COLOMBIA POTENCIA DE LA VIDA

Instituto Nacional de Cancerología Colombia Por el control del cáncer

0322 -

RESOLUCIÓN NÚMERO _____ DE 2024

"Por medio de la cual se adopta la actualización de la Política de Seguridad y Privacidad de la Información (PSPI), en el Instituto Nacional de Cancerología"

LA DIRECTORA GENERAL DEL INSTITUTO NACIONAL DE CANCEROLOGÍA

En uso de sus facultades Constitucionales y Legales, en especial las conferidas por la Ley 2291 de 2023 y,

C O N S I D E R A N D O:

Que de conformidad con el artículo 1 de la ley 2291 de 2023, el Instituto Nacional de Cancerología, es una entidad pública de naturaleza especial, con personería jurídica, patrimonio propio y autonomía administrativa, técnica y financiera, perteneciente al sector descentralizado de la rama ejecutiva del orden nacional, adscrita al Ministerio de Salud y Protección Social e integrante del Sistema General de Seguridad Social en Salud y el Sistema Nacional de Ciencia, Tecnología e Innovación. Regulada en lo pertinente por la Ley 100 de 1993, las Leyes 1122 de 2007, 1438 de 2011 y las demás normas aplicables a los prestadores de servicios de salud de carácter público.

Que, de acuerdo con los numerales 1, 13 y 17 del artículo 9 de la ley 2291 de 2023 el director general tiene dentro de sus funciones expedir los actos administrativos para el desarrollo de su objeto, en lo relacionado con su competencia, que sean necesarios para el funcionamiento de la entidad.

Que, de conformidad con el artículo 209 de la Constitución Política se establece que la función administrativa está al servicio de los intereses generales y se desarrolla con fundamento en los principios de igualdad, moralidad, eficiencia, economía, celeridad, imparcialidad y publicidad, mediante la descentralización, la delegación y la desconcentración de funciones.

Que la Política de Seguridad y Privacidad de la Información es una declaración de las responsabilidades y de la conducta aceptada para mantener un ambiente seguro en el Instituto Nacional De Cancerología. Esta Política establece las directrices y los lineamientos relacionados con el manejo seguro de la información, esto en aras del cumplimiento normativo y regulatorio vigente, la protección de los derechos y el acatamiento a los deberes. La política encuentra alineada para responder a las misiones transformativas del Plan de Desarrollo Institucional PDI con vigencia 2023-2026, formalizado mediante acuerdo 003 de febrero de 2024.

Que mediante acta interna institucional AI-24-00300 del 19 de febrero de 2024, el Comité Directivo del Instituto Nacional de Cancerología aprobó la actualización de la resolución 0238 - Política de Seguridad y Privacidad de la Información (PSPI).

Que la norma ISO 27001:2022, "Tecnología de la información - Técnicas de seguridad - Sistema de gestión de seguridad de la información (SGSI) - Requisitos", ha sido publicada y proporciona pautas actualizadas y mejores prácticas en la gestión de la seguridad de la información.

Que se ha realizado una revisión de los cambios y actualizaciones introducidos en la norma ISO 27001:2022 y se ha identificado la necesidad de actualizar y mejorar ciertos aspectos del SGSI actual para cumplir con los nuevos requisitos y recomendaciones
Que el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) expide el decreto 338 de 2022 por medio del cual se establece los lineamientos generales para fortalecer la gobernanza de la seguridad digital, la identificación de infraestructuras críticas

RESOLUCIÓN NÚMERO 0322 DE 2024

"Por medio de la cual se adopta la actualización de la Política de Seguridad y Privacidad de la Información (PSPI), en el Instituto Nacional de Cancerología"

cibernéticas y servicios esenciales, la gestión de riesgos y la respuesta a incidentes de Seguridad Digital.

Que el decreto 1789 de 2021 por el cual se reglamenta el artículo 18 de la Ley 2069 de 2020 y se adicionan los artículos 2.2.2.47.9 y 2.2.2.47.10 al Decreto 1074 de 2015, en lo relacionado con el uso de la firma electrónica y digital como una herramienta para facilitar la innovación y la transformación digital

Que el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) expide la Resolución 500 de 2021, por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad MSPI como habilitador de la Política de Gobierno Digital, la guía de gestión de riesgos de seguridad de la información y el procedimiento para la gestión de los incidentes de seguridad digital.

Que en la directiva presidencial 03 de 2021 emite lineamientos para el uso de servicios en nube, inteligencia artificial, gestión de datos y seguridad digital para entidades públicas de la rama ejecutiva de orden nacional e invita a su aplicación a entidades territoriales, así como a la rama legislativa y judicial.

Que mediante Documento CONPES 3995 de 2020 del Departamento Nacional de Planeación - Política Nacional de Confianza y Seguridad Digital, se establecen medidas para desarrollar la confianza digital a través de la mejora la seguridad digital de manera que Colombia sea una sociedad incluyente y competitiva en el futuro digital mediante el fortalecimiento de capacidades y la actualización del marco de gobernanza en seguridad digital, así como con la adopción de modelos con énfasis en nuevas tecnologías.

Que la Ley 1952 de 2019 por medio de la cual se expide el Código General Disciplinario, se derogan la Ley 734 de 2002 y algunas disposiciones de la Ley 1474 de 2011, relacionadas con el derecho disciplinario.

Que la Ley 1915 de 2018, por la cual se modifica la Ley 23 de 1982, establece disposiciones en materia de derecho de autor y derechos conexos

Que la Resolución 0185 del 28 de febrero de 2018 por la cual se actualiza el Sistema Integrado de Gestión del Instituto, se adopta el nuevo Modelo Integrado de Planeación y Gestión - MIPG y se constituye el comité institucional de gestión y desempeño, y que acogerá las funciones de comité de seguridad de la información.

Que mediante documento CONPES 3854 de 2016 - Política Nacional de Seguridad Digital, se establece un marco institucional claro y preciso en torno a la seguridad digital.

Que la Ley 1712 de 2014, Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional, tiene por objeto 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, y constituye el marco general de la protección del ejercicio del derecho de acceso a la información pública en Colombia.

Que el Decreto 1377 de 2013, reglamenta parcialmente la Ley 1581 de 2012, por la cual se dictan disposiciones generales para la protección de datos personales, y se definen los objetivos para implementar y cumplir dicha ley.

Que mediante la Ley 1581 de 2012 se expidió el Régimen General de Protección de Datos Personales, el cual, de conformidad con su artículo 1, 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

RESOLUCIÓN NÚMERO 0322 DE 2024

"Por medio de la cual se adopta la actualización de la Política de Seguridad y Privacidad de la Información (PSPI), en el Instituto Nacional de Cancerología"

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 (...)".

Que la ley 1273 de 2009, por medio de la cual se modifica el Código Penal, 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

Que la Circular 015 de 2003 de Ministerio de Protección Social, establece algunos estándares para la historia clínica como proceso y procedimientos del sector salud.

La Ley 527 de 1999, por medio de 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 sobre los mensajes de datos.

Que la Ley 23 de 1982 sobre derechos de autor regula los derechos morales y patrimoniales que la Ley concede a los autores (los derechos de autor), por el solo hecho de la creación de una obra literaria, artística o científica, esté publicada o inédita.

R E S U E L V E:

ARTÍCULO PRIMERO: Adoptar la política de seguridad y privacidad de la información en el Instituto Nacional de Cancerología, la cual se contiene en el documento anexo que hace parte integral de esta resolución.

ARTÍCULO SEGUNDO: Adoptar la norma ISO 27001:2022 como fundamento para actualizar el Sistema de Gestión de Seguridad de la Información (SGSI). Esta actualización desde la norma ISO 27001:2013 refleja el reconocimiento de la institución sobre la importancia de mantenerse actualizada en un entorno digital en constante evolución.

ARTÍCULO TERCERO: OBJETIVOS.

La Política de Seguridad y Privacidad de la informacion (PSPI) adoptada por la institución, tiene como objetivos, los siguientes:

OBJETIVO GENERAL

Establecer las reglas, lineamientos y principios para proteger la información del Instituto Nacional de Cancerología frente a amenazas y riesgos, garantizando su confidencialidad, integridad y disponibilidad durante todo su ciclo de vida.

OBJETIVOS ESPECÍFICOS

1. Identificar y evaluar las posibles amenazas y riesgos de seguridad de la información y continuidad de negocio, desarrollando e implementando estrategias y medidas de mitigación y prevención adecuadas para minimizar los riesgos identificados
2. Promover una cultura organizacional de seguridad de la información y ciberseguridad, fomentando la responsabilidad compartida y la participación de todo el personal.
3. Cumplir con las regulaciones y normativas aplicables en materia de seguridad digital, ciberseguridad y continuidad de negocio.

4. Implementar y mantener un sistema de gestión de la seguridad de la información (SGSI) que asegure el cumplimiento de los lineamientos y reglas establecidos, así como la capacidad de detectar y responder eficazmente a incidentes de seguridad
5. Establecer mecanismos de monitoreo y evaluación para garantizar la eficacia de las medidas de seguridad implementadas, así como para realizar ajustes y mejora continua.
6. Implementar medidas de seguridad específicas para sistemas biomédicos e infraestructuras críticas cibernéticas, para garantizar la integridad de los procesos clínicos y la protección de la salud y vida de los pacientes y partes interesadas.

ARTÍCULO CUARTO: DECLARACIÓN DE LA POLÍTICA.

Nos comprometemos a asegurar la confidencialidad, integridad y disponibilidad de la información, la ciberseguridad, la continuidad operativa y la protección de nuestras infraestructuras críticas, con un enfoque prioritario en la salvaguarda de la salud y la vida de nuestros pacientes y partes interesadas.

ARTÍCULO QUINTO: ALCANCE.

Esta política abarca todas las actividades relacionadas con la gestión de la información, incluyendo la recolección, almacenamiento, procesamiento, transmisión y disposición final de los datos, tanto en formatos físicos como digitales, y se extiende a todas las áreas y sedes del Instituto Nacional de Cancerología.

ARTÍCULO SEXTO: APLICABILIDAD.

Esta política abarca todas las actividades relacionadas con la gestión de la información, incluyendo la recolección, almacenamiento, procesamiento, transmisión y disposición final de los datos, tanto en formatos físicos como digitales, y se extiende a todas las áreas y sedes del Instituto Nacional de Cancerología.

ARTÍCULO SEPTIMO: COMPROMISO DE LA ALTA DIRECCIÓN.

La Dirección del Instituto Nacional de Cancerología reitera su compromiso de liderar la implementación, operación, evaluación y mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI). Se compromete a asignar recursos financieros y humanos adecuados para garantizar la efectiva aplicación de la política y planes de seguridad de la información y la continuidad de negocio. Asimismo, se compromete a integrar la seguridad de la información como un elemento fundamental en las decisiones estratégicas de la institución.

ARTÍCULO OCTAVO: PRINCIPIOS DE SEGURIDAD DE LA INFORMACIÓN.

Los principios fundamentales de seguridad de la información que guían la protección de los datos y sistemas de información institucional son:

- **Confidencialidad**: Garantizar que la información sensible sea accesible únicamente para aquellos autorizados y con un propósito legítimo.
- **Integridad:** Mantener la precisión y completitud de la información a lo largo de su ciclo de vida.
- **Disponibilidad:** Asegurar que la información esté disponible y accesible cuando sea necesario para su uso autorizado.

ARTÍCULO NOVENO: ENFOQUE DE SEGURIDAD DE RED - CONFIANZA CERO (ZTA)

El Instituto adopta la Confianza Cero (Zero Trust Architecture - ZTA) como su modelo de seguridad de red, que requiere la autenticación y verificación rigurosa de cada persona y dispositivo cada vez que intenta acceder a los activos o recursos en la red privada institucional, estableciendo la premisa que ninguna entidad, usuario o dispositivo se considera de confianza por defecto, independientemente de su origen o ubicación.

ARTÍCULO DECIMO: PRINCIPIOS DE LA CONFIANZA CERO (ZTA)

El Instituto establece los siguientes principios fundamentales de seguridad de red basados en el modelo de arquitectura de Confianza Cero (ZTA) para fortalecer su operación de seguridad:

1. **Autenticación fuerte:** Para proteger los sistemas de la entidad contra el acceso no autorizado, se utilizará una combinación de autenticación multifactorial, autorización basada en roles, integración con servicios de autenticación de dominio, y/o implantación de sistemas de autenticación fuerte e inicio de sesión unificado SSO (Single Sign On.)
2. **Menor Privilegio:** Los usuarios y dispositivos solo deben tener acceso a los recursos y datos necesarios para llevar a cabo sus funciones, evitando privilegios innecesarios.
3. **Segmentación de redes:** Se debe segmentar la red en zonas de seguridad para limitar el acceso a los sistemas y datos confidenciales, contener y corregir el impacto de posibles ataques cibernéticos. Los recursos críticos se aislarán y protegerán, minimizando la exposición a amenazas potenciales.
4. **Cifrамiento extremo a extremo:** Los datos sensibles en reposo o en tránsito se deben cifrar para protegerlos contra accesos no autorizados
5. **Telemetría continua:** Se deben detectar, supervisar información de múltiples fuentes de datos de telemetría, salud y capacidad, para identificar patrones y relaciones que podrían indicar una amenaza, fallo, o un riesgo potencial.
6. **Perfilamiento:** Se debe recopilar y analizar información detallada sobre usuarios y dispositivos para determinar su identidad, roles y privilegios, y así garantizar un control de acceso adecuado y preciso.
7. **Inteligencia de amenazas automatizada:** El instituto debe utilizar técnicas y herramientas basadas aprendizaje automático, inteligencia artificial y correlación de riesgo para identificar, detectar y analizar, proteger y automatizar la respuesta ante amenazas cibernéticas, y desplegar capacidades de recuperación efectiva ante ciberincidentes.

ARTÍCULO UNDÉCIMO: PRINCIPIOS INSTITUCIONALES

En el Instituto Nacional de Cancerología, existe un compromiso individual y colectivo de todos los servidores públicos en respetar los principios y valores éticos del actuar institucional (COTOSS):

- Cultura Organizacional centrada en la persona
- Oportunidad de nuestras acciones
- Trabajo multidisciplinario
- Orientación a resultados
- Seguridad de nuestras acciones
- Servicio basado en el respeto y la diferencia

COLOMBIA POTENCIA DE LA VIDA

Instituto Nacional de Cancerología Colombia Por el control del cáncer

0322

RESOLUCIÓN NÚMERO _____ DE 2024

"Por medio de la cual se adopta la actualización de la Política de Seguridad y Privacidad de la Información (PSPI), en el Instituto Nacional de Cancerología"

ARTÍCULO DUODÉCIMO: VIGENCIA.
La presente resolución rige a partir de la fecha de su expedición.

COMUNÍQUESE Y CÚMPLASE

Dada en Bogotá D.C., el 30 ABR 2024

CAROLINA WIESNER CEBALLOS

Director(a) General

Elaboro:<<Carlos Andrés Guerrero – Profesional Especializado – Gestión de Sistemas >>

Revisó: :<<Luis Eduardo Martinez – Coordinador Grupo Area – Gestión de Sistemas>>

Revisó:<<Paula Andrea Solis – Profesional Universitaria – Oficina Asesoría Jurídica>>

Revisó:<< María Margarita Cárdenas – Asesora Jurídica– Oficina Asesoría Jurídica>>

Revisó:<< Lia Margarita Alvarez – Subdirectora – Subdirección Administrativa y Financiera>>

Versión 1 – Fecha 12-07-2023

	INSTITUTO NACIONAL DE CANCEROLOGÍA	CÓDIGO:	GSI-P01-F-01
	GESTIÓN DEL SISTEMA DE DESEMPEÑO INSTITUCIONAL	VERSIÓN:	4
	POLÍTICA INSTITUCIONAL	VIGENCIA:	19-01-2024
		Página 1 de 9	

1. NOMBRE DE LA POLÍTICA:

Política de seguridad y privacidad de la información

2. ALINEACIÓN CON EL PLAN DE DESARROLLO INSTITUCIONAL (PDI):

La Política de Seguridad y privacidad de la información se encuentra alineada para responder a las misiones transformativas del Plan de Desarrollo Institucional PDI con vigencia 2023-2026, formalizado mediante acuerdo 003 de febrero de 2024.

2.1. MISIONES TRANSFORMATIVAS

Implementar la transformación institucional para posicionar al INC como un instituto de investigación, desarrollo, innovación, salud pública, docencia y prestación de servicios oncológicos.

2.2. METAS

Desarrollar estrategias de transformación digital e implementar tecnologías de la información y la comunicación (TIC) para mejorar, de forma permanente, el análisis de la información con seguridad informática.

3. JUSTIFICACIÓN

La implementación de la política de seguridad y privacidad de la información es crucial para los proteger activos críticos, incluyendo datos sensibles, y preservar la integridad y reputación de la institución. Además, asegura el cumplimiento de regulaciones legales y éticas. La prevención de pérdidas financieras es una prioridad estratégica debido a los costos asociados con brechas de seguridad. Los costos asociados con la recuperación de datos, acciones legales y las posibles repercusiones en la salud y vida de pacientes y del personal pueden ser significativos. La gestión de riesgos y la adaptación tecnológica son esenciales para mantener la resiliencia ante amenazas. La confianza de pacientes, familiares y entidades del sector se fortalece mediante la transparencia y el compromiso con la privacidad. La implementación de esta política no solo fortalece la reputación y sostenibilidad del instituto, sino que también establece una base ética y confiable para la atención, la interoperabilidad y el crecimiento sostenible de la entidad.

4. OBJETIVO (S) DE LA POLÍTICA

4.1. OBJETIVO GENERAL

Establecer las reglas, lineamientos y principios para proteger la información del Instituto Nacional de Cancerología frente a amenazas y riesgos, garantizando su confidencialidad, integridad y disponibilidad durante todo su ciclo de vida.

4.2. OBJETIVOS ESPECÍFICOS

1. Identificar y evaluar las posibles amenazas y riesgos de seguridad de la información y continuidad de negocio, desarrollando e implementando estrategias y medidas de mitigación y prevención adecuadas para minimizar los riesgos identificados.

2. Promover una cultura organizacional de seguridad de la información y ciberseguridad, fomentando la responsabilidad compartida y la participación de todo el personal.

3. Cumplir con las regulaciones y normativas aplicables en materia de seguridad digital, ciberseguridad y continuidad de negocio.

4. Implementar y mantener un sistema de gestión de la seguridad de la información (SGSI) que asegure el cumplimiento de los lineamientos y reglas establecidos, así como la capacidad de detectar y responder eficazmente a incidentes de seguridad.

5. Establecer mecanismos de monitoreo y evaluación para garantizar la eficacia de las medidas de seguridad implementadas, así como para realizar ajustes y mejora continua.

6. Implementar medidas de seguridad específicas para sistemas biomédicos e infraestructuras críticas cibernéticas, con el fin de garantizar la integridad de los procesos clínicos, la protección de la salud y la vida de los pacientes y partes interesadas.

5. DECLARACIÓN DE LA POLÍTICA

Nos comprometemos a asegurar la confidencialidad, integridad y disponibilidad de la información, la ciberseguridad, la continuidad operativa y la protección de nuestras infraestructuras críticas, con un enfoque prioritario en la salvaguarda de la salud y la vida de nuestros pacientes y partes interesadas.

6. DESARROLLO DE LA POLÍTICA

6.1. ALCANCE.

Esta política abarca todas las actividades relacionadas con la gestión de la información, incluyendo la recolección, almacenamiento, procesamiento, transmisión y disposición final de los datos, tanto en formatos físicos como digitales, y se extiende a todas las áreas y sedes del Instituto Nacional de Cancerología.

6.2. APLICABILIDAD.

Esta política es de aplicación obligatoria para todo el personal, tanto interno como externo, que tenga acceso a la información del Instituto Nacional de Cancerología, así como para todos los sistemas, procesos y recursos tecnológicos involucrados en el manejo y procesamiento de dicha información.

6.3. COMPROMISO DE LA ALTA DIRECCIÓN.

La Dirección del Instituto Nacional de Cancerología reitera su compromiso de liderar la implementación, operación, evaluación y mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI). Se compromete a asignar recursos financieros y humanos adecuados para garantizar la efectiva aplicación de la política y planes de seguridad de la información y la continuidad de negocio. Asimismo, se compromete a integrar la seguridad de la información como un elemento fundamental en las decisiones estratégicas de la institución.

6.4. PRINCIPIOS DE SEGURIDAD DE LA INFORMACIÓN.

Los principios fundamentales de seguridad de la información que guían la protección de los datos y sistemas de información institucional son:

- **Confidencialidad**: Garantizar que la información sensible sea accesible únicamente para aquellos autorizados y con un propósito legítimo.
- **Integridad:** Mantener la precisión y completitud de la información a lo largo de su ciclo de vida.
- **Disponibilidad:** Asegurar que la información esté disponible y accesible cuando sea necesario para su uso autorizado.

6.5. ENFOQUE DE SEGURIDAD DE RED - CONFIANZA CERO (ZTA)

El Instituto adopta la Confianza Cero (Zero Trust Architecture - ZTA) como su modelo de seguridad de red, que requiere la autenticación y verificación rigurosa de cada persona y dispositivo cada vez que intenta acceder a los activos o recursos en la red privada institucional, estableciendo la premisa que ninguna entidad, usuario o dispositivo se considera de confianza por defecto, independientemente de su origen o ubicación.

6.6. PRINCIPIOS DE LA CONFIANZA CERO (ZTA)

El Instituto establece los siguientes principios fundamentales de seguridad de red basados en el modelo de arquitectura de Confianza Cero (ZTA) para fortalecer su operación de seguridad:

1. **Autenticación fuerte:** Para proteger los sistemas de la entidad contra el acceso no autorizado, se utilizará una combinación de autenticación multifactorial, autorización basada en roles, integración con servicios de autenticación de dominio, y/o implantación de sistemas de autenticación fuerte e inicio de sesión unificado SSO (Single Sign On.)
2. **Menor Privilegio:** Los usuarios y dispositivos solo deben tener acceso a los recursos y datos necesarios para llevar a cabo sus funciones, evitando privilegios innecesarios.
3. **Segmentación de redes:** Se debe segmentar la red en zonas de seguridad para limitar el acceso a los sistemas y datos confidenciales, contener y corregir el impacto de posibles ataques cibernéticos. Los recursos críticos se aislarán y protegerán, minimizando la exposición a amenazas potenciales.
4. **Cifrамiento extremo a extremo:** Los datos sensibles en reposo o en tránsito se deben cifrar para protegerlos contra accesos no autorizados.
5. **Telemetría continua:** Se deben detectar, supervisar información de múltiples fuentes de datos de telemetría, salud y capacidad, para identificar patrones y relaciones que podrían indicar una amenaza, fallo, o un riesgo potencial.
6. **Perfilamiento:** Se debe recopilar y analizar información detallada sobre usuarios y dispositivos para determinar su identidad, roles y privilegios, y así garantizar un control de acceso adecuado y preciso.
7. **Inteligencia de amenazas automatizada:** El instituto debe utilizar técnicas y herramientas basadas aprendizaje automático, inteligencia artificial y correlación de riesgo para identificar, detectar y analizar, proteger y automatizar la respuesta ante amenazas cibernéticas, y desplegar capacidades de recuperación efectiva ante ciberincidentes.

6.7. NORMATIVA Y MARCOS DE TRABAJO

El Instituto incorpora las siguientes normativas y marcos de trabajo con el fin de gestionar de manera eficaz la seguridad de la información, haciendo uso de las mejores prácticas disponibles:

- ISO/IEC 27001:2022 - Establece el sistema de gestión de seguridad de la información (SGSI). Proporciona un marco para establecer políticas, procedimientos y controles de seguridad.

- ISO/IEC 27002:2022 - Proporciona un conjunto de controles y buenas prácticas específicos que ayudan a implementar los requisitos de seguridad de la información de ISO 27001.
- La ISO 270032:2023 establece una guía de directrices de ciberseguridad para proteger la información, gestionar riesgos y amenazas cibernéticas, y mantener la confianza en el entorno digital.
- MPSI DE MINTIC: El Modelo de Seguridad y Privacidad de la Información - MSPI, imparte lineamientos a las entidades públicas en materia de implementación y adopción de buenas prácticas de seguridad, permitiendo habilitar la implementación de la Política de Gobierno Digital.
- MARCO DE CIBERSEGURIDAD DEL INSTITUTO NACIONAL DE ESTÁNDARES Y TECNOLOGÍA (NIST) - Permite identificar, proteger, detectar, responder y recuperarse de amenazas y vulnerabilidades de ciberseguridad.
- GUÍA PARA LA ADMINISTRACIÓN DEL RIESGO Y EL DISEÑO DE CONTROLES EN ENTIDADES PÚBLICAS - Departamento Administrativo de la Función Pública: Establece la metodología para la gestión del riesgo de seguridad digital basado en la Norma ISO/IEC 31000.
- ISO/IEC 22301:2019 Establece los requisitos para establecer, implementar y mantener el sistema de gestión de la continuidad del negocio.
- LEY 1581 DE 2012 (y sus decretos reglamentarios): desarrolla 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

6.8. IMPLEMENTACIÓN.

La política de seguridad y privacidad de la información, y el sistema de gestión de seguridad de la información SGSI se implementan mediante:

- Plan estratégico de seguridad y privacidad de la información (PESI), en el cual se define el Sistema de gestión de seguridad de la información institucional SGSI
- Plan de riesgos de seguridad y continuidad digital
- Plan de sensibilización y capacitación en seguridad digital y ciberseguridad
- Procedimiento para gestión de tecnologías de la información y la comunicación
- Declaración de controles de Seguridad
- Manual de seguridad de historia clínica y telesalud
- Manual de política seguridad y continuidad digital
- Manual de contraseñas y control de acceso
- Manual de Criptografía
- Manual de gestión de capacidad TI
- Manual de gestión de incidentes de Seguridad
- Manual de política de tratamiento de datos personales
- Manual para recuperación de desastres informáticos
- Guía de estrategia de respaldo de la información
- Plan de emergencias y contingencias hospitalarias

6.9. INDICADORES.

Se describen los indicadores que miden la política frente a los objetivos generales y específicos, los cuales se registran en el sistema SIAPINC.

Objetivo general	Indicador	Medición
Establecer las reglas, lineamientos y principios para proteger la información del Instituto Nacional de Cancerología frente a amenazas y riesgos, garantizando su confidencialidad, integridad y disponibilidad durante todo su ciclo de vida.	• POA: Porcentaje de ejecución del plan de seguridad y privacidad de la información • POA: Adopción de la norma ISO27001:2022	• Frecuencia: Trimestral • Frecuencia: Anual
Objetivos Específicos	**Indicador**	**Medición**
Identificar y evaluar las posibles amenazas y riesgos de seguridad de la información y continuidad de negocio, desarrollando e implementando estrategias y medidas de mitigación y prevención adecuadas para minimizar los riesgos identificados.	• POA: Porcentaje de cumplimiento de monitoreo y seguimiento de riesgos proceso GTI • POA: Porcentaje de riesgos materializados proceso GTI • POA: Actualización del mapa de riesgos del proceso GTI	• Frecuencia Trimestral • Frecuencia Mensual • Frecuencia Anual
Promover una cultura organizacional de seguridad de la información y ciberseguridad, fomentando la responsabilidad compartida y la participación de todo el personal.	• POA: Porcentaje de ejecución del plan de capacitación y sensibilización en seguridad de la información • PROCESO: Porcentaje apropiación de seguridad digital	• Frecuencia Semestral • Frecuencia Anual
Cumplir con las regulaciones y normativas aplicables en materia de seguridad digital, ciberseguridad y continuidad de negocio.	• POA: Diligenciamiento de Ejercicio de autoevaluación de MSPI de MINTIC • POA: Registro de activos de Información actualizados • PROCESO: Porcentaje de disponibilidad en canales de comunicación para recepción de solicitudes de tratamiento de datos personales en digital • PROCESO: Porcentaje de tratamiento de eventos de datos personales en digital	• Frecuencia Anual • Frecuencia Anual • Frecuencia Trimestral • Frecuencia Trimestral

	• PROCESO: Porcentaje de incidentes de seguridad y continuidad con nivel Crítico y altos, gestionados y reportados a Csirt Gobierno	• Frecuencia Mensual
Implementar y mantener un sistema de gestión de la seguridad de la información (SGSI) que asegure el cumplimiento de los lineamientos y reglas establecidos, así como la capacidad de detectar y responder eficazmente a incidentes de seguridad	• PROCESO: E-Disponibilidad de los Sistemas de información (7x24)	• Frecuencia Mensual
	• PROCESO: Disponibilidad de Servicio publicados en WEB	• Frecuencia Mensual
	• PROCESO: Porcentaje de disponibilidad del sistema SAP	• Frecuencia Mensual
	• PROCESO: Porcentaje de acciones realizadas para el tratamiento de programas maliciosos	• Frecuencia Trimestral
	• Porcentaje de actualizaciones críticas aplicadas y liberadas en el mismo periodo	• Frecuencia Mensual
	• PROCESO: Porcentaje de eventos e incidentes solucionados antes de una hora relacionados con la seguridad de la información	• Frecuencia Mensual
	• Porcentaje de eventos relacionados con seguridad de la información cerrados	• Frecuencia Mensual
	• Porcentaje de incidentes de seguridad y continuidad con nivel Crítico y altos, gestionados y reportados a Csirt Gobierno	• Frecuencia Mensual
	• PROCESO: Investigaciones realizadas por inteligencia artificial	• Frecuencia Mensual
	• PROCESO: Tiempo de respuesta de NDR - SOC	• Frecuencia Mensual
	• PROCESO Comportamientos anómalos controlados - NDR /**SOC**	• Frecuencia Mensual
	• Porcentaje de disponibilidad en canales de comunicación para recepción de solicitudes de tratamiento de datos personales en digital	• Frecuencia Mensual

	• Porcentaje de tratamiento de eventos de datos personales en digital	• Frecuencia Trimestral
Establecer mecanismos de monitoreo y evaluación para garantizar la eficacia de las medidas de seguridad implementadas, así como para realizar ajustes y mejora continua.	• POA: Indicador - Porcentaje de acciones de mejora cerradas oportunamente, proceso GTI • POA: Documento BIATI Actualizado • Porcentaje apropiación de seguridad digital	• Frecuencia: Mensual • Frecuencia: Anual • Frecuencia Anual
Implementar medidas de seguridad específicas para sistemas biomédicos e infraestructuras críticas cibernéticas, con el fin de garantizar la integridad de los procesos clínicos, la protección de la salud y la vida de los pacientes y partes interesadas	• PROCESO: Porcentaje de actualizaciones críticas aplicadas y liberadas en el mismo periodo • PROCESO: Porcentaje de cumplimiento de las pruebas programadas del centro de Recuperación de Desastres • Porcentaje de ejecución promedio de backup y custodia de la información • POA: Ejecución de pruebas de Hacking Ético	• Frecuencia: Mensual • Frecuencia: Anual • Frecuencia: Semestral • Frecuencia: Anual

6.10. REVISIONES Y ACTUALIZACIONES.

Esta política tiene una vigencia máxima de 3 años, será revisada periódicamente para garantizar su relevancia y eficacia continua, y se actualizará según sea necesario para adaptarse a los cambios en el entorno tecnológico y normativo.

El Instituto Nacional de Cancerología realizará revisiones periódicas al SGSI. Dichas revisiones estarán enfocadas en los siguientes aspectos:

- Revisión de cumplimiento de la norma ISO 27001
- Revisión de indicadores definidos para Política de segruidad y privacidad y SGSI
- Revisión de avance en la implementación del Modelo de Seguridad y Privacidad de la Información.
- Revisión de avance de la Política de Seguridad Digital de acuerdo con lo solicitado por FURAG o la herramienta definida para tal fin.

6.11. CUMPLIMIENTO Y SANCIONES.

El incumplimiento de esta política puede dar lugar a medidas disciplinarias, incluyendo sanciones administrativas y legales, de acuerdo con las políticas y regulaciones internas del Instituto Nacional de Cancerología, el código general disciplinario, y demás leyes aplicables.

6.12. PRINCIPIOS INSTITUCIONALES

En el Instituto Nacional de Cancerología, existe un compromiso individual y colectivo de todos los servidores públicos en respetar los principios y valores éticos del actuar institucional (COTOSS):

- **C**ultura Organizacional centrada en la persona
- **O**portunidad de nuestras acciones
- **T**rabajo multidisciplinario
- **O**rientación a resultados
- **S**eguridad de nuestras acciones
- **S**ervicio basado en el respeto y la diferencia

7. ANEXOS

Sin Anexos

8. CONTROL DE ACTUALIZACIÓN DE LA POLÍTICA

Versión	Fecha de la actualización	Descripción de la actualización
5	19-02-2024	Actualización por cambio de norma ISO 27001:2013 a ISO 27001:2022, y cambio de enfoque de seguridad Cero Confianza - ZTA

0322

VERSIÓN	FECHA DE ACTUALIZACIÓN	DESCRIPCIÓN DE ACTUALIZACIÓN	RESPONSABLE OYM
1	07-06-2017	Versión inicial del documento	Administrador del Sistema Tms
2	06-09-2019	Actualización se incluye declaración de la política, justificación , Nombre de la política y alineación con el PDI	Paula Andrea Salamanca Medina
3	23-09-2020	Se elimina el campo de antecedentes, se incluye el máximo de palabras en el campo de objetivo general, declaración de la política, en el punto de desarrollo de la política se desagrega en implementación e indicadores	Paula Andrea Salamanca Medina
4	19-01-2024	No se realizan cambios en la estructura del documento, se actualiza la razón social del documentos eliminando las siglas ESE y se genera nueva versión	Xiomara Faizuly Rubiano Aguilar

ELABORÓ		REVISÓ		APROBÓ	
Cargo:	Profesional Universitario	Cargo:	Jefe Oficina Asesora de Planeación y Sistemas	Cargo:	Jefe Oficina Asesora de Planeación y Sistemas
Dependencia:	Oficina Asesora de Planeación y Sistemas	Dependencia:	Oficina Asesora de Planeación y Sistemas	Dependencia:	Oficina Asesora de Planeación y Sistemas
Fecha:	16-01-2024	Fecha:	18-01-2024	Fecha:	18-01-2024

30 ABR 2024

Vo.Bo. PS