollo, prueba y producción estarán separados físicamente (diferente hardware) siempre que sea posible, y se definirán y documentarán las reglas para la transferencia de software desde el estado de prueba hacia el estado producción.

La Oficina de Tecnología de la Información y las Comunicaciones, cuenta con el procedimiento "*Gestión de Cambios" Código: xxxx* para el control de cambios en el desarrollo de nuevas aplicaciones y en los diferentes ambientes y en general para cualquier cambio que afecte los servicios y la infraestructura tecnológica que soporta la información del INS.

La Oficina de Tecnología de la Información y las Comunicaciones, debe monitorear permanentemente el estado de los recursos y plataformas tecnológicas, (Espacios en disco, memoria, procesamiento, ancho de banda, etc.), así como proyectar el crecimiento de ***los mismos*****,** con el fin de prever y proyectar las futuras necesidades de ampliación de recursos para garantizar su capacidad y adecuada operación.

Control A.12.1.3 Gestión de Capacidad

La Oficina de Tecnología de la Información y las Comunicaciones, debe monitorear permanentemente el estado de los recursos y plataformas tecnológicas, (Espacios en disco, memoria, procesamiento, ancho de banda, etc.), así como proyectar el crecimiento de **estos**, con el fin de prever y proyectar las futuras necesidades de ampliación de recursos para garantizar su capacidad y adecuada operación.

Control A.12.2. Protección de Códigos Maliciosos

La Oficina de Tecnología de la Información y las Comunicaciones designará el funcionario(a) y/o contratista, responsable del software de antivirus para que administre la plataforma y regule el uso y despliegue de la herramienta en todo el INS

Todos los equipos de cómputo de propiedad de la entidad deben tener instalado el software de antivirus debidamente actualizado y licenciado a nombre del INS, por lo tanto, todo nuevo equipo debe ser incluido dentro del dominio de la red de la entidad, para que apliquen las actualizaciones y detecciones correspondientes.

Antes de distribuir, archivos a otros usuarios internos o externos en los equipos de cómputo de la entidad, se debe hacer un análisis de los archivos y medios con el software de antivirus.

Está prohibido desinstalar o deshabilitar el software antivirus de los computadores de la entidad por parte de los usuarios. Si existen indicios de infección por virus informáticos, se debe realizar un análisis del

equipo y sus archivos y verificar su eliminación mediante el software de antivirus y reportar el incidente a la Oficina de Tecnología de la Información y las Comunicaciones.

Todo medio de almacenamiento removible como discos duros externos, dispositivos USB, discos compactos, etc., que vaya a ser conectado a un equipo de la entidad, debe ser analizado con el software de antivirus, como medida previa antes de su uso.
Está prohibido el uso y/ o instalación de software no autorizado por la Oficina de Tecnología de la Información y las Comunicaciones. En caso de necesitar la instalación de algún software, el funcionario(a) y/o contratista responsable debe solicitar la autorización y apoyo a la Oficina de Tecnología de la Información y las Comunicaciones.

La Oficina de Tecnología de la Información y las Comunicaciones, está facultada para revisar periódicamente la información y el software instalado en los equipos de cómputo del INS y realizará la eliminación de los archivos o información no autorizados que puedan atentar contra la seguridad de la información, así como la desinstalación inmediata del software no autorizado.

Control A.12.4. Registro y Seguimiento

La Oficina de Tecnología de la Información y las Comunicaciones, realiza dentro del procedimiento POE-D04.1400-005 el seguimiento y registro de la plataforma tecnológica.

Todas las aplicaciones en producción que la entidad estime pertinentes y que contengan información misional del INS, deben generar logs o trazas de auditoría; igualmente los sistemas que operen y administren información misional valiosa o critica para la entidad, deben tener archivos de logs que contengan evidencia sobre los eventos relevantes que sucedan con la información, y con la seguridad necesaria para su consulta, modificación o borrado.

Todos los logs del sistema y de las aplicaciones deben mantenerse en forma segura, de tal forma que se evite el acceso no autorizado para garantizar la seguridad de esta información.

Todo software o aplicativo habilitado en ambiente de producción de la entidad debe incluir archivos logs que registren como mínimo la siguiente información:
La actividad realizada en la sesión abierta por el usuario incluyendo la identificación del código del usuario, fecha y hora de ingreso y salida de cada sesión del sistema y aplicaciones invocadas.

Control A.12.5. Control de Software Operacional

El INS establece mecanismos para la instalación de software autorizado en los equipos que hacen parte de su infraestructura tecnológica, implementando controles y definiendo el personal responsable de la instalación y soporte.

La Oficina de Tecnología de la Información y las Comunicaciones, validará y realizará las respectivas pruebas calidad y funcionamiento del software a instalar, antes de ser puesto en producción.
La Oficina de Tecnología de la Información y las Comunicaciones, será la responsable de analizar el software y autorizar su instalación, la cual debe ser realizada exclusivamente por personal idóneo y autorizado.

Se debe mantener un registro actualizado del software propiedad Del INS

Control A.12.6. Gestión de la Vulnerabilidad Técnica

La Oficina de Tecnología de la Información y las Comunicaciones, revisará periódicamente las vulnerabilidades y debilidades técnicas de los sistemas de información y la infraestructura tecnológica, mediante el uso de herramientas de software especializadas, en pruebas de penetración, ***pruebas de ingeniería social,*** detección de vulnerabilidades y verificación de controles. En caso de ser necesario, las revisiones podrán realizarse mediante la contratación de una asistencia técnica especializada. El resultado de las revisiones se presentará en un informe técnico para su interpretación y remediación por parte de los especialistas de la entidad.

Se prohíbe la instalación de software por parte de personal diferente a los autorizados por la Oficina de Tecnología de la Información y las Comunicaciones.

DOMINIO 13 SEGURIDAD DE LAS COMUNICACIONES

Control A.13.1. Gestión de la Seguridad de las Redes

La Oficina de Tecnología de la Información y las Comunicaciones, gestiona y establece mecanismos y controles para prestar el servicio de redes de datos y comunicaciones en la entidad y propende por la protección de los datos y los servicios conectados en las redes del INS, contra el acceso no autorizado.

Establecer los procedimientos para la administración de los equipos remotos, incluyendo los equipos en las áreas restringidas.

Establecer controles especiales para salvaguardar la confidencialidad e integridad de los datos que pasan a través de redes públicas, y para proteger los sistemas conectados.

Implementar controles especiales para mantener la disponibilidad de los servicios de red y computadores conectados.

La Oficina de Tecnología de la Información y las Comunicaciones, implementa los mecanismos necesarios y establece acuerdos de niveles de servicio, para garantizar la disponibilidad de los servicios de redes de datos y comunicaciones.

Se debe mantener la confidencialidad de las políticas de enrutamiento y direccionamiento de las redes de datos y comunicaciones de la entidad.

Las direcciones IP internas, configuraciones e información relacionada con la topología y diseño de los sistemas de comunicación y redes de la entidad, serán restringidas, de tal forma que no sean conocidas por usuarios internos, clientes o personas ajenas a la entidad sin la previa autorización de la Oficina de Tecnología de la Información y las Comunicaciones.
Los equipos de acceso a la red estarán protegidos contra accesos no autorizados.

Los funcionarios(as), contratistas o terceros que desarrollen actividades en los sistemas de información de la entidad de manera remota, deben utilizar equipos de cómputo seguros que garanticen la no afectación de la seguridad de la red.

El INS, implementa mecanismos de segmentación de redes a través de ***una Vlan,*** dependiendo de la criticidad de los recursos y servicios involucrados, con el fin de contribuir al control de acceso y optimizar el rendimiento en la red.

Control A.13.2. Transferencia de Información

El INS, establecerá mecanismos seguros para la transferencia de información institucional internamente y con terceros, en cumplimiento de sus funciones y obligaciones legales.

La Oficina de Tecnología de la Información y las Comunicaciones, proporcionará las herramientas para garantizar la seguridad de la información, durante la transferencia a nivel interno y externo.

La entidad proporcionará tecnologías de acceso remoto a sus funcionarios(as) a través de medios como VPN (Red virtual privada), y autorizará su uso de forma particular cuando así se requiera. La Oficina de Tecnología de la Información y las Comunicaciones, garantizará un adecuado esquema de seguridad para los mismos.

Todos los computadores de la entidad que sean accedidos remotamente a través de mecanismos como Internet, enlaces dedicados y otros, deben ser protegidos por mecanismos de control de acceso aprobados por la Oficina de Tecnología de la Información y las Comunicaciones.

La conexión directa entre los sistemas de información de la entidad y otra organización o tercero vía redes públicas de datos como Internet, requieren de la aprobación de la Oficina de Tecnología de la Información y las Comunicaciones, quien definirá los mecanismos de seguridad apropiados.

Como requisito para interconectar las redes de la entidad con otras redes externas, los sistemas de comunicación de terceros deben cumplir con los requisitos de seguridad dispuestos por este documento.
El INS, se reserva el derecho de cancelar y/o terminar la conexión a sistemas de terceros, que no cumplan con los requerimientos internos de seguridad y confidencialidad establecidos o acordados.
Está prohibido el uso de herramientas de acceso remoto o de transferencia de información que no hayan sido autorizadas por la Oficina de Tecnología de la Información y las Comunicaciones.

Está prohibido el envío o intercambio de información sensible, confidencial o reservada, sin la autorización del responsable o jefe inmediato.

Está prohibido utilizar el correo electrónico personal, para el envío y recepción de información institucional sensible, clasificada o reservada.

No está permitido almacenar información institucional en la nube diferente al Office 365 institucional.

El servicio de correo electrónico institucional debe ser utilizado exclusivamente para las tareas propias de la función desarrollada por el INS. El uso del servicio de correo electrónico del INS, para fines personales no está autorizado.

Todo funcionario(a) o contratista inscrito en el INS, dispondrá de una cuenta de correo electrónico activa, y para su creación se debe seguir con el procedimiento Administración de Usuarios Código: POE-D04.1400-001.

El servicio de correo electrónico oficial del INS es el aprobado por la Oficina de Tecnología de la Información y las Comunicaciones; los funcionarios(as), contratistas y terceros reconocen y aceptan que los incidentes de seguridad de la información generados por el uso de servicios de correo electrónico no autorizados serán de su entera responsabilidad.
La clave de acceso al servicio de correo electrónico es personal e intransferible, no debe ser divulgada a ninguna persona, exhibirse en público y para su gestión se debe seguir los controles de protección de contraseñas definidos por el Sistema de Gestión de Seguridad de la Información - SGSI del INS.

El INS, puede supervisar el uso del servicio de correo electrónico para verificar que se está usando para el cumplimiento de las funciones misionales de la entidad, en los procesos de verificación de uso apropiado del servicio de correo electrónico se respetará el derecho a la privacidad e intimidad del titular de la cuenta de correo electrónico.

En los casos en los que se requiera envío o recepción de información confidencial, sensible, reservada o pública clasificada, el usuario del servicio de correo electrónico debe cumplir con las políticas de cifrado establecidas por la entidad, y si es el caso solicitar apoyo técnico a la Oficina de Tecnología de la Información y las Comunicaciones.

La vigencia de la cuenta para funcionarios(as) y contratistas comprende el periodo desde la fecha de ingreso o firma del contrato y finaliza el último día de la fecha de retiro o terminación/suspensión del contrato.

El uso de la cuenta de correo es con fines del cumplimiento de las funciones y/o objeto contractual y su uso es de carácter obligatorio, en ella llegará información oficial de conocimiento necesario para los funcionarios(as) y contratistas de la entidad.

Se prohíbe el uso de cuentas de correo gratuito con propósitos institucionales o cuentas de suscripción gratuita a otros proveedores.

Es responsabilidad del funcionario(a) o contratista depurar su cuenta periódicamente siendo el responsable de realizar las copias de seguridad de sus correos, o si la cuenta es de Office 365 el backup se realizará desde OTIC.

El usuario debe leer diariamente su correo y borrar aquellos mensajes obsoletos, para liberar espacio en su buzón de correo.

No están autorizados los siguientes usos del servicio de correo electrónico y pueden constituir un incidente de seguridad de la información con las consecuencias legales correspondientes:

- Exceder los servicios para los cuales se autorizó la cuenta.
- Enviar mensajes para la difusión de noticias, mensajes políticos, religiosos, correos sin identificar plenamente a su autor o autores o enviar anónimos.
- Difundir “cadenas” de mensajes que saturen el servicio entre otros problemas.

- Perturbar el trabajo de los demás enviando mensajes que puedan interferir con sus actividades laborales.
- Agredir o lesionar directa o indirectamente a otras personas a través del envío de mensajes con contenido que atente contra la integridad y el buen nombre de las personas o instituciones, cualquier contenido que represente riesgo para la seguridad de la información de la entidad o esté prohibido por la leyes, regulaciones o normas a las cuales está sujeta la entidad.
- Crear, enviar, alterar, borrar mensajes suplantando la identidad de un usuario.
- Abrir, usar o revisar indebidamente la cuenta de correo electrónico de otro usuario, sin contar con la autorización formal del titular de la cuenta.
- Suscribir las cuentas de correo institucional en servicios externos (comerciales) con fines no gubernamentales o afines a la misión institucional.
- Enviar correos de información masivos sin estar autorizado para ello.
- Envío de mensajes no deseados o que puedan ser considerados como SPAM.

DOMINIO 14 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS
Control A.14.1. Requisitos de Seguridad de los Sistemas de Información

La Oficina de Tecnología de la Información y las Comunicaciones, se asegurará que, en los procesos de adquisición de nuevos sistemas de información, o de mejora a las aplicaciones de software existentes, se incluyan los requisitos suficientes para garantizar la seguridad de la información de acuerdo a las normas y estándares de desarrollo de software, y a las disposiciones del presente manual.

La Oficina de Tecnología de la Información y las Comunicaciones, será responsable de ejecutar las pruebas necesarias junto con los desarrolladores y/o proveedores externos, que garanticen que las aplicaciones de software adquiridas o mejoradas cumplan con los requisitos de seguridad de la información y exigidos.

La Oficina de Tecnología de la Información y las Comunicaciones, deberá asegurarse que todas las aplicaciones de software desarrolladas o adquiridas cuenten con los respectivos acuerdos de licenciamiento, condiciones de uso y derechos de propiedad intelectual.

La actualización de la información contenida en los portales Web e Intranet del INS, debe hacerse de acuerdo con lo establecido en el POE Actualización de contenidos de los portales web (Internet e Intranet del INS) POE-D04.0000-002.

En caso de que algún componente o servicio del portal Web e Intranet se encuentre en mantenimiento o no disponible por fallas técnicas, se debe publicar una imagen o texto que informe al usuario sobre dicho evento.
La redacción de cada uno de los contenidos de los portales Web e Intranet del INS, está a cargo de los gestores de contenido asignados por cada dependencia.

Los cambios solicitados que requieran modificación de la estructura básica de los portales Web e Intranet o creación de otras nuevas, serán ejecutados exclusivamente por la Oficina de Tecnología de la Información y las Comunicaciones.

Control A.14.2. Seguridad en los Procesos de Desarrollo y Soporte

Los requerimientos de nuevos desarrollos o ajustes a las aplicaciones existentes serán realizados por los responsables de las dependencias propietarias de estas por la mesa de ayuda, de acuerdo con el procedimiento formalmente establecido.

La identificación de las necesidades y requisitos de funcionalidad, calidad y seguridad, se documentan entre la dependencia solicitante y la Oficina de Tecnología de la Información y las Comunicaciones. Los requerimientos del software se deben validar durante el proceso de aceptación del desarrollo de software.

Para el desarrollo y puesta de producción del software, se debe contar con ambientes separados de desarrollo, pruebas y producción, determinando roles y responsabilidades claramente establecidas a fin de evitar modificaciones no autorizadas del código fuente del software.

Los cambios requeridos sobre el software del INS se controlan a través del procedimiento de “Gestión de Cambios”, el cual permite que se documenten y establezcan los requerimientos y los niveles de aceptación del cambio. Dentro de los requerimientos de los cambios es necesario analizar los riesgos asociados a la seguridad de la información y la identificación de los controles a implementar para su adecuada gestión.

En los procesos de desarrollo, el INS, se asegura de establecer las condiciones necesarias para la transferencia de los derechos de propiedad intelectual de códigos fuentes.

La Oficina de Tecnología de la Información y las Comunicaciones se debe asegurar que los desarrollos de software en la entidad se realicen utilizando herramientas de programación licenciadas y reconocidas.

Los desarrollos de software en la entidad deben contar con los manuales técnicos y de usuario además de la respectiva documentación de acuerdo a la metodología utilizada.

Control A.14.3. Datos de Prueba

Para la realización de pruebas, los datos utilizados no deben contener información real de los ambientes de producción, se deben preparar conjuntos de datos de prueba especiales que impidan la pérdida de confidencialidad de la información institucional.

DOMINIO 15 RELACIONES CON LOS PROVEEDORES
Control A.15.1. Seguridad de la Información en las Relaciones con los Proveedores

Los proveedores del INS deberán cumplir las políticas de seguridad en cuanto a la confidencialidad de la información de la entidad.

El INS, establecerá con los proveedores Acuerdos de Niveles de Servicio (ANS) con sus respectivas penalizaciones en caso de incumplimiento de los niveles acordados para cada servicio contratado, y realizará el seguimiento periódico de los mismos.

Antes de conceder acceso a la información institucional del INS, se debe dar a conocer el presente manual a los proveedores a los cuales se otorgará el permiso.

Antes de conceder permisos de acceso a la información a los proveedores, el responsable del activo debe analizar la justificación de la necesidad del acceso, el acceso requerido (físico o lógico), el nivel de clasificación de la información a acceder, la finalidad de uso y los controles mínimos de seguridad a tener en cuenta frente al tratamiento de la información.

En ningún caso se otorgará acceso a los sistemas de información o áreas seguras del INS, hasta no haber formalizado la relación contractual y firmado el acuerdo de confidencialidad con los Proveedores.

En contratos y acuerdos que se establezca con proveedores, se deben considerar y dar tratamiento a los riesgos de seguridad de la información asociados con el cumplimiento de las obligaciones contractuales, la calidad de los productos y servicios adquiridos y la seguridad de la información institucional.

Control A.15.2. Gestión de la Prestación de Servicios de Proveedores

El INS, será responsable de hacer el seguimiento periódico, supervisar y velar por el cumplimiento de las obligaciones contractuales y la calidad de los productos y servicios, así como el cumplimiento de los acuerdos de niveles de servicio establecidos con sus proveedores.

La Oficina de Tecnología de la Información y las Comunicaciones, será la encargada de aprobar los cambios que deban realizar sus proveedores durante la prestación de los servicios, garantizando los principios de seguridad de la información y teniendo en cuenta la criticidad del servicio afectado.

Los proveedores de productos o servicios del INS deben abstenerse de realizar cambios que afecten la prestación de los servicios contratados con la entidad o generen riesgo para la seguridad de la información institucional, sin previo aviso y autorización de la Oficina de Tecnología de la Información y las Comunicaciones.

DOMINIO 16. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Control A.16.1. Gestión de Incidentes y Mejoras en la Seguridad de la Información

El INS establece los responsables para el tratamiento de los incidentes relacionados con la seguridad de la información, en concordancia con las competencias, responsabilidades y los activos a su cargo.

Todos los funcionarios(as) y contratistas y de la entidad deberán reportar de manera oportuna a la Oficina de Tecnología de la Información y las Comunicaciones, las debilidades e incidentes de seguridad que detecte o que sean de su conocimiento.
La Oficina de Tecnología de la Información y las Comunicaciones será el encargado del seguimiento, documentación y análisis de los incidentes de seguridad reportados, así como de su comunicación al jefe inmediato y a los propietarios de la información afectada.

La Oficina de Tecnología de la Información y las Comunicaciones, será la responsable de establecer el procedimiento para la gestión de incidentes de seguridad de la información, en el cual se deben considerar y determinar los criterios para clasificar un evento de seguridad como un incidente, así como los pasos a seguir para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.

Todo evento que se clasifique como un incidente de seguridad, debe ser documentado y tratado de forma inmediata y de acuerdo a los procedimientos formalmente implementados por la entidad.

La solución de un incidente se registrará en una base de conocimientos y lecciones aprendidas, con el fin de que pueda ser consultada y sirva de apoyo oportuno para la prevención de eventos recurrentes o similares. La recurrencia de un incidente deberá ser tratada como un problema.

El INS dará cumplimiento a lo relacionado con Ciberdefensa y Ciberseguridad del Estado Colombiano, según lo dispuesto por los Entes responsables, y reportará cualquier evento o incidente relacionado a los organismos encargados como COLCERT, CSIRT, Policía Nacional, Fiscalía General, etc.

DOMINIO 17. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DE NEGOCIO

Control A.16.1. Continuidad de Seguridad de la Información

La Oficina de Tecnología de la Información y las Comunicaciones será la responsable de identificar las amenazas que puedan ocasionar interrupciones de los procesos y/o las actividades de la entidad en seguridad de la información, evaluará los riesgos para determinar el impacto de dichas interrupciones, identificaran los controles preventivos, y recomendarán ajustes a los planes de contingencia necesarios para garantizar la continuidad de las actividades del INS.

La Oficina de Tecnología de la Información y las Comunicaciones, Formulará los planes, controles y procedimientos necesarios, para asegurar la continuidad de las operaciones en las cuales se de tratamiento a la información institucional del INS.

Los planes deben incluir procedimientos de emergencia, escenarios de contingencia, responsabilidades asignadas, directorio de contactos, plan de capacitación, plan de comunicaciones, plan de adquisiciones, plan de pruebas, entre otros.

En las instalaciones, plataformas o sistemas donde se procese o almacene información institucional crítica, se deben implementar medidas de redundancia suficientes para asegurar la disponibilidad de la información.

DOMINIO 18. CUMPLIMIENTO
Control A.18.1. Cumplimiento de Requisitos Legales y Contractuales

El INS, identificará, documentará, actualizará cuando sea necesario, y dará cumplimiento a la normatividad y requisitos legales relacionados con la seguridad de la información, que estén directamente relacionados con el ejercicio de sus funciones,

Se deben implementar mecanismos o procedimientos para evitar el incumplimiento de las normas de propiedad intelectual, derechos de autor y el uso de software patentado. Validar Resolución 186 de 2019

Cuando el personal de soporte técnico de Oficina de Tecnología de la Información y las Comunicaciones encuentre programas instalados en los equipos de la entidad sin autorización, procederá con la desinstalación inmediata de los mismos.

Las licencias de uso de software estarán bajo custodia de la Oficina de Tecnología de la Información y las Comunicaciones. Así mismo, los manuales y los medios de almacenamiento (CD, cintas magnéticas, dispositivos, etc.), que acompañen a las versiones originales de software.
La Oficina de Tecnología de la Información y las Comunicaciones es la única dependencia autorizada para realizar copia de seguridad del software original, cualquier otra copia del programa original será considerada como una copia no autorizada y su utilización puede conllevar a las sanciones administrativas y legales pertinentes.

El software adquirido por el INS no puede ser copiado o suministrado a terceros sin la debida autorización de la Oficina de Tecnología de la Información y las Comunicaciones y/o sin que se suscriba algún tipo de contrato o convenio por parte del INS, y el tercero.

Se prohíbe el uso e instalación de juegos, software pirata o que aun siendo software libre no esté autorizado por la Oficina de Tecnología de la Información y las Comunicaciones para su uso.

Se prohíbe el acceso y consulta de páginas web o material pornográfico en los computadores del INS. De igual manera está prohibido almacenar archivos de música o videos o cualquier otro elemento que requiera para su uso de una licencia relacionada con derechos de propiedad intelectual, patentes o similares.
Los funcionarios(as), contratistas o terceros responsables de la publicación de la información en los sitios Web e Intranet de la entidad, deberán atender el cumplimiento a las normas en materia de propiedad intelectual y demás políticas establecidas en el presente manual, y bajo ninguna circunstancia deben publicar información sensible, reservada o confidencial que se encuentre en poder del INS.
La entidad efectuará constantes revisiones al cumplimiento de las normas en materia de propiedad intelectual registro de auditoría.

La Oficina de Tecnología de la Información y las Comunicaciones podrá autorizar el uso de material o software declarado como de uso libre, el producido por ella misma o el producido por el titular o propietario externo cuando medie autorización de este, en los términos y condiciones acordados y lo dispuesto en la normatividad vigente; para esto la Oficina de Tecnología de la Información y las Comunicaciones se asegurará que el software cumpla con los requisitos mínimos de seguridad y licenciamiento para su uso.

Control A.18.2. Revisiones de Seguridad de la Información

La Oficina de Tecnología de la Información y las Comunicaciones, verificará permanentemente el cumplimiento de los controles, procedimientos y directrices establecidos en el presente manual de políticas de seguridad de la información y velará por el cumplimiento de las políticas establecidas en el presente manual.

8. DOCUMENTOS DE REFERENCIA

- Anexo 4 Modelo nacional de gestión de riesgos de seguridad de la información para entidades públicas"
- Organización Internacional de Normalización (ISO). Norma Técnica Colombiana NTC-ISO-IEC 27001 – Tecnología de la información. Técnicas de Seguridad. Sistemas de gestión de la seguridad de la Información. Requisitos

9. CONTROL DE CAMBIOS

VERSION	FECHA APROBACION			DESCRIPCIÓN
	aaaa	mm	dd	
00	2021	12	10	Creación del Documento
01	2024	02	16	Como resultado de la revisión manual de la política de seguridad de la información, se actualiza, modifica e incluye lo siguiente: • Cambiar el nombre del documento "MANUAL POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN" A "POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN" • Ajustes de forma a la totalidad del documento en cuanto a ortografía y gramática. • Reorganización de la estructura del documento. o Se mueve el Control A.5.1.1 Política para la Seguridad de la Información, al ítem 7.1 POLITICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN. o Se mueve del ítem 7.1 COMPROMISO DE LA DIRECCION al ítem 7.2 COMPROMISO DE LA ALTA DIRECCIÓN o Se mueve al ítem 7.2.1 Planificación del ítem 7.2 del documento. o Se mueve al ítem 7.2.2 Soporte al ítem 7.3 del documento. o Se mueve al ítem 7.2.3 Operación al ítem 7.4 del documento. o Se mueve al ítem 7.2.4 Evaluación de desempeño al ítem 7.5 del documento. o Se mueve al ítem 7.2.5 Mejora al ítem 7.6 del documento. o Se mueve el Control A.5.1.2 Revisión de las políticas para la Seguridad de la Información al ítem 7.2.6 Aprobación y revisiones de la política. o Se mueve el ítem 5 Definiciones y abreviaturas o Se unifica el ítem 8.3.1 Gestión de los medios, el cual se encontraba duplicado o Se unifica el ítem 8.3.2 Disposición de los medios, el cual se encontraba duplicado o Se unifica el ítem 8.3.3 Transferencia de los medios, el cual se encontraba duplicado • Reorganización y actualización de la tabla de contenido • Modificación del ítem 3. Alcance • Modificación del ítem 7.2 Compromiso alta dirección • Modificación del ítem 6. Condiciones Generales • Modificación e inclusión de Controles A.6.2.1 Uso de dispositivos móviles. • Modificación e inclusión de Controles A.7.1.1 Selección y verificación de antecedentes. • Modificación e inclusión de Controles A.7.1.2 Términos y condiciones del Empleo • Modificación e inclusión de Controles A.7.3.1 Terminación o cambio de responsabilidades del empleo. • Modificación e inclusión de Controles A.8.1 Política de Responsabilidad por los Activos. Inclusión de: • Objetivos • Pie de página mencionando citas bibliográficas del contenido • Ítem 7.3 Organización de la seguridad de la información (roles y

				responsabilidades) • Ítem 7.4 Marco legal • Ítem 8. Definiciones y abreviaturas, en orden alfabético y fuente. • Control A.6.2.2 Teletrabajo • Control A.7.1 Política Antes de asumir la Vinculación de funcionarios. • Controles A.7.3.1 Terminación o cambio de responsabilidades del empleo. • DOMINIO 8 GESTIÓN DE ACTIVOS DE INFORMACIÓN. • Controles A.8.2.1 Clasificación de la Información. • Controles A.9.1 Requisitos para el Control de Acceso Ítem 4, Control A.8.3.1 Gestión de Medios

10. ANEXOS

N/A

INSTITUTO NACIONAL DE SALUD	ELABORÓ	REVISÓ	APROBÓ
	Roger Smith Londoño Buriticá	**Walter Alfonso Floréz Floréz** **Jairo Gómez Mariño** **Jaime Fernando Pérez González**	**Alexandra María López Sevillano**
	Profesional Especializado (E)	**Asesor Dirección General** **Profesional Especializado** **Profesional Contratista OTIC**	**Jefe Oficina de Tecnología Información y Comunicaciones**