REPUBLICA DE COLOMBIA

Libertad y Orden

MINISTERIO DE SALUD Y PROTECCIÓN SOCIAL
INSTITUTO NACIONAL DE CANCEROLOGIA
Empresa Social del Estado

RESOLUCION NÚMERO

(0238)

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 Cancerologia Empresa Social del Estado

EL DIRECTOR GENERAL DEL INSTITUTO NACIONAL DE CANCEROLOGIA-EMPRESA SOCIAL DEL ESTADO

En uso de sus facultades legales y en especial las conferidas por el artículo 9º literal a., del decreto 1177 de 1999, y

CONSIDERANDO

Que el INSTITUTO NACIONAL DE CANCEROLOGÍA - EMPRESA SOCIAL DEL ESTADO (INC), es una entidad descentralizada, adscrita al Ministerio de Salud y Protección Social, con personería jurídica y autonomía administrativa y financiera, regulada en lo pertinente por la ley 100 de 1993, las leyes 1122 de 2007, 1438 de 2011, 1751 de 2015 y las demás normas aplicables a los prestadores de servicios de salud de carácter público en general y, en particular, por el decreto 1876 de 1994 y el decreto 5017 de 2009.

Que la Constitución Política en el artículo 15 establece que todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar.

Que la Ley 1555 de 2019 por el cual se expide el Plan Nacional de Desarrollo 2019-2022 “Pacto por Colombia, Pacto por la Equidad” en su artículo 147 define los principios orientadores de Transformación Digital Pública.

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 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.

Que la Ley 1341 de 2009 en su Artículo dos por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC–, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones, establece como principio orientador que el Estado velará por la adecuada protección de los derechos de los usuarios de las Tecnologías de la Información y de las Comunicaciones, así como por el cumplimiento de los derechos y deberes derivados del Hábeas Data, asociados a la prestación del servicio.

Que todos los funcionarios y contratistas de Instituto Nacional de Cancerología deben acogerse a lo estipulado en la Ley 23 de 1982 sobre derechos de autor, la Decisión 351 de 1993 de la Comunidad Andina de Naciones, así como cualquier otra que adicione, modifique o reglamente la materia de comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.

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 Cancerologia Empresa Social del Estado

Que en el capítulo VII de la Ley 599 de 2000 se establecen las disposiciones relacionadas con la violación a la intimidad, reserva e interceptación de comunicaciones.

Que la ley 527 de 1999 define 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.

Que la Ley 1266 de 2008 dicta las disposiciones generales del hábeas data y 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.

Que la Ley 1581 de 2012, por la cual se dictan disposiciones generales para la protección de datos personales tiene como 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 y que dicta, además de las disposiciones generales para la protección de datos personales.

Que la 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, define en su Artículo 1, que "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.

Que a su vez el artículo 20 de la misma Ley indica que los sujetos obligados deberán mantener un índice actualizado de los actos, documentos e informaciones calificados como clasificados o reservados.

Que mediante el Decreto 1377 de 2013, por el cual se reglamenta la Ley 1581 de 2012, estableció en su artículo 13 que los responsables del tratamiento deberán desarrollar sus políticas para el tratamiento de los datos personales y velar porque los Encargados del Tratamiento den cabal cumplimiento a las mismas.

Igualmente consagró que las políticas de tratamiento de la información deberán constar en medio físico o electrónico, en un lenguaje claro y sencillo y ser puestas en conocimiento de los titulares.

Que mediante el Conpes 3854 de 2016 se establecen los lineamientos y directrices de seguridad digital y se tienen en cuenta componentes como la educación, la regulación, la cooperación la investigación, el desarrollo y la innovación

Que mediante el Decreto 1078 de 2015, se expidió el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.

Que el Decreto 1008 del 14 de junio de 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

Que la Ley 734 de 2002 por la cual se expide el “Código Disciplinario Único” por la cual se rigen los procesos y acciones disciplinarias que se emprenden contra funcionarios que hayan cometido una violación a la seguridad de la información.

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 el Decreto 1080 de 2015 "Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado".

Que la Resolución Numero 1995 DE 1999 del Ministerio de salud por la cual se establecen normas para el manejo de la Historia Clínica, y en particular en el artículo 15 donde se definen periodos de retención obligatorios para para los prestadores.

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 Cancerologia Empresa Social del Estado

Que el Modelo de Seguridad y Privacidad (MSPI) del Ministerio de Tecnologías de la Información y Comunicaciones, define las buenas prácticas de seguridad, reúne los cambios técnicos de la norma ISO/IEC 27001:2013, legislación de la Ley de Protección de Datos Personales, Transparencia y Acceso a la Información Pública, entre otras.

Que alineados con las políticas de Gobierno en Línea y teniendo en cuenta que la ISO/IEC 27001:2013 es una norma técnica emitida por la Organización Internacional de Normalización, que describe cómo gestionar la seguridad de la información en una organización, se determina que la implementación del Sistema de Gestión de Seguridad de información (SGSI) del INSTITUTO NACIONAL DE CANCEROLOGÍA E.S.E. se realice en el marco de dicha norma, sobre el cual se desarrolla la Política de Seguridad y Privacidad de la Información.

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 E.S.E. Esta Política establece las directrices y los lineamientos relacionados con el manejo seguro de la información, esto en aras de acatar la normatividad vigente, la protección de los derechos y el acatamiento a los deberes.

Que, de acuerdo con lo señalado antes, se precisa realizar la actualización y ajustes a la Política de seguridad y privacidad de la Información (PSPI) de la entidad.

Que mediante acta 011 del 13 de diciembre de 2019, el Comité Directivo aprobó la actualización de la política de seguridad y privacidad de la información.

RESUELVE

CAPITULO 1
DISPOSICIONES GENERALES

ARTÍCULO 1. Objeto. La presente Resolución tiene como objeto adoptar la Política General de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de los servicios en el INSTITUTO NACIONAL DE CANCEROLOGÍA E.S.E., así como definir lineamientos frente al uso y manejo seguro de la información.

ARTÍCULO 2. Alcance. La Política de Seguridad y Privacidad de la Información del INSTITUTO NACIONAL DE CANCEROLOGÍA E.S.E., aplica para toda la entidad: a sus funcionaros, contratistas, docentes, estudiantes terceros, y aquellas personas y ciudadanos que en razón del cumplimiento de sus funciones y las de la entidad compartan, utilicen, recolecten, procesen, intercambien o consulten su información, así como a los Entes de Control, Entidades relacionadas que accedan, ya sea interna o externamente a cualquier archivo de información, independientemente de su ubicación. Así mismo, esta Política aplica a toda la información creada, procesada o utilizada por el INSTITUTO NACIONAL DE CANCEROLOGÍA E.S.E, sin importar el medio, formato o presentación o lugar en el cual se encuentre.

ARTÍCULO 3. Objetivo general de la política. Determinar los lineamientos que permitan proteger la Información y los datos personales que adopta el INSTITUTO NACIONAL DE CANCEROLOGÍA E.S.E (INC), a través de acciones de aseguramiento de la Información teniendo en cuenta los requisitos legales, operativos, tecnológicos, de seguridad y de la institución, alineados con el contexto de direccionamiento estratégico y de gestión del riesgo con el fin de asegurar el cumplimiento de la integridad, disponibilidad, confidencialidad y legalidad de la información. La Seguridad de la Información es una prioridad para el INC, por lo tanto, es responsabilidad de todos los funcionarios y contratistas de la Entidad vigilar por el continuo cumplimiento de las políticas definidas.

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 Cancerologia Empresa Social del Estado

ARTÍCULO 4. Objetivos específicos de la política. El INSTITUTO NACIONAL DE CANCEROLOGÍA E.S.E (INC), para asegurar el cumplimiento de su misión, visión, y objetivos estratégicos alineados a sus valores institucionales, establece la compatibilidad de la Política de Seguridad y Privacidad de la Información y los objetivos específicos de seguridad de la información, estos últimos correspondientes a:

- Minimizar el riesgo de los procesos misionales de la entidad.
- Prevenir el daño antijurídico.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de los funcionarios, contratistas y terceros.
- Apoyar la innovación tecnológica.
- Apoyar la interoperabilidad segura de la información entre entidades
- Implementar el sistema de gestión de seguridad de la información.
- Proteger los activos de información.
- Establecer los procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los servidores públicos, funcionarios, contratistas, estudiantes, pasantes, especialistas en entrenamiento, personal de proveedores, terceros y clientes del INC.
- Garantizar la continuidad del negocio frente a incidentes después de una interrupción no deseada o desastre.

ARTÍCULO 5. Principios rectores de seguridad de la información. A continuación, se establecen los 13 principios rectores de seguridad de la información que soportan el SGSI del Instituto Nacional de Cancerología E.S.E (INC):

1. Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, proveedores, socios de negocio o terceros.

2. El INC protegerá la información generada, procesada o resguardada por los procesos institucionales, su infraestructura tecnológica, activos de información, y activos del riesgo que se genera de los accesos otorgados a terceros (ej.: proveedores o clientes), o como resultado de un servicio interno en outsourcing.

3. El INC protegerá la información creada, procesada, transmitida o resguardada por sus procesos institucionales en físico y digital, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.

4. EL INC protegerá su información de las amenazas originadas por parte del personal, y estará preparado para reconocer ataques de ingeniería social.

5. EL INC protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.

6. EL INC protegerá la infraestructura que identifique como critica para la Ciberdefensa y Ciberseguridad del Estado Colombiano.

7. EL INC controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.

8. EL INC implementará control de acceso a la información, sistemas y recursos de red.

9. EL INC garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.

10. EL INC garantizará la protección de datos en la administración de esquemas de interoperabilidad de historia clínica.

11. EL INC garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.

12. EL INC garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basada en el impacto que pueden generar los eventos.

13. EL INC garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales relacionadas con Seguridad de la Información.

ARTÍCULO 6. Declaraciones de Seguridad de la Información. El INSTITUTO NACIONAL DE CANCEROLOGÍA E.S.E (INC) declara que:

- Es obligación de todos los servidores públicos, funcionarios, contratistas, estudiantes, pasantes, especialistas en entrenamiento, personal de proveedores, terceros y clientes adscritos al INC, cumplir con la Política de Seguridad y Privacidad de la Información, el Manual Interno de Seguridad y Privacidad de la Información, la política de Privacidad y Confidencialidad para el Tratamiento de Datos Personales, y propender por la integridad, disponibilidad y confidencialidad de la información del instituto, so pena de que la entidad tome las medidas disciplinarias, legales y administrativas correspondientes.

- El INC establece los roles y responsabilidades relacionados con la presente política de seguridad de la información en lo que tiene que ver con el gobierno, gestión, administración y operación en la seguridad de la información.

- El INC protege la información producida, custodiada y transmitida de forma adecuada en desarrollo de sus procesos misionales.

- Los grupos pertenecientes al estándar Gerencia de la Información son los encargados de diseñar e implementar un modelo de datos estratégicos para proteger la información generada, recolectada, procesada y utilizada para el cumplimiento de la misión el INC.

- El grupo Área Gestión Documental y Correspondencia es la facultada para establecer la política y los lineamientos para la identificación, caracterización, clasificación y buen uso de los activos de información física y electrónica, para su protección.

- El grupo área de Gestión Documental y Correspondencia, la oficina de Organización y Métodos, y el grupo Área Gestión TI lideran los ejercicios de levantamiento, la identificación y clasificación de los activos de información.

- El grupo Área Gestión TI suministra y gestiona las herramientas de hardware y software para el procesamiento y almacenamiento de la información y a su vez implementa controles para mitigar los riesgos sobre dicha información

- Los propietarios de la información son los responsables de los procesos institucionales y por ende de la información registrada, la autorización de cambios y la solicitud de modificaciones a realizar sobre los sistemas de información, o sobre los activos de información.

- Todas las dependencias del INSTITUTO NACIONAL DE CANCEROLOGÍA E.S.E que tienen a su cargo la custodia de la información generada en el marco de sus funciones, deben aplicar los controles correspondientes para protegerla, y deben mantener actualizado el inventario de activos de información relacionado con su servicio y funciones, esto, teniendo en cuenta la normatividad vigente para el efecto. Cada Grupo Area debe identificar y mantener actualizado su inventario de infraestructuras críticas, que pueda causar indisponibilidad de los servicios de la entidad.

- Los activos de información, equipos, bienes, aplicaciones, herramientas tecnológicas y servicios de tecnologías de la información y las comunicaciones, son para uso exclusivo del cumplimiento de las funciones y finalidades designadas al personal del INSTITUTO NACIONAL DE

CANCEROLOGÍA E.S.E; razón por la cual la información almacenada, procesada y generada a través de dichos activos, herramientas y dispositivos se considera propiedad de la entidad y el uso inadecuado de dichos recursos puede conllevar a sanciones disciplinarias y legales correspondientes.

- Todos los activos de información deben tener un responsable dentro del INC y deben estar debidamente identificados y clasificados, de conformidad con los procedimientos y formatos dispuestos para ello.

- Es responsabilidad los funcionarios, contratistas y terceros del INSTITUTO NACIONAL DE CANCEROLOGÍA E.S.E. realizar una copia de seguridad de los archivos más sensibles que se almacenan en los equipos de cómputo y servidores asignados; esta copia debe almacenarse en los medios designados por el INC tales como servidor de archivos, almacenamiento en la nube, carpetas compartidas, entre otros. Una vez finalizada la vinculación con la entidad se deberá entregar toda la información procesada dentro de los equipos a cargo al jefe inmediato o al supervisor de contrato.

- El Grupo Área Gestión TI lidera la planificación, establecimiento, implementación, operación, revisión y mantenimiento continuo de un plan de Recuperación ante Desastres Informáticos (DRP), que cubre los datos, el hardware y el software, para que las plataformas informáticas y tecnológicas criticas pueda comenzar de nuevo sus operaciones en caso de un desastre natural o causado por intervención humana.

- La oficina Asesora de Planeación liderará la planificación, establecimiento, implementación, operación, revisión y mantenimiento continuo de un Plan de Continuidad de Negocio, para prepararse, responder y recuperarse de incidentes que interrumpan los procesos críticos del INC, cuando éstos ocurren.

ARTÍCULO 7. Declaración de cumplimiento de la Política de Seguridad y Privacidad de la información. El INSTITUTO NACIONAL DE CANCEROLOGIA E.S.E garantizará la seguridad y privacidad de su información, realizando cumplimiento de la norma ISO27001:2013. Como consecuencia de lo anterior, tanto responsables como encargados, acogerán íntegramente esta política enmarcada dentro del sistema de Gestión de Seguridad de la Información (SGSI) de la entidad, junto con las obligaciones y procedimiento que de aquí se desprendan, velando por la implementación de la misma al interior de la entidad, divulgando su contenido y efectos entre su personal, es decir, entre sus subordinados o dependientes (operadores), y vigilando su cumplimiento. Todo ello, en garantía de la confidencialidad, integridad y privacidad de la información de acuerdo con las disposiciones legales anteriormente citadas.

Todos los usuarios identificados en las políticas, manuales, procedimientos o instructivos internos relacionados con la Política de Seguridad y Privacidad de la Información están obligados con el cumplimiento de las medidas de seguridad y controles establecidos en el INSTITUTO NACIONAL DE CANCEROLOGIA E.S.E, y están sujetos al deber de confidencialidad, incluso después de acabada su relación laboral o profesional con la institución o con el responsable del tratamiento.

CAPITULO 2

DESARROLLO DE LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

ARTICULO 8. (ANEXO A - A.6) Organización de Seguridad de la Información.

A.6.1 Organización interna

A.6.1.1 Roles y Responsabilidades de seguridad de la información. A continuación, se describen los principales roles y responsabilidades de los colaboradores frente de la política de seguridad y privacidad de la información y seguridad digital:

ROL	PARTICIPANTES	FUNCIONES

Comité Institucional de Gestión y desempeño y Equipo Técnico de Gestión y Desempeño con Valores para Resultados o quien haga sus veces	• El Subdirector General de la Gestión Administrativa y Financiera, quién lo presidirá. • El Asesor de la Oficina de Planeación y Sistemas, quién actuará como secretario del comité. • El Subdirector General de Atención Médica y Docencia, o su delegado • El Subdirector General de Investigación, Vigilancia Epidemiológica, Promoción y Prevención, o su delegado • El Asesor de Calidad • El Asesor de Comunicaciones • El Asesor Dirección General • El Coordinador Grupo Área de Gestión y Desarrollo del Talento Humano • El Coordinador Grupo Área Gestión de TI • El Coordinador Grupo Área Gestión Documental y Correspondencia • El Coordinador Grupo Gestión a Usuarios • El jefe de la Oficina de Control Interno será invitado permanente con voz, pero sin voto • El Oficial de seguridad de la información.(CISO)	• Fijar las acciones y estrategias orientadas al buen uso y aprovechamiento de las Tecnologías de Información y las Comunicaciones, así como la gestión y la protección de los activos de información de la Entidad. • Acoger las funciones de comité de seguridad de la información. • Uso y aprovechamiento de Tecnologías de Información y las Comunicaciones • Gestión y Protección de Activos de Información • Toma de sesiones sobre activaciones de contingencia y continuidad de negocio • Aprobar Planes y Programas relacionados con la seguridad de la información
Oficial de Seguridad de la información	• Oficial de Seguridad de la Información	• Definir, seguir y controlar la estrategia TI que permita lograr los objetivos y minimizar de los riesgos de seguridad digital de la institución. Es el encargado de guiar la prestación del servicio y la adquisición de bienes y servicios relacionados y requeridos para garantizar la seguridad de la información. • Verificar el cumplimiento de las obligaciones legales y regulatorias del estado relacionadas con la seguridad de la información. • Desarrollar y supervisar los resultados del plan de formación y sensibilización establecido para la entidad, con el fin de identificar oportunidades de mejora • Implementar el Sistema de Gestión Seguridad de la Información, mediante el plan de seguridad y privacidad de la información • Liderar el proceso de gestión de incidentes de seguridad, así como la posterior investigación de dichos eventos para determinar causas, posibles responsables y recomendaciones de mejora para los sistemas afectados, ayudando con las cuestiones disciplinarias y legales necesarias. • Vigilar por el mantenimiento y actualización de la documentación del Sistema de Gestión de Seguridad y de la información, su custodia y protección. • Liderar la gestión de Ciberdefensa y Ciberseguridad del instituto para la protección de infraestructura critica. • Liderar procesos de Habeas data y confidencialidad en el INC • Trabajar con la alta dirección y los dueños de los procesos misionales dentro de la entidad en el desarrollo de los planes de recuperación de desastres, y apoyar la ejecución de los planes de continuidad del negocio. • Realizar y/o supervisar pruebas de vulnerabilidad sobre los diferentes recursos tecnológicos para detectar vulnerabilidades y oportunidades de mejora a nivel de seguridad de la información
Administradores de seguridad informática	• Administrador de seguridad informática • Administrador De Servidores	• Administración y Monitoreo de plataformas y controles de seguridad de la información. • Garantizar una adecuada identificación, gestión y tratamiento de las vulnerabilidades técnicas identificadas en los sistemas administrados, e

		infraestructura en general. • Ejecución de proyectos de seguridad informática • Resolución técnica de incidentes de seguridad informática. • Responsable de Ejecución y pruebas de backup para plataformas administradas. • Hardening de equipos y sistemas administrados. • Implantar medidas de sanidad informática. • Liderar planes de contingencia de Outsourcing de TI de sistemas administrados • Realizar capacitación a usuario final y mesa de ayuda sobre seguridad informática. • Mantener documentación actualizada de plataformas y controles de seguridad
Administradores de Plataformas Tecnológicas	• Administradores plataformas y sistemas de información INC • Administradores de bases de Datos. • Administradores de plataformas de correo e ofimática • Administradores de plataformas y sistemas de información Outsourcing • Administradores de plataformas y sistemas de información Proveedores y terceros • Administradores de plataformas y sistemas de información sistemas y servicios Cloud	• Implementar el conjunto de políticas de control de acceso y los controles de seguridad para asignar los privilegios adecuados a los usuarios • Implementar y Garantizar la separación de los ambientes de desarrollo, pruebas y producción. • Implementar y mantener la Gestión de cambio dentro de un marco de trabajo desarrollo seguro • Responsables de ejecución y pruebas de backup en sus respectivas plataformas. • Seleccionar, proteger y controlar cuidadosamente los datos de prueba • Garantizar una óptima respuesta a los incidentes de seguridad de la información • Garantizar la revisión periódica de los sistemas de información para verificar el cumplimiento de políticas y normas de seguridad informática. • Ejecutar periódicamente pruebas de continuidad en sus plataformas. • Implantar y mantener una adecuada protección a los equipos de usuarios desatendidos. • Implementar medidas de higiene de seguridad informática en los sistemas y plataformas administrados. • Implementar y mantener trazabilidad de eventos para evitar el repudio de las acciones efectuadas dentro de las plataformas administradas. • Implementar controles criptográficos en las comunicaciones y transferencias de información.
Oficina de Control Interno	• Profesionales delegados del área	Llevar las auditorías periódicas (mínimo anualmente) a los sistemas y actividades relacionadas a la gestión de activos de información de acuerdo con la normatividad vigente.
Equipo del Proyecto implementación SGSI	• Profesionales delegados de las áreas del Comité de Seguridad de la Información • Responsable del tratamiento de los datos personales	• Apoyar al Oficial de Seguridad al interior de la entidad, de acuerdo a los cronogramas establecidos. • Coordinar la interacción con consultores externos • Analizar el riesgo de los activos de información del INC y verificar la aplicación de las medidas de seguridad necesarias para la protección de la misma. • Oficiar como consultores de primer nivel en cuanto a las dudas técnicas y de procedimiento que se puedan suscitar en el desarrollo del proyecto. • Tomar las decisiones sobre las bases de datos personales a que hubiere lugar y direccionar las actividades de los encargados de los datos personales • Generación, revisión, aprobación, seguimiento, apoyo y/o plan de mejora para el cambio de protocolo IPV4 a

		IPV6 • Correr Autodiagnósticos del MPSI. iSO27001 y seguridad digital • Apoyar con el desarrollo de la documentación de seguridad. • Apoyar en las diversas actividades relacionadas que determine MINTIC en cuando al cumplimiento de MSPI
Lideres del proceso	• Persona nombrada que ejerce como responsable de un proceso de la organización y/o aplicación especializada relacionada	• Actúa como el "administrador del activo de información" para todos los aspectos de seguridad de la información relacionados con el procesamiento de datos dentro de este proceso particular de la institución. • Clasificar los activos de información de su proceso, de acuerdo con el grado de sensibilidad y criticidad de la misma, documentar y mantener actualizada la clasificación efectuada, y definir qué usuarios deberán tener permisos de acceso a la información de acuerdo a sus funciones y competencia • Vigilar el cumplimiento de los controles de seguridad identificados para su área encargada.
Usuarios de la Entidad	• Toda persona con vínculo contractual con la Entidad • Personal outsourcing de terceros con contrato con la Entidad • Ciudadanos que requieren de los servicios de la Entidad	Conocer y dar a conocer, cumplir y hacer cumplir la Política de Seguridad de la Información vigente
Entidades Externas	• Alta Consejería de las Tics MINTIC • Ministerio de Salud y protección social • CCIRT Gobierno • CCOCI Fuerzas Militares • Otros	• Brindar asesoría y generar convenios con el instituto, sobre seguridad de la información. • Compartir experiencia y conocimiento • Construir y extender directrices sobre la gestión de la seguridad en el sector.

A.6.1.2 Separación de deberes. Los administradores de plataformas, sistemas de información y bases de datos del INC deben tener asignados únicamente los roles necesarios para ejecutar su labor. Los usuarios con permisos de administración total de las diferentes plataformas no deberían utilizarse para realizar la administración diaria de los servicios.

A.6.1.3 Contacto con las Autoridades. El instituto mantiene contactos con las siguientes autoridades de Seguridad de la información: CSIRT Gobierno, CSIRT Policía nacional, Comando conjunto Cibernético de las Fuerzas militares, Fiscalía General de la Nación.

A.6.1.4 Contacto con Grupos de interés especial: El instituto mantiene contactos con los siguientes grupos de interés especial : Grupo Ciberdefensa y Ciberseguridad Ministerio de salud y protección Social, CSIRT, Superintendencia de Industria y Comercio SIC, Certicamara , Microsoft, MINTIC, Grupos de soporte de fabricantes de Antivirus y FWNG.

A.6.2 Política para dispositivos móviles, trabajo remoto y en casa

A.6.2.1 Política para dispositivos móviles. Los dispositivos móviles de propiedad de la institución asignados para uso laboral del personal deben ser protegidos con, un antivirus, un aplicativo o sistema de bloqueo automático, y el almacenamiento debe ser cifrado antes del primer uso. El almacenamiento de dispositivos móviles se debe tratar como lo indica el numeral " *A.8.3. Manejo de medios de soporte removibles"* de la presente política.

Los dispositivos móviles de propiedad personal deben cumplir con la política BYOT (Uso de dispositivos de tecnología de propiedad personal en el trabajo) relacionada en el numeral "*A.8.1.3. Uso aceptable de los activos.*"

A.6.2.2 Trabajo remoto y en casa. El trabajo en casa por defecto no se encuentra autorizado para los trabajadores del INSTITUTO NACIONAL DE CANCEROLOGÍA E.S.E. Sin embargo, de conformidad con lo dispuesto en el inciso segundo de su artículo 2 del Decreto 884 de 2012, si debido a una contingencia se requiere una conexión remota a los sistemas del INC en un lugar distinto a las sedes de la entidad, el instituto debe implementar una manual para trabajo remoto o en casa y unas medidas de seguridad, para garantizar el acceso a los sistemas y servicios de la institución y proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza trabajo remoto o en casa.

El trabajo remoto o en casa durante periodos de contingencia se autoriza únicamente en equipos y dispositivos portátiles de propiedad del INC. No se permite trabajo remoto o en casa realizando uso de herramientas de conexión remota o equipos de propiedad personal, con la excepción de las herramientas y aplicativos que el INC publique o autorice en su Portal VPN WEB. Si el trabajador no tiene asignado equipo portátil o dispositivo propiedad del INC, es necesario que el INC le suministre, mientras se tengan existencias, el correspondiente equipo a través del cual el mismo prestara sus servicios a la Entidad desde su residencia o el lugar que se escoja y determine para tal fin.

Únicamente los subdirectores generales pueden aprobar solicitudes de trabajo remoto y en casa, con la firma previa de acuerdo de confidencialidad GTI-P01-F-18 que se encuentra registrado en Siapinc, por parte del trabajador remoto o en casa.

ARTÍCULO 9. (ANEXO A - A.7) Seguridad de los Recursos Humanos. El INSTITUTO NACIONAL DE CANCEROLOGÍA E.S.E. es responsable de divulgar y garantizar el cumplimiento y aplicación de la Política de Seguridad y Privacidad de la Información a todo el personal que se vincule a la entidad.

Por lo tanto, el INC en la gestión de su talento humano debe:

- Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran incluyendo sus responsabilidades con la seguridad de la información.
- Exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos en el INC.
- Asegurarse de que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan.
- Contar con un proceso formal y comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.
- Asegurarse que una vez el funcionario o contratista cese en sus funciones o culmine la ejecución de un contrato en el INC, el jefe inmediato o supervisor recepcione y custodie los activos de información, y sean retirados oportunamente todos los permisos y cuentas que tenía el funcionario o contratista.
- Garantizar que las responsabilidades y los deberes de seguridad de la información permanezcan válidos y se cumplan después de la terminación o cambio de empleo de los funcionarios o contratistas.

A.7.1 Antes de asumir el empleo

A.7.1.1 Verificación de Antecedentes: El Grupo Area de Gestión de Talento Humano debe garantizar que se realicen las verificaciones de los antecedentes de todos los candidatos a un empleo, la cuales se deben llevar a cabo de acuerdo con las leyes, reglamentos y ética pertinentes, y deben ser proporcionales a los requisitos de la operación, a la clasificación de la información a que se va a tener acceso, y a los riesgos percibidos

A.7.1.2 Términos y condiciones de Empleo: El Grupo Área Gestión de Compras y Contratación y el grupo área Gestión Estudios Previos y supervisión deben realizar las tareas pertinentes para que todos los contratos de prestación de servicios incorporen las obligaciones correspondientes a exigir el cumplimiento de la Política de Seguridad y Privacidad de la Información, el manejo confidencial de la información, la protección de derechos de autor y la protección de datos personales.

A.7.2 Durante la ejecución del empleo. El INC debe Asegurarse de que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan. Para esto se establecen los siguientes lineamientos:

A.7.2.1 Responsabilidades de la dirección. La Dirección del Instituto exige a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos de la entidad. La oficina de Gestión TI cuenta con el compromiso de la Alta Dirección del INC para el correcto desempeño del sistema de gestión de seguridad de la información (SGSI).

Para ello, la dirección lleva a cabo las siguientes actividades:

- Garantizar el cumplimiento de planes y objetivos de Sistema de Gestión de Seguridad de la Información.
- Aprobar la política de seguridad de la información y Política de Manejo de datos personales.
- Aprobar roles y responsabilidades de seguridad de la información, y aprobar asignación de funciones de comité de seguridad de la información al comité de MIPG
- Informar a la empresa la importancia de alcanzar los objetivos de seguridad de la información y de cumplir con la política de seguridad.
- Designar todos los recursos necesarios para llevar a cabo el SGSI.
- Investir de mando suficiente al personal de seguridad de la información para garantizar el cumplimento de las políticas, planes, procedimientos y manuales del SGSI
- Revisar y aprobar todos los criterios de aceptación de riesgos de seguridad digital y sus correspondientes niveles.
- Aprobar el presupuesto suficiente para todas las fases del SGSI, implantación de controles, y la mejora continua determinada por la Gestión de riesgos de seguridad digital.
- Aprobar los recursos para que se realicen las auditorías sobre la Norma Iso27001:2013 y manejo de datos personales
- Llevar a cabo revisiones periódicas del SGSI.

A.7.2.2 Toma de conciencia, educación y formación en la seguridad de la información: Los Grupos Area Gestión y Desarrollo de Talento Humano y Grupo Area Gestión TI deben asegurarse que todos los empleados de la organización, funcionaros, contratistas, docentes, estudiantes y personal de proveedores y terceros, reciban la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos necesarios para su cargo o desempeño de su funciones dentro de la entidad. Para esto el instituto cuenta con un plan de capacitación y sensibilización en seguridad de la información el cual se revisar y ejecutar anualmente de acuerdo con las necesidades de capacitación identificadas en el periodo anterior.

Todo el personal del INC debe participar de las actividades de capacitación y sensibilización sobre la seguridad de la información y de gestión de riesgo, y debe estar en la capacidad de identificar y reaccionar adecuadamente ante las continuas amenazas y vulnerabilidades que ponen en riesgo la información del instituto.

A.7.2.3 Proceso disciplinario: El INC en cabeza del Grupo Asesor de Control Interno Disciplinario cuenta con un proceso formal y comunicado, para emprender acciones contra funcionarios que hayan cometido una violación a la seguridad de la información

La Ley 734 de 2002 y la ley 1952 de 2019 rigen el Derecho Disciplinario. En ellas se señala que todas las Entidades del Estado tienen un área jurídica que realiza las investigaciones disciplinarias correspondientes a las faltas cometidas por los funcionarios públicos. Y la Procuraduría General de la Nación y las Personerías Distritales y Municipales tienen la potestad del poder preferente para llevar un control interno del funcionario público que haga u omita una función que corresponda a su cargo, incluyendo el incumplimiento de las políticas relacionadas con seguridad de la información y tratamiento de datos personales.

Las acciones por incumplimiento de los requerimientos de seguridad de la Información por parte de contratistas y personal de proveedores y terceros del INC se rigen por medio de La Ley 80 de 1993, la cual aclara que el Contratista debe responder civil y penalmente por el contrato realizado.

Si el contrato o labor se trata de la vigilancia de un contrato (INTERVENTOR), el particular se ve enfrentado disciplinariamente, por el hecho, a su vez, de ejercer una función pública.

A.7.3 Terminación y cambio de empleo. El Grupo Area de Gestión de Talento Humano se encarga proteger los intereses de la organización como parte del proceso de cambio o terminación de empleo. Para esto debe tener en cuenta:

A.7.3.1 Terminación o cambio de responsabilidades de empleo. Las responsabilidades y los deberes de seguridad de la información que permanecen válidos después de la terminación o cambio de empleo se deben definir, comunicar al empleado o contratista y se deben hacer cumplir.

ARTÍCULO 10 (ANEXO A – A.8) Gestión de los Activos de Información. El INC a través del Grupo de Gerencia de la Información, el Grupo Área Gestión Documental y Correspondencia y el Grupo Área Gestión TI, debe establecer y divulgar los lineamientos específicos para la identificación, clasificación y buen uso de los activos de información en físico y digital, con el objetivo de garantizar su protección.

A.8.1 Responsabilidad por los activos. El INC Identifica los activos organizacionales y define las responsabilidades de protección apropiadas así:

A.8.1.1 Inventario de activos de información: Los activos de Información del INC deben ser identificados, clasificados y controlados para garantizar su uso adecuado, protección y la recuperación ante cualquier desastre. La oficina de Organización y Métodos, el grupo Area Gestión Documental y el responsable de Seguridad de la información se encargan del el diseño y la programación del ejercicio de recolección inventarios de activos de información que se debe realizar de manera anual. La consolidación de dicho inventario está bajo la responsabilidad de la Oficina de Organización y Métodos.

Los coordinadores de Grupos Area y líderes de Oficinas son responsables del reporte, registro y clasificación de los inventarios de activos a su cargo

A.8.1.2 Propiedad de los activos de información. La responsabilidad de la administración, gestión, y cumplimiento de controles de los activos de información está en cabeza del propietario registrado en el inventario de activos. Los propietarios de la información deben propender para que los custodios mantengan actualizado el inventario de sus activos de información y hagan entrega de éste al menos una vez por año.

Con el objeto de implementar los controles de seguridad, las dependencias que tienen la custodia de la información en el marco de su función se encargaran de ubicar, clasificar y marcar la información con la estructura y los metadatos requeridos para el correcto funcionamiento de las herramientas de seguridad y de Gestión Documental del INC.

Todos los contratos, convenios, y contratos laborales que se establezcan en el INC deben contener clausulas establecer la propiedad de la información del INC durante la ejecución de las labores.

A.8.1.3 Uso aceptable de los activos de información. Los recursos tecnológicos al igual que los archivos, documentos, carpetas, sistemas de información, correo electrónico, plataformas tecnológicas, instalaciones de procesamiento de información, bases de datos estructuradas e intermedias, aplicaciones, carnets y tarjetas de identificación, tokens entre otros, son activos de información que pertenecen al INC. El uso de estos activos de información es exclusivamente institucional, y es responsabilidad de aquel a quien se asigne o corresponda el propender por su confidencialidad, integridad, disponibilidad, privacidad y buen uso.

A continuación, se identifican, documentan e implementan reglas para el uso aceptable de información y de activos asociados con:

Correo Electrónico. El correo electrónico institucional asignado es un servicio para la comunicación colaboración de los funcionarios y contratistas del INC; es de uso personal e intransferible y debe utilizarse responsablemente cumpliendo como mínimo con los siguientes lineamientos:

El correo electrónico asignado debe ser para uso única y exclusivamente institucional y no podrá ser utilizado para fines personales económicos, comerciales propaganda, campañas, cadenas, chistes, invitaciones y cualquier otro ajeno a los propósitos o finalidades del INC.

Las cuentas de correo electrónico se asignarán únicamente de acuerdo con la nomenclatura definida por el Grupo Área Gestión TI.

La cuenta de correo es personal e intransferible, por lo tanto, cada usuario es responsable de la información enviada o reenviada desde su cuenta de correo.

Está expresamente prohibido distribuir a través del correo electrónico información del INC que no sea considerada de uso público a otras entidades o ciudadanos, sin la debida autorización de dueño del activo de información. Para esto el INC establecerá controles para restringir la circulación de información confidencial únicamente con aprobación previa del responsable de dichos activos, a través correo electrónico.

El correo electrónico autorizado para el manejo de la información institucional es el asignado con el dominio "@cancer.gov.co" pues este cumple con los parámetros de seguridad y requerimientos de ley para tal fin. Los proveedores, únicamente con previa autorización podrán usar su propio sistema de correo si así lo determina el tipo de contrato, pero deben acogerse a todas las políticas, controles, monitoreo, y requerimientos de seguridad para el buen uso de correo electrónico del INC, registrado en el manual de BYOT (Traiga su propia tecnología) y en la presente política.

A través del correo electrónico está prohibido enviar información o material que posea contenidos falsos, que causen alarma o pánico, que pretendan fines de terrorismo o asonada, que vaya en contra de la ley o que constituya o fomente un comportamiento que dé lugar a responsabilidades civiles, administrativas o penales.

Está prohibido el envío de correos masivos (más de 100 destinatarios) tanto internos como externos, salvo a través de los correos oficiales para comunicaciones masivas que administra la mesa de ayuda (comunicaciones@cancer.gov.co y circulares@cancer.gov.co), o que dichos envíos sean autorizados mediante control de cambios por los Subdirectores Generales o la Dirección General.

Los correos electrónicos catalogados como tipo SPAM (Cadenas de correos o correos dirigidos masivamente a diferentes destinatarios) o correos sospechosos, se deberán reportar al Grupo Área Gestión TI a través de la mesa de ayuda y serán tratados como incidentes de seguridad de la información. No está permitido el envío o reenvío de ningún tipo de SPAM o publicidad no autorizada en el INC.

Pese a que la entidad cuenta con un servicio de antivirus y antispam para la revisión de los mensajes de correo electrónico entrante, los usuarios del correo deben ser cuidadosos cuando decidan abrir los archivos anexos colocados en mensajes de remitentes desconocidos o sospechosos. Debe informarse al Grupo Área Gestión TI para tratar estos casos como incidentes de seguridad.

La cuenta de correo institucional no podrá ser utilizada para el registro o autenticación, en páginas o sitios publicitarios, de comercio electrónico, deportivos, redes sociales, casinos, concursos, sitios de citas o cualquier otro portal ajeno a las funciones que le correspondan en el INC.

Está expresamente prohibido el uso del correo para el envío de contenidos insultantes, ofensivos, injuriosos, obscenos, discriminatorios, violatorios de los derechos fundamentales, derechos de autor o que atenten contra la integridad moral de las personas.

No se permite el uso de correo electrónico para descargar o instalar programas o software para instalar en el equipo.

Para el envío de ficheros de gran tamaño, se debe hacer uso del Servicio Institucional de nube privada y de centro para el trabajo en equipo de office 365, que permite compartir ficheros grandes mediante envío de link. El uso de nubes privadas y servicios gratuitos de transferencia de archivos queda restringido para uso en el INC, con las excepciones que únicamente determinen los Subdirectores Generales mediante control de cambio.

Es obligatorio enviar un correo con una dirección de retorno válida y propia del sistema a través del cual se está enviando el correo. No se podrá usar como remitente direcciones externas de otros proveedores (del tipo @gmail.com, @hotmail.com, etc.) enmascaradas con el domino del INC

Todo usuario del correo electrónico está obligado a identificarse correctamente en sus comunicaciones vía correo electrónico, dando uso obligatorio a la firma de correo institucional y el aviso de privacidad para comunicaciones electrónicas del INC. No se permite modificar la firma de correo institucional con imágenes, texturas, diseños propios, la cual debe estar conforme al manual de Imagen corporativa institucional, que cuenta con la aprobación de la Oficina de Comunicaciones del INC.

Internet. Si bien el grupo Area Gestión de TI establece controles a la navegación de acuerdo con las políticas y perfiles establecidos, es responsabilidad de todos los funcionarios y contratistas del INC hacer un uso responsable del Internet y cumplir con las políticas para tal fin aquí determinadas:

La Dirección y Subdirecciones Generales del INC, en conjunto con el Grupo Área Gestión TI y la Oficina de Comunicaciones definen las políticas, restricciones de acceso, ancho de banda máximo a utilizar horarios, derechos de descarga de archivos, permisos de navegación y demás relacionados, para garantizar el uso eficiente, racional y seguro del Internet.

El INC se reserva el derecho de monitorear el uso de Internet con motivos de calidad del servicio, hacer seguimiento y auditoría al uso que los usuarios le den a este servicio, y para verificar que se haga un uso responsable y racional de dicho recurso. A través de herramientas de monitoreo y análisis de tráfico y amenazas, se detectará, reportará y bloqueará a los usuarios que hagan mal uso de los servicios de Internet.

El uso del Internet deberá ajustarse a las necesidades de la función u obligaciones contractuales dentro del marco institucional y se prohíbe expresamente el acceso o consulta de páginas Web con contenido insultante, ofensivo, injurioso, discriminatorio, obsceno, pornográfico, violatorio de los derechos de autor y propiedad intelectual.

El INC restringirá la descarga y reproducción de música y video, así como utilizar el acceso a internet para participar en juegos de entretenimiento en línea, redes sociales no autorizadas y demás que afecten o sean elementos distractores de las labores diarias, salvo que dichas aplicaciones se requieran para el ejercicio de las funciones a cargo.

El INC restringirá el uso de los servicios de Radio y TV a través de Internet, salvo que dichas aplicaciones se requieran para el ejercicio de las funciones a cargo y aquellas que determine la Oficina de Comunicaciones del INC.

El acceso a sitios Web o la instalación de aplicaciones, redes, y utilidades para intentar evadir los controles y políticas de seguridad de navegación, está totalmente prohibidos y su detección será tratada como un incidente de seguridad. La evidencia de dichas acciones será reportada a la Subdirección General Correspondiente y al grupo Área Gestión y Desarrollo del Talento Humano para iniciar con la investigación y sanciones a las que tenga lugar.

El descargar software y archivos provenientes de Internet cuya fuente no sea confiable, o que infrinja las protecciones y términos de uso determinados por sus autores o desarrolladores, implica un riesgo para la seguridad de la información, así como un riesgo de infracción al régimen legal de derechos de autor y Copyright. El INC restringirá las descargas y sitios potencialmente peligrosos o reportados como infractores de derechos de autor, y establecerá controles para evitar instalaciones sin autorización en los equipos del instituto. Cualquier instalación de software debe ser acompañada y controlada por la mesa de ayuda.

Equipos de cómputo y dispositivos tecnológicos. El INC podrá hacer entrega a funcionarios y contratistas de servidores, computadores de escritorio, workstation, portátiles, Tablet, celulares y smartphones, teléfonos IP, scanners, impresoras, equipos y sistemas biomédicos, y demás tipo de periféricos para el desarrollo de sus labores; el manejo de dichos equipos por parte de éstos conlleva responsabilidades y deben ajustarse a las siguientes directrices generales:

La nomenclatura de nombres de los equipos y dispositivos determinada por el Grupo Área Gestión TI debe se implantada de forma obligatoria a todos los equipos de propiedad o uso en el instituto, para poder ser identificados plenamente antes de cualquier conexión a las redes de datos del INC.

En todos los equipos y dispositivos se deben activar sistemas protección por usuario y clave de acceso, para evitar acceso no autorizados a los mismos.

El usuario debe verificar el bloqueo de sus equipos o dispositivos a cargo, cada vez que tenga que retirarse de su puesto de trabajo, o cuando estos queden desatendidos. El grupo Área Gestión TI debe establecer de forma obligatoria el bloqueo automático de los equipos al no detectar actividad en el mismo. Está prohibido el uso de fondos y protectores de pantalla diferentes a los definidos institucionalmente.

Los equipos y dispositivos asignados a los usuarios del INC solo podrán usarse para fines laborales relacionados con las funciones y obligaciones designadas, razón por la cual no hay autorización de instalar software diferente al autorizado por el Grupo Área Gestión TI. Está prohibido usar versiones de licencias de software tipo hogar, o de propiedad personal de los usuarios en los equipos asignados por el instituto. Se debe siempre constatar la necesidad de su uso, y que el Grupo Área Gestión TI autorice y/o cuente con el respectivo licenciamiento.

La instalación y uso de software libre, servicios gratuitos en la nube o tipo Opensourse debe ser evaluado y autorizado previamente por el grupo área Gestión TI. Al tratarse de software desarrollado por terceros, el Grupo Área Gestión TI no puede dar ninguna garantía de su funcionamiento o de la información que allí se procesa, por lo que su uso debe respaldarse con el establecimiento de backups periódicos y contratos de soporte. Está prohibido el uso de software libre o tipo opensource sin contrato de soporte especializado para manejar datos confidenciales o información sensible del INC.

Los equipos y dispositivos de cómputo y móviles que sean asignados a los funcionarios y contratistas serán para uso institucional exclusivamente, de carácter intransferible, y la responsabilidad de su uso seguro dentro y fuera del INC recaerá sobre la persona a la que le fue asignado.

Teniendo en cuenta que los equipos y dispositivos son para uso exclusivamente institucional, el INC se reserva el derecho de monitorear el contenido y software instalado en los equipos de la entidad para verificar el tipo de información, su uso y licenciamiento del software instalado. De esta manera contenidos de música, video, fotos, archivos de propiedad personal, o demás que no correspondan al desempeño de las funciones u obligaciones contractuales respectivas del funcionario o contratista podrían ser accesados y borrados sin previa consulta, y sin ningún tipo responsabilidad o compromiso del INC.

Los únicos autorizados para realizar cambio de partes, actualizaciones destapar, desconectar, retirar, y/o reparar equipos, son los técnicos de mesa de ayuda del INC, y personal debidamente autorizado de los grupos áreas de Gestión TI y Gestión de Infraestructura e ingeniería Clínica, previa solicitud a través de la mesa de servicio.

Es responsabilidad de los funcionarios y contratistas del INC mantener organizada y clasificada su información, y almacenarla en las respectivas ubicaciones del equipo o dispositivo donde determine el Grupo Área Gestión TI para la realización de copias de seguridad de la información. Está prohibido realizar copias de seguridad de equipos/dispositivos en medios extraíbles que no sean de propiedad del INC

Está prohibido fumar, ingerir alimentos o bebidas en el área de trabajo donde se encuentren equipos y dispositivos electrónico, en especial aquellos de uso hospitalario.

El Grupo Área de Gestión TI en cabeza del equipo de mesa de ayuda deberá aprovisionar los computadores antes de ser entregados garantizando que:

- El software instalado sea el software base definido por el Grupo Área de Gestión TI y cuente con el respectivo licenciamiento.

- Los sistemas operativos y demás aplicativos tengan instaladas las últimas actualizaciones liberadas a la fecha de entrega del equipo.

- El antivirus que determine el instituto de instalarse en los equipos y dispositivos sin excepción; debe estar siempre operativo, debe poder ser actualizado y administrado desde la consola centralizada. Los administradores de sistemas, aplicativos y plataformas deberán acordar y probar con el INC las exclusiones necesarias para permitir la ejecución del antivirus en sus equipos y dispositivos sin afectar el correcto funcionamiento de sus plataformas. En caso de no poder ejecutar el antivirus, los equipos y dispositivos procederán a ser aislados en redes de cuarentena y no podrán consumir servicios de las demás redes del INC.

- Los equipos deberán quedar apagados cuando el funcionario o contratista finalice su jornada laboral, por motivos de seguridad y ahorro de energía.

- Los equipos antes de ser reutilizados o retirados del INC serán formateados con un software de borrado seguro especializado usando un algoritmo DOD-5220 con mínimo 3 pasadas, para que la información de los anteriores usuarios no sea recuperable o accesible. Los equipos que contengan información sensible o confidencial del INC deben ser borrados con un algoritmo DOD-5220 o SCHNEIER de mínimo 7 pasadas. También es válido realizar borrado seguro utilizando hardware especializado para tal fin.

El grupo área de Gestión TI debe implementar servidores para las pruebas, distribución y despliegue de actualizaciones y parches de seguridad, y diseñar estrategias que permitan mantener actualizada toda la plataforma computacional de INC. Los responsables de aplicaciones o sistemas que no permitan la instalación de los últimos parches en los equipos deben documentar y ejecutar su propia estrategia de pruebas y aplicación de parches para sus sistemas administrados, entregando la evidencia correspondiente en los informes mensuales de supervisión de contrato. En caso de no poder ejecutar las actualizaciones, los equipos procederán a ser aislados en redes de cuarentena y no podrán consumir servicios de las demás redes del INC.

BYOT (Uso de dispositivos de tecnología de propiedad personal). El INC debe instaurar un manual de BYOT - USO DE DISPOSITIVOS DE TECNOLOGIA DE PROPIEDAD PERSONAL EN EL TRABAJO, para establecer las responsabilidades, principios, criterios, directrices y conductas dentro de los lineamientos de ética, técnicos y el buen gobierno para el uso controlado de tecnologías ajenas a la propiedad del INC para uso laboral o institucional, que minimice el riesgo de pérdida de datos, accesos no autorizados, divulgación no controlada, duplicación e interrupción intencional de la información.

Por defecto, el uso de los dispositivos de propiedad personal dentro de las redes corporativas del INC no está autorizado. El paciente, ciudadano y comunidad en general podrá realizar uso gratuito de conexión a internet por medio de las redes WIFI (inalámbricas) destinadas para conexión abierta (Internet para la gente).

El uso de dispositivos BYOT de propiedad personal o de terceros y proveedores para fines laborales, debe ser autorizado por el Coordinador de Grupo Area correspondiente, y requiriendo la verificación de la firma del acuerdo de confidencialidad institucional. La conexión de estos dispositivos o recursos se permitirá únicamente en redes inalámbricas aisladas para personas, proveedores, terceros o visitantes según corresponda, con acceso a internet y sin contar con acceso a los recursos servicios y equipos corporativos del INC. Para este caso, cualquier conexión a los recursos y servicios corporativos del INC debe realizarse a través de la VPN corporativa previamente autorizada por el Subdirector General correspondiente.

El Grupo Área TI del INC en cualquier caso se reserva del derecho de:

- Denegar o cancelar la solicitud BYOT por incumplimiento de requerimientos técnicos mínimos y de seguridad para la operación en las redes del INC.
- Denegar o cancelar la solicitud BYOT por incumplimiento, y/o el manejo no seguro de la información del instituto.
- Detección de virus, amenazas y/o vulnerabilidades en el dispositivo.
- Mantener en todo momento el monitoreo sobre el uso de estos dispositivos y sobre la información del INC.

En todo caso los responsables de estos estos dispositivos y tecnologías BYOT deben proteger los datos corporativos en la misma medida que en la operación Biomédica, Hospitalaria y de TI corporativa del INC, y deben cumplir con las políticas y controles de seguridad de la información, privacidad, licenciamiento y normatividad del Instituto, sin introducir riesgos inaceptables.

A.8.1.4 Devolución de los activos de información. Todos los empleados y usuarios de partes externas deben devolver todos los activos de información en físico y electrónico, que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo con el INC.

De acuerdo Articulo 15 de la Ley 594 de 2000 "Los servidores públicos, al desvincularse de las funciones titulares, entregarán los documentos y archivos a su cargo debidamente inventariado, conforme a /as normas y procedimientos que establezca el Archivo General de la Nación, sin que ello implique exoneración de la responsabilidad a que haya lugar en caso de irregularidades".

A.8.2 Clasificación de la información: El INC asegura que la organización recibe un nivel apropiado de protección, de acuerdo con su importancia para la organización como se describe a continuación.

A.8.2.1 Clasificación. Los coordinadores y líderes de grupos área y oficinas asesoras deben garantizar que todo el personal del INC clasifique la información en función de los requisitos legales, valor, criticidad, confiabilidad, manejo de datos personales y susceptibilidad a divulgación o a modificación no autorizada entre otros.

La clasificación de la información se debe realizar con base en la ley 1712 de 2014 reglamentada por el Capítulo 2 del Título 1 de la Parte 1 del Decreto 1081 de 2015, la ley 594 de 2000 (Ley General de Archivos), y Clasificación según Ley 1581 de 2012 (Habeas Data).

Los propietarios de los activos de información deben reportar y documentar la clasificación de seguridad de los activos de los que son responsables a la Oficina de Organización y Métodos, y asignaran un custodio para cada activo de información; a su vez éste custodio será responsable del cumplimiento de los diferentes controles y protocolos de seguridad que se implementen sobre dichos activos.

A.8.2.2 Etiquetado. El Grupo Área de Gestión Documental y Correspondencia debe desarrollar, implementar y garantizar el cumplimiento de un conjunto apropiado de procedimientos para el etiquetado de la información en físico y electrónico, de acuerdo con el esquema de clasificación de información adoptado en el INC. Igualmente debe mantener un índice actualizado de los actos, documentos e informaciones calificados como clasificados o reservados, incluyendo la denominación, motivación e individualización de su calificación.

El Grupo Área de Gestión TI debe acoger e implantar las directrices de etiquetado de información dentro de los sistemas de información y repositorios de archivos del instituto, e implementar los controles necesarios para garantizar la fuga de información marcada como confidencial o sensible.

A.8.2.3 Manejo de activos. El INC a través del Grupo de Gerencia de la Información, debe establecer y divulgar los lineamientos específicos para establecer uso permitidos y finalidades de los activos de información en físico y digital, con el objetivo de garantizar su conservación y salvaguarda.

El Grupo Área de Gestión Documental y Correspondencia, el Grupo de Organización y Métodos, y el Grupo Area Gestión TI deben desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por el instituto.

A.8.3 Manejo de medios de soporte removibles

A.8.3.1 Gestión de medios de soporte y almacenamiento removibles. El INC debe prevenir la divulgación, la modificación, el retiro o la destrucción de información almacenada en medios de soporte removibles.

Para esto, el INC debe implementar controles DLP para restringir la gestión de medios de soporte removibles, (Memorias USB, tarjetas de memoria, discos duros externos, unidades de CD/DVD-RW, Unidad de disco magneto-óptico, unidades de estado sólido, unidades de almacenamiento en cinta, almacenamiento en dispositivos celulares, tablets, móviles, reproductores de música, wereables, unidades y sistemas de recuperación de datos, etc.), de acuerdo con el esquema de clasificación de activos de información adoptado por la entidad.

Los medios de soportes removibles de propiedad del INC asignados a los usuarios son de uso personal e intransferible, y solo podrán usarse para portar y desplegar información en los equipos de propiedad del INC. Estos medios de soporte removibles no servirán para transportar información a equipos personales o equipos de propiedad externa al instituto.

Se prohíbe el uso de medios de soporte removibles de propiedad personal de los servidores públicos, contratistas, estudiantes, pasantes, especialistas en entrenamiento, terceros y personal externo del INC. Por defecto los puertos USB y puertos de los equipos de cómputo y portátiles

serán bloqueados para uso de medios de soporte removibles. La habilitación de uso puertos USB para dispositivos de soporte removible de propiedad personal requiere la firma de un contrato de aceptación de trasferencia de riesgo y revisión y firma de acuerdo de confidencialidad adicional aprobado por el Subdirector General correspondiente.

El Grupo Área Gestión TI implantará controles de cifrамiento sobre los medios de soporte removibles autorizados por el INC, para protegerlos contra acceso no autorizado, uso indebido, o corrupción durante el transporte. Los beneficiarios de los medios de soporte son responsables de mantener su información debidamente cifrada y de no copiarla o ponerla disponible en equipos fuera del control del INC.

Está prohibido cargar y portar información marcada como Confidencial o sensible a los medios de soportes removibles autorizados, ya que estos medios podrían perderse, o dañarse la información contenida en cualquier momento, sin la posibilidad de ser recuperada debido al cifrамiento.

A.8.3.2 Disposición de los medios de soporte removibles. Los medios de soportes removibles autorizados de propiedad del INC una vez finalice su uso, asignación o vida útil deben ser devueltos mediante acta al Grupo Área Gestión TI para su verificación y disposición final, y emisión o firma del respectivo paz y salvo.

Los medios de soportes removibles autorizados de propiedad personal del usuario, una vez finalice su relación laboral con el INC o su uso, deben ser presentados a revisión para su verificación, backup, y borrado seguro de la información del INC, para dar por finalizado el acuerdo de trasferencia de riesgo, y la emisión o firma del respectivo paz y salvo.

El INC, a través de la oficina de Almacén y Activos Fijos debe disponer en forma segura de los medios de soporte removibles de propiedad del INC cuando ya no se requieran, utilizando procedimientos formales de borrado seguro y destrucción de activos.

A.8.3.3. Transferencia de medios de soporte físicos. Los medios que contienen información se deben proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte. Esto también aplica para todos los medios de backup, medios magnéticos y medios removibles autorizados en el INC.

ARTÍCULO 11 (ANEXO A - A.9). Controles de Acceso

A.9.1. Requisitos del negocio para control de acceso. El INC determina los siguientes lineamientos para limitar el acceso a información y a instalaciones de procesamiento de su información:

A.9.1.1. Política de control de acceso a las instalaciones. El INC a través del Grupo Área Gestión y Desarrollo del Talento Humano debe establecer, documentar y revisar una política/manual/procedimiento de control de acceso con base en los requisitos del negocio y de seguridad de la información; e implementar y socializar los procedimientos y mecanismos necesario para controlar y comunicar a los responsables de todas las áreas involucradas, la Información sobre las novedades de ingreso y retiro de los servidores públicos, funcionarios, contratistas, estudiantes, pasantes, especialistas en entrenamiento, personal de proveedores y terceros en misión en el INC.

El INC, por intermedio de los Grupos Área Gestión Infraestructura Ingeniería Clínica y Grupo Área Gestión TI, establecerá los controles físicos y lógicos para que sólo el personal autorizado pueda acceder a las instalaciones del instituto y áreas de trabajo críticas de la entidad, limitando el acceso a información solo a personal autorizado.

A.9.1.2. Acceso a redes y a servicios en red. El Grupo Área Gestión TI debe implementar controles, para proveer el acceso seguro a las redes cableadas y Wifi, y restringir cualquier actividad sobre la red a dispositivos no autorizados. Solo se debe permitir uso de servicios y puertos de red para aquellos que los usuarios hayan sido autorizados específicamente

A.9.2. Gestión de acceso de usuarios: El INC presenta los siguientes lineamientos para asegurar el acceso de los usuarios autorizados e impedir el acceso no autorizado a sistemas de información y servicios tecnológicos.

A.9.2.1. Registro y cancelación del registro de usuarios: El INC debe implementar un proceso formal de registro y de cancelación del registro, para posibilitar la asignación de los derechos de acceso a sistemas de información, aplicaciones y servicios tecnológicos.

A.9.2.2. Suministro de acceso de usuario. Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o cancelar los derechos de acceso a todo tipo de usuarios para todos los sistemas y servicios, que garantice que solo el usuario conoce los datos de autenticación de sus cuentas.

A.9.2.3. Suministro de acceso de usuario. El Grupo gestión de Aplicaciones debe restringir y controlar la asignación y uso de derechos de acceso privilegiado para servidores y plataformas de TI. Debe garantizar también la toma de logs y en general garantizar el registro y la trazabilidad de eventos generados por los usuarios.

A.9.2.4. Gestión de información de autenticación secreta de usuarios. Los usuarios solo pueden entregarse de forma personal en las áreas designadas para esta labor dentro del INC, realizando una validación de identidad previa de documento de identidad. Las claves de los sistemas tecnológicos son de carácter personal e intransferible, y se debe solicitar cambio obligatorio de credenciales de autenticación al primer ingreso en las plataformas.

A.9.2.5 Revisión de los derechos de acceso de usuarios. Los dueños o responsables de los activos de información deben revisar y documentar los derechos de acceso de los usuarios, a intervalos regulares. El Grupo área Gestión TI debe implantar controles para la detección de elevación de permisos no autorizadas.

A.9.2.6 Cancelación o ajuste de los derechos de acceso. Los responsables designados en el Grupo Área Gestión y Desarrollo del Talento Humano, deben reportar con oportunidad las novedades de personal para que los administradores de sistemas y plataformas puedan modificar o revocar oportunamente los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información, al cambiar o terminar su labor, empleo, contrato o acuerdo con el INC.

A.9.3. Responsabilidades de los usuarios. A continuación, se presentan los lineamientos para que los usuarios del INC rindan cuentas por la salvaguarda de su información de autenticación:

A.9.3.1 Uso de información de autenticación secreta. Los usuarios de INC son responsables por la salvaguarda de su información de autenticación, carnets y tarjetas, tokens, y de los usuario y contraseñas de red, sistemas de información, plataformas, aplicativos, y activos de información asignados.

La información de autenticación asignada en el INC a los usuarios es de uso personal e intransferible; no se debe divulgar, compartir, ni dejar recordatorios escritos de la misma en notas, post-it, monitores, teclados, tableros, carteleras o demás lugares visibles.

Está prohibida cualquier forma de suplantación de personal sobre de los sistemas de autenticación y controles de acceso físico y lógico, implantados por el instituto. La suplantación de personal acarrea sanciones disciplinarias, contractuales y penales relacionadas en el Articulo 9 numeral A7.2.3 “Proceso y Sanciones Disciplinarias” de la presente política.

Todo funcionario y contratista será responsable del cambio de su información de autenticación de forma periódica. El Grupo Área Gestión TI establecerá cambios de manera automática en los sistemas de información, plataformas y aplicativos para que periódicamente los usuarios tengan que realizar cambio de su información de autenticación.

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 Cancerologia Empresa Social del Estado

A.9.4. Control de acceso a sistemas y aplicaciones. El INC, en cabeza del Grupo área Gestión TI, establece los siguientes son los lineamientos establecidos por el INC para Prevenir el uso no autorizado de sistemas y de aplicaciones:

A.9.4.1. Restricción de acceso a información: Se debe restringir el acceso a la información y a las funciones de los sistemas de las aplicaciones de acuerdo con el manual de control de acceso del INC.

A.9.4.3. Sistema de gestión de contraseñas. En relación con la autenticación y manejo de contraseñas, de forma obligatoria el personal del INC debe:

- Hacer uso de contraseñas fuertes diferenciadas en función del uso de acuerdo a los lineamientos el manual de criptografía y/o manual de requerimientos de seguridad del INC.
- Evitar el almacenamiento de información de autenticación por parte de los usuarios y administradores en archivos electrónicos sin protección de cifrado.
- Implantar el uso de un gestor de contraseñas interactivo y que asegure uso de contraseñas de calidad, para el almacenamiento y recordación segura de la información de autenticación de usuarios y administradores de sistemas y plataformas.
- Monitorear, restringir y controlar estrechamente el uso de programas utilitarios que podrían tener capacidad de anular el sistema y los controles de las aplicaciones.
- Restringir el acceso a códigos fuente de programas y documentación sobre el desarrollo y controles de cambio de los mismos.

A.9.4.4 Uso de programas utilitarios privilegiados. Esta prohibido el uso de programas utilitarios en el INC que podrían tener capacidad de anular el sistema y los controles de las aplicaciones.

El INC bloquea por defecto y sin previo aviso programas utilitarios tales como: proxys virtuales, redes tor, vpns gratuitas, DNS dinámicos, sniffers, mapeadores de red, programas Command and control, programas de conexión remota, programas de creación de redes alternas, sistemas de hacking y craking, anonimizadores de ip, escaners de vulnerabilidades, perfiladores de red, programas para ejecución de script, entre otros.

Los agentes de antivirus y DLP (Prevención de fuga de información) deben permanecer siempre activos en los equipos y dispositivos, y no debe deshabilitarse para instalación de programas y software de origen desconocido.

Cualquier instalación de Software en los equipos del instituto debe bloquearse, y solo debe poder realizarse con permisos elevados, verificación previa de licenciamiento, y acompañamiento de mesa de ayuda.

A.9.4.5 Control de acceso a códigos fuente de programas. El INC debe restringir el acceso a códigos fuente de programas, y debe controlar las versiones de los cambios que se realicen sobre estos. El INC y sus proveedores de desarrollo utilizan las herramienta estándar o propias de los sistemas de información Misionales para controlar el versionamiento y protección del código fuente.

ARTÍCULO 12 (ANEXO A – A.10) Criptografía. La criptografía en el INC es la técnica que protege documentos y datos. Funciona a través de la utilización de algoritmos y manejo de llaves para cifrar y encriptar (ocultar) documentos y datos confidenciales que circulan en redes locales o en internet.

Las comunicaciones secretas en el INC son usadas, entre otras finalidades, para:

- Autentificar la identidad de usuarios

- Autentificar y proteger el sigilo de comunicaciones personales y de transacciones comerciales y bancarias
- Proteger la integridad de transferencias electrónicas de fondos
- Proteger la comunicación entre sesiones del portal web y aplicaciones del INC.
- Proteger el almacenamiento y custodia de documentos electrónicos sensibles, críticos o que contengan datos personales, secretos industriales, y/o de investigación.
- Proteger la información en las comunicaciones sensibles a través de las redes del INC
- Dar legalidad y autenticidad y evitar el repudio a los documentos e información por medio de firmas electrónicas
- Proteger las sesiones de conexión remota
- Proteger la información de equipos y dispositivos que por su función se encuentre expuestos al publico o con un riesgo alto de pérdida o hurto.

A.10.1 Controles criptográficos. El INC debe asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad y/o la integridad de información en sus comunicaciones. Para esto el Grupo Área Gestión TI debe implementa la siguiente política sobre el uso adecuado de controles criptográficos, con el fin de establecer una guía bajo las mejores prácticas de Ciframiento:

A.10.1.1 Política sobre el uso de controles criptográficos. A continuación, se presenta la política implantada en el INC sobre el uso de controles criptográficos para protección de la información:

- Los propietarios de los activos de información deben identificar las necesidades de criptografía de información de acuerdo con el grado de criticidad y privacidad de estos, e informar de dicha necesidad al Grupo Área Gestión TI quien debe analizar y si es procedente aprobar.

- Todos los discos duros de equipos portátiles, y equipos de escritorio que contengan información crítica o se encuentren expuestos al público, salas de juntas o áreas abiertas deben estar cifrados para evitar perdida de información en caso de evento de robo o perdida.

- Los dispositivos de soporte removible y dispositivos móviles que sean autorizados para uso laboral en el INC deben ser cifrados y protegidos por contraseña antes de cargar información en ellos para evitar perdida de información en caso de robo o perdida.

- Los usuarios que tengan asignado tokens o certificados digitales de terceros son responsables de su correcto uso y custodia. Estos dispositivos de autenticación son de uso personal e intransferible.

- Todos los servicios publicados a internet en el INC relacionados con servidores y portales web requieren la instalación de un certificado SSL, garantizando a los visitantes la autenticidad del sitio, y validando el establecimiento de una comunicación debidamente cifrada entre el servidor web y los navegadores de usuario final.

- Las conexiones con sucursales o con oficinas de proveedores o terceros utilizando como vínculo Internet, se deben realizar haciendo uso de las herramientas para establecer túneles virtuales con ciframiento (VPN) que determine grupo Área Gestión TI, para evitar interceptación o manipulación no autorizada.

A.10.1.2 Gestión de claves. El INC establece directrices de sobre el uso, protección y tiempo de vida de claves criptográficas, las cuales se documentan en el manual de requerimientos de seguridad de la información de la entidad.

ARTÍCULO 13 (ANEXO A - A.11). Seguridad física y ambiental. El INC debe prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización. Para esto se determinan los siguientes lineamientos:

A.11.1 Áreas seguras. El INC debe prevenir el acceso físico no autorizado, el daño y la interferencia a la información y sus instalaciones de procesamiento de información. Para esto los grupos Área Gestión Infraestructura e Ingeniería Clínica, Grupo Área gestión de TI, y grupo área Gestión Documental y correspondencia, deben diseñar procedimientos e implementar y controles para:

A.11.1.1 Establecer Perímetro de seguridad Física. Asilar y proteger áreas que contengan información confidencial o crítica, e instalaciones de manejo de información, así como aquellas en las que se encuentren los equipos y demás infraestructuras críticas de soporte asistencial, a los sistemas de información y a las comunicaciones.

Debe existir áreas de recepción y filtros de seguridad suficientes que solo permitan la entrada de personal autorizado.

Las medidas de seguridad perimetral que se deban tomar dependerán directamente del valor de los activos de información, su nivel de confidencialidad, y los valores requeridos de disponibilidad

A.11.1.2 Controles físicos de entrada. Las áreas seguras del INC se deben proteger mediante controles de entrada apropiados para asegurar que solamente se permite el acceso a personal autorizado. Los controles de entrada deben tener trazabilidad completa de los eventos de acceso, y se deben revisar periódicamente para detectar anomalías.

Todos los sitios en donde se encuentren sistemas de procesamiento informático o de almacenamiento, deben ser protegidos de accesos no autorizados, utilizando tecnologías de autenticación, monitoreo y registro de entradas y salidas.

A.11.1.3 Seguridad de Oficinas e instalaciones. El instituto en cabeza del grupo de Gestión Ambiental y Soporte Hotelero debe realizar periódicamente un estudio de seguridad con la empresa contratada para realizar la vigilancia de la entidad, para establecer los anillos de seguridad y controles para aplicar seguridad física a oficinas, consultorios, salones e instalaciones, y garantizar la protección de los activos del INC. Se debe considerar el uso complementario de seguros contra robo, perdida, vandalismo, asonada. etc.

Todos los visitantes o extraños deben ser autorizados durante su estadía en INC, y den ser monitoreados por medio de CCTV. El personal de INC, pacientes, visitantes o terceras personas, que ingresen a las instalaciones de la entidad, deberán poseer una identificación a la vista que claramente los identifique como tal, y estas identificaciones serán intransferibles. Se debe además hacer una revisión periódica de identificadores de acceso.

No se permite el uso de equipos como videograbadoras, cámaras fotográficas, grabadoras, sniffers, analizadores de datos, (ej: hardware especial) etc., dentro de las instalaciones del INC a menos que exista una autorización formal por el oficial de seguridad de la información o personal de la Oficina asesora de Comunicaciones.

El sitio escogido para colocar los sistemas de información, equipos de cómputo y comunicaciones, deben estar protegidos por barreras y controles físicos, para evitar intrusión física, inundaciones, y otro tipo de amenazas que afecten su normal operación.

Las salas de juntas, oficina y sitios desatendidos que contengan activos de información, equipos o dispositivos, deben permanecer bajo llave, o medidas de protección complementarias.

A.11.1.4 Protección contra amenazas externas y ambientales. El instituto diseña y aplica mediante el plan de emergencias, la protección física de instalaciones y personal contra desastres naturales, ataques maliciosos o accidentes.

Todo el cableado estructurado debe estar protegido contra acceso no autorizado y deben contar con medidas de protección ambiental y de riesgo eléctrico adecuadas.

Adicionalmente el INC debe identificar la Infraestructura critica del INC relevante para la ciberdefensa y ciberseguridad del Estado Colombiano, y gestionar protección física de los mismos contra desastres naturales, ataques maliciosos o accidentes.

A.11.1.5 Trabajo de áreas seguridad. Los Grupos Area Gestión TI, Grupo Gestión Documental y Correspondencia y Grupo Área Gestión de Tecnología Clínica G, Se deben diseñar y aplicar procedimientos para trabajo en áreas seguras.

A.11.1.6 Áreas de carga y Despacho. Se deben controlar los puntos de acceso tales como áreas de despacho y de carga y otros puntos en donde pueden entrar personas no autorizadas, y si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado.

Los materiales que deban entrar al INC deben ser inspeccionados debidamente en la zona de descargue, para evitar la entrada de elementos peligrosos a las áreas internas.

El material entrante o saliente debe ser registrado, con el fin de mantener el listado de inventario actualizado

A.11.2 Seguridad Física de Equipos. El INC debe prevenir la pérdida, daño, robo o compromiso de activos, y la interrupción de las operaciones del instituto. Para esto debe:

A.11.2.1 Ubicar y proteger los equipos. Proteger áreas que contengan información confidencial o crítica, e instalaciones de manejo de información, así como proteger las instalaciones y sedes del INC para asegurar que solamente se permite el acceso a personal autorizado.

Se deben adoptar o mantener al día, controles para minimizar el riesgo potencial de Robo. Fuego, explosivos, humo, inundación, interferencia eléctrica, y radiación electromagnética.

Las áreas en donde se operen equipos de procesamiento de información, no se permitirá fumar, tomar ningún tipo de bebidas o consumir alimento.

A.11.2.2 Servicios públicos de soporte. Los equipos críticos para la operación del INC se protegen de fallas de potencia y otras interrupciones causadas por fallas en los servicios públicos de soporte.

El centro de datos del INC opera bajo medidas de contingencia y redundancia eléctrica y aire acondicionado. Se debe realizar mantenimiento programado a las plantas eléctricas, subestaciones y UPS, los cuales se deben probar según las recomendaciones del fabricante, de tal forma que garanticen el suficiente tiempo para realizar las funciones de respaldo en servidores y aplicaciones.

Las fallas en el control de la temperatura o humedad pueden afectar la operación de la entidad, así que, se debe tener un estricto monitoreo sobre estas variables.

A.11.2.3 Servicios públicos de soporte. El cableado de potencia y de telecomunicaciones que porta datos o brinda soporte a los servicios de información en el INC se protege contra interceptación, interferencia o daño, se encuentra debidamente canalizado, y se ampara bajo contrato de mantenimiento.

A.11.2.4 Mantenimiento de Equipos. Los equipos, cableado estructurado, y datacenters se deben soportar y mantener bajo contratos o programas periódicos de mantenimiento según las recomendaciones de los fabricantes, para asegurar su disponibilidad e integridad continua. Cada supervisor de contrato debe asegurarse de la ejecución y de mantener la documentación de los ejercicios de mantenimiento.

Los dispositivos y sistemas Biomédicos deben estar sujetos a programas de mantenimiento periódicos, y deben estar amparados por contratos de soporte y mantenimiento por parte de fabricantes o representaciones.

A.11.2.5 Retiro de Activos. Los equipos de cómputo no se deben retirar de su sitio sin pasar por un proceso de autorización previa, controlado mediante procedimiento de Gestión de Activos por el grupo de Almacén mediante el diligenciamiento del formato que dispone el área según tipo de activo.

A.11.2.6 Seguridad de Activos y equipos fuera de las instalaciones. Se deben aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones del INC, teniendo en cuenta los diferentes riesgos de trabajar con información fuera de dichos predios.

Los usuarios deben tener especial cuidado contra fallas del sistema de control del medio ambiente donde ubican el equipo o dispositivo, y otras amenazas electromagnéticas externas que puedan afectar la normal operación del sistema.

No dejar los equipos y dispositivo s desatendidos en zonas públicas, Los equipos portátiles siempre deben estar protegidos por guayas.

Los computadores personales deben evitar su apariencia y ser llevados con morral de equipaje de mano. Esta prohibido llevar el equipo portátil a actividades y sitios no laborales que puedan poner el riesgo de hurto estos activos sin justificación.

Para equipos que se retiran constantemente de las instalaciones se debe considerar siempre el uso de seguros contra robo, perdida etc.

A.11.2.7 Disposición segura o reutilización de equipos. Se debe establecer un procedimiento de disposición final segura de los equipos, para verificar todos los elementos de equipos que contengan medios de almacenamiento ejecuten un proceso de borrado seguro antes de su baja o reusó, y para asegurar que software y licencias haya sido retiradas o sobrescritas.

A.11.2.8 Equipos de usuarios desatendidos. Los usuarios deben asegurarse de que a los equipos desatendidos se les da protección apropiada.

Se deben establecer controles no modificables para que los equipos de cómputo y dispositivos se bloqueen automáticamente después de cierto tiempo de inactividad

Los equipos de cómputo siempre deben apagarse después de finalizar la jornada laboral.

Los equipos en salas de juntas y auditorios deben permanecer bajo llave, anclados con guaya a las mesas de trabajo, y sus discos deben estar cifrados.

Los puntos de red del instituto deben contralarse de tal forma que ningún dispositivo pueda conectarse ni ver el tráfico de red sin pasar una validación previa del Grupo Area Gestión TI.

A.11.2.9 Política de Escritorio Limpio y Pantalla Limpia. Todo el personal del INC durante y fuera del horario laboral debe prevenir el acceso no autorizado y la pérdida o daño de la información que se encuentra en los puestos de trabajo, equipos de cómputo, medios extraíbles, dispositivos de impresión y digitalización de documentos, mediante lineamientos establecidos que se presentan a continuación:

- Al retirarse del puesto de trabajo y al finalizar la jornada laboral, los escritorios deben permanecer despejados y libres de documentos físicos y/o medios extraíbles que contengan información clasificada, sensible o pública reservada, éstos deben guardarse en un lugar seguro y bajo llave. Los documentos y/o medios extraíbles con información pública también deben guardarse para evitar la pérdida de esta información.

- Los puestos de trabajo deben permanecer limpios y ordenados. No deben ingerirse bebidas o alimentos encima de teclados y equipos.

- Los puntos de envío y recepción del correo, Maquinas de fax, escáneres e impresoras deben ser protegidos de acceso no autorizado, y deben bloquearse automáticamente.

- Los dispositivos de impresión y digitalización deben permanecer limpios de documentos. Cuando se imprima o digitalice documentos con información pública clasificada o pública reservada, éstos deben recogerse inmediatamente.

- No se deben utilizar como papel de reciclaje documentos clasificados, que contengan de datos personales, historia clínica o cualquiera de sus soportes.
- Los gabinetes, cajones y archivadores de contengan documentos y/o medios extraíbles con información pública, clasificada o privada deben quedar cerrados bajo llave, durante la hora de almuerzo, y al finalizar la jornada laboral.

- El escritorio del computador no debe contener ningún tipo de archivo, salvo los accesos directos a las aplicaciones necesarias para que los funcionarios o contratistas ejerzan sus funciones o cumplan sus obligaciones contractuales, según el caso.

- Los documentos digitales y electrónicos que producen los funcionarios o contratistas en el ejercicio de sus labores o en el cumplimiento de sus obligaciones contractuales, según el caso, deben guardarse en la carpeta de almacenamiento en red, o sistema corporativo de almacenamiento en la nube dispuesto y autorizado por el INC

- Al levantarse del puesto de trabajo, todos los usuarios de equipos deben bloquear la sesión de cómputo mediante la combinación de teclas Windows + L para proteger el acceso a las aplicaciones y servicios de la entidad.

- Todos los equipos de cómputo y dispositivos de impresión y digitalización deben apagarse cuando no estén en uso.

ARTICULO 14 (ANEXO A - A.12) Seguridad de las operaciones

A.12.1 Procedimientos operacionales y responsabilidades. El INC a través del Grupo Área Gestión TI se debe encargarse de la operación y administración de los recursos tecnológicos que soportan la operación del instituto, y propender por la implementación de los controles asociados a éstos para mitigar los riesgos sobre la confidencialidad, integridad y disponibilidad de la información; para este fin debe cumplir con los siguientes lineamientos:

A.12.1.1. Los procedimientos operativos deben estar documentados y actualizados, y deben estar a disposición de todos los usuarios que los necesitan en el instituto.

A.12.1.2. Se debe implementar un procedimiento para la gestión o control de cambios de las TIC donde los cambios en la configuración de los equipos, redes, sistemas de información, bases de datos, aplicaciones o cualquier activo de información sean registre, controle, evalué y apruebe. Se deben controlar los cambios en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.

A.12.1.3. Se debe monitorear y realizar seguimiento al uso de recursos, hacer los ajustes, y proyecciones de los requisitos de capacidad futura, para asegurar el desempeño requerido de los sistemas.

A.12.1.4. Se deben separar los ambientes de desarrollo, prueba y producción de los sistemas de información misionales y de apoyo crítico, para reducir los riesgos de acceso o cambios. La data de prueba debe ser debidamente ofuscada para evitar fuga de información.

A.12.2 Protección contra códigos maliciosos. De deben Implementar y monitorear controles de detección, de prevención, alerta automática y de recuperación contra códigos maliciosos, para asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra ataques de este tipo. Los controles contra código malicioso deben proteger la red perimetral, la red interna y los equipos (A.12.2.1)

A.12.3 Copias de Respaldo. Se debe implantar y mantener actualizado un manual de backup y recuperación, que permita en caso de desastre proteger la información crítica alojada en el Data Center del INC, en los servidores administrados por proveedores y terceros, y de la configuración de todas las plataformas y dispositivos de red.

Los backups de la información, software e imágenes de los sistemas deben ponerse a prueba regularmente de acuerdo con el plan de backup.

Los sistemas de backup deben estar desconectados o asilados de la red, y deben establecerse contratos con empresas especializadas para resguardar medios en custodia externa con frecuencia adecuada.

A.12.4 Registro y Seguimiento

A.12.4.1. Registro de eventos y correlación de riesgo. Se deben elaborar, conservar de forma segura, y revisar regularmente los registros de eventos en los sistemas misionales y críticos, acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información. Se debe propender por la consecución y el uso de aplicaciones o sistemas de correlación de eventos para facilitar analítica sobre esta actividad. El INC se reserva el derecho de monitorear la actividad en sus redes y sistemas con finalidad de propender por la calidad de sus servicios y de la seguridad de la información del INC.

A.12.4.2. Protección de Logs. Las actividades y operadores de los administradores de plataformas tecnológicas, sistemas de información y bases de datos se deben registrar (toma de logs), y los registros se deben proteger y revisar con regularidad. Estos registros se deben proteger adecuadamente de su integridad y disponibilidad, además de fijar un proceso periódico de revisión.

Deben establecerse directrices institucionales para la retención, almacenamiento, manejo y eliminación de los registros de log de la institución, incluyendo también los registros de los sistemas de monitoreo.

Los controles de protección de los registros log deben considerar al menos: Alteraciones a los tipos de mensajes que se registran, Archivos de registro editados o eliminados, y Capacidad de almacenamiento

Las revisiones de auditoría deben limitarse al acceso de sólo lectura y no afectar la disponibilidad de las plataformas o sistemas revisados en horarios de servicio

A.12.4.3. Registros de Administradores y Operadores. Las actividades de los administradores y de los operadores de sistemas se deben registrar, y los registros se deben proteger y revisar con regularidad.

Se deben definir roles y sus responsabilidades dentro de las áreas claves de la entidad que realicen administración u operación sobre sistemas de registro, para hardware, software, redes y medios, tanto a nivel individual de cada sistema como de una infraestructura global de manejo de logs.

A.12.4.4. Sincronización de relojes. Los relojes de todos los sistemas de procesamiento, plataformas tecnológicas, servidores y sistemas de información administrados o que trabajen en las redes del INC, al igual que las herramientas de seguridad de la información y monitoreo se deben sincronizar con una única fuente de referencia de tiempo. (Controlador de dominio sincronizado previamente contra una fuente externa.)

A.12.5 Control de Software Operacional

A.12.5.1. Instalación de software en sistemas operativos: La instalación de software en sistemas operativos de equipos finales y servidores es restringida y debe ser controlada por medio de solicitud de gestión de cambio a la mesa de ayuda.

Cualquier instalación de software en los sistemas operativos está sujeta a una revisión de licenciamiento y disponibilidad de licencias. No se permite instalación de software que no cumpla los requerimientos del manual de requisitos técnicos de seguridad técnicos de seguridad, los de la política de privacidad y confidencialidad para el tratamiento de datos personales, y las leyes de protección de derechos de autor.

La entidad propende por el uso de software libre para procesos no críticos del instituto. El responsable de seguridad de la información debe revisar los términos de uso y licenciamiento de cada software libre antes de ser autorizado su uso dentro de la institución. Por defecto no se autoriza el uso de software libre sin establecer previamente un contrato de soporte y mantenimiento con un partner autorizado, para el resguardo de secretos industriales o laborales, información que contenga de datos personales, o que acceda a la historia clínica.

El Grupo Area Gestión TI debe llevar control estricto del inventario de licenciamiento instalado en cada uno de los equipos y servidores, incluyendo software instalado en máquinas virtuales.

A.12.6 Vulnerabilidades y Amenazas Técnicas. El INC debe evitar el aprovechamiento de vulnerabilidades técnicas por parte de un atacante interno o externo. Para esto debe:

A.12.6.1 Gestión sobre Vulnerabilidades. Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de la red y de los sistemas conectados; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.

La entidad debe implantar una arquitectura de seguridad integrada con capacidades de administración de registros y seguridad basada en el análisis y la visibilidad de amenazas y vulnerabilidades en la red perimetral y en la red interna, para proporcionar una mejor detección contra violaciones.

Se deben ejecutar de forma programada ejercicios de pruebas de penetración de Hacking Ético sobre los sistemas de información misionales y sistemas de apoyo para obtener, con el fin de evaluar, fortalecer y mejorar la seguridad.

Para la gestión de actualizaciones de seguridad de sistemas operativos, se tiene que llevar a cabo mediante un procedimiento que pruebe y controle los cambios de los aplicativos instalados. Antes del cambio, la actualización debe ser probada en sistemas físicos o virtuales controlados y se debe asegurar de que se guarde una copia de seguridad de la versión anterior por si fuera necesaria una restauración.

La liberación de actualizaciones de seguridad debe realizarse de manera programada y escalonada usando una herramienta de control de distribución de parches, y en horarios acordados previamente con la operación para no consumir todos los recursos de red o bloquear uno o varios servicios que presta la entidad.

La detección de vulnerabilidades debe alinearse con la gestión de riesgo de la entidad para identificar y corregir las fallas de software y plataformas tecnológicas, identificar amenazas y falencias, y ofrecer alternativas para la minimización del riesgo y remediación de las vulnerabilidades

A.12.6.2 Restricciones sobre la instalación de software. Está prohibida la descarga e instalación de software en los equipos finales por parte de los usuarios del INC. El grupo are gestión TI debe implantar controles que impidan la libre instalación de programas, ejecución de bats y scripts, y la ejecución de programas portables en la maquinas.

Todos los equipos del instituto deben estar registrados en el directorio activo, y deben permitir la aplicación de las políticas y controles de restricción de software según el perfil del usuario.

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 Cancerologia Empresa Social del Estado

A.12.7 Controles de Auditorias sobre sistemas de información. El grupo Area de Control interno debe preparar e implementar un programa de auditoria para la revisión de cumplimiento de la norma iso27001, por lo menos una vez al año. Las sesiones de auditoria que involucre n la verificación de los sistemas operativos se deben planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos de la entidad.
Los activos de información (físicos y electrónicos) deben ser auditados anualmente por una empresa externa, sobre la gestión de tratamiento de datos personales.

ARTICULO 15 (ANEXO A – A.13) Seguridad de las Comunicaciones.

A.13.1. Gestión de la seguridad en redes

El INC, a través del Grupo área Gestión TI, gestionará y controlará las redes de comunicaciones para proteger la información en sistemas y aplicaciones. Para esto debe:

A.13.1.1. Controles de Redes. El instituto debe contra un procedimiento de gestión de redes, e implantar políticas para el acceso de red basado en roles y perfiles, con el fin de asegurar el sistema de red antes de que los usuarios hagan uso de las misma. Para esto se deben implantar controles, incluyendo preadmisión, chequeo de políticas de seguridad en el usuario final y controles post-admisión sobre los recursos a los que pueden acceder en la red los usuarios y dispositivos, y que pueden hacer en ella.

Las redes se deben monitorear mediante herramientas que permitan la supervisión de manera continua la disponibilidad, la capacidad y salud de los servicios de red.

El Instituto debe contar con herramientas de software de prevención de intrusión y denegación de servicio para sus redes perimetrales.

A.13.1.2. Seguridad de los servicios de Red. El instituto debe identificar e implantar los procedimientos, mecanismos y herramientas para:

- Establecer los mecanismos de seguridad de red, y los Acuerdos de Niveles de Servicios - ANS requeridos para que los proveedores de servicios de tecnologías de Información garanticen la disponibilidad de las redes WAN e Internet.
- Proteger la información que se transporta a través de las redes de datos del instituto, propendiendo la integridad y confidencialidad de la información.
- Desplegar controles de prevención de perdida de datos para proteger apropiadamente la información incluida en los mensajes electrónicos.
- Revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades del INC para la protección de la información.
- Establecer la transferencia segura de información entre el instituto y las partes externas mediante herramientas como VPN, o mecanismos de cifrado de comunicaciones.
- Establecer el cumplimiento de los acuerdos de confidencialidad y de transferencia de datos, y blindar jurídicamente la transferencia segura de información del negocio entre la organización y las partes externas

Se prohíbe a los usuarios del INC la instalación y uso sin autorización del Grupo Área Gestión TI, de las siguientes herramientas de gestión de redes:

- Sniffers
- Mapeadores o escáneres de red
- Analizadores de tráfico
- Analizadores de amenazas y vulnerabilidades,
- Conexiones de programas de soporte remoto no autorizados por el instituto

- Conexiones de redes VPN tipo gratuito o de uso personal,
- Conexiones a redes tipo TOR, uso de proxys virtuales.
- Cualquier otro programa destinado a evadir los controles de seguridad del instituto, o que pueda poner en riesgo la información institucional.

Se prohíbe de igual manera la implantación de redes de tipo personal sobre la infraestructura de red, equipos del instituto y/o cualquier conducta similar que atente contra la seguridad de las comunicaciones. Las infracciones sobre estas restricciones serán consideradas como faltas muy graves y causarán el bloqueo y aislamiento inmediato del equipo o dispositivo fuente, y la aplicación de sanciones relacionadas en el apartado “incumplimiento y Sanciones” de la presente política.

A.13.1.3. Separación de las redes. Segmentar el tráfico de red para evitar acceso a servicios y sistemas no autorizados. Para esto el instituto debe diseñar, implantar y mantener documentada una arquitectura segmentada de seguridad de redes, donde se separen como mínimo los usuarios, los servicios de información y tecnológicos, los sistemas biomédicos, las infraestructuras críticas, los dispositivos móviles, y las redes wifi.

El INC debe implantar zonas desmilitarizadas para publicar servicios tipo web que no permitan conexiones ilegales hacia las redes internas de la entidad.

A.13.2. Transferencia de la información. El INC para mantener la seguridad de la información transferida a cualquier entidad externa debe:

A.13.2.1. Políticas y Procedimientos de Transferencias de Información. Contar con políticas, procedimientos y controles de transferencia formales para:

- Transferencias documentales al archivo general de la nación y entes relacionados
- Transferencia de datos electrónicos a terceros
- Establecimiento de sistemas VPN punto a punto entre el INC y un ente externo.
- Ofuscamiento y supresión de datos sensibles y datos personales para investigaciones, convenios y publicaciones.
- Interoperabilidad de la historia clínica con entidades relacionadas del sector salud.

A.13.2.2. Acuerdos de transferencia de la Información. Las transferencias de información en el INC requieren el establecimiento obligatorio de cláusulas especiales de confidencialidad en el contrato/ convenio, de la firma de un acuerdo de confidencialidad, y la firma de un contrato de trasmisión de información con finalidades definidas por parte del responsable de tratamiento de datos identificado por la Superintendencia de Industria y Comercio (SIC) en el registro nacional de bases de datos.

A.13.2.3. Mensajes Electrónicos. El instituto debe proteger con técnicas de Ciframiento adecuadas la transferencia de información que se realice por medios electrónicos.

La información confidencial o que se termine como privada o semiprivada se deben enviar como mensajes cifrados y protegidos con derechos a personas de dentro y fuera de la entidad.

A.13.2.4. Acuerdos de Confidencialidad y deber de secreto. Se deben identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades del instituto para la protección de la información.
El deber de confidencialidad, recogido en el artículo 4 literal h) de la ley de Protección de Datos (LEPD), se formaliza en el INSTITUTO NACIONAL DE CANCEROLOGIA E.S.E a través de la firma de un acuerdo de confidencialidad y deber de secreto suscrito entre el usuario o tercero, y el responsable del tratamiento.

Los acuerdos de confidencialidad se deben establecer y formalizar para todos servidores públicos, contratistas, terceros, docentes, estudiantes, y todos aquellos que tengan algún tipo de acceso a la información del INSTITUTO NACIONAL DE CANCEROLOGÍA ESE.

Todas las personas que intervengan en el INSTITUTO NACIONAL DE CANCEROLOGIA E.S.E. en el tratamiento de información, o que tenga acceso a la misma debido la solución de interoperabilidad de la historia clínica, sin importar su naturaleza están obligadas a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende el tratamiento, pudiendo solo realizar suministro o comunicación de datos personales ajenos cuando ello corresponda al desarrollo de las actividades autorizadas en la Política de Tratamiento de Datos Personales del INC, y en la LEPD o por requerimiento de autoridad administrativa y judicial según el caso.

ARTICULO 16 (ANEXO A - A.14) Adquisición, desarrollo y mantenimiento de sistemas

El Grupo Área Gestión TI será la única área autorizada para solicitar la adquisición, desarrollo, administración, mantenimiento e implementación de aplicaciones y sistemas de información. La adquisición de sistemas de información se ejecutará siguiendo el proceso determinado de Gestión del Gasto.

A.14.1 Requisitos de seguridad de los sistemas de información. El Grupo Área Gestión TI a través del Grupo Gestión de Aplicaciones debe garantizar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida de los mismos. Para esto debe

A.14.1.1. Realizar análisis y especificación de requisitos de seguridad de la información para nuevos sistemas de información o para mejoras a los sistemas de información existentes.

A.14.1.2. Proteger de actividades fraudulentas la Información involucrada en servicios de aplicaciones que pasan por redes públicas mediante técnicas de Ciframiento, certificados digitales SSL y uso de VPN.

A.14.1.3 Proteger la información involucrada en las transacciones de servicios de aplicaciones para prevenir la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizada.

A.14.2 Seguridad en los procesos de desarrollo y de soporte. El INC debe asegurar que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información, incluyendo también la gestión de los proveedores de desarrollo contratados por el INC. Para esto debe:

A.14.2.1. Establecer una política/manual de desarrollo seguro y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos dentro de la organización (Si aplica). Se debe exigir a proveedores y terceros desarrolladores la aplicación reglas para el desarrollo seguro de software y de sistemas, validar la metodología que se aplique, y realizar supervisión de la actividad de desarrollo de sistemas subcontratada.

A.14.2.2. Controlar los cambios a los sistemas dentro del ciclo de vida de desarrollo mediante el uso de procedimientos formales de control de cambios, ordenes de transporte y herramientas de versionamiento.

A.14.2.3 Revisar las aplicaciones críticas del negocio cuando se cambien las plataformas de operación y la infraestructura que la soporta, y poner a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad.**A.14.2.4.** Asegurar que las modificaciones a los paquetes de software se deben limiten a los cambios necesarios, y que todos los cambios se controlen, versionen y documenten estrictamente.

A.14.2.5. Establecer, documentar y mantener un manual de requerimientos de seguridad de la información, que contenga los principios para la organización y la contratación de sistemas seguros, y aplicarlos a cualquier trabajo de implementación de sistemas de información.

A.14.2.6. Establecer y proteger adecuadamente los ambientes de desarrollo, calidad y producción, seguros y segmentados, para las tareas de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas.

A.14.2.7. Supervisar y hacer seguimiento de la actividad de desarrollo de sistemas subcontratada. Verificar periódicamente el acceso y uso de las plataformas por parte de proveedores de desarrollo.

A.14.2.8. Estandarizar, llevar a cabo y documentar pruebas de funcionalidad de la seguridad durante el desarrollo.

A.14.2.9. Establecer programas de prueba y criterios relacionados, en caso de tratarse de sistemas de información nuevos, actualizaciones y nuevas versiones.

A.14.3 Datos de Prueba

A.14.3.1. Los datos de prueba se deben seleccionar, proteger y controlar cuidadosamente. Se deben Parametrizar y enmascarar datos para evitar su uso inadecuado en las pruebas; en los casos que sea posible de deben generan de forma escalable sub-conjuntos de datos de Bases de datos acorde a las necesidades para no usar toda la data real como pruebas.

ARTICULO 17 (ANEXO A - A.15) Relaciones con los proveedores

A.15.1 Seguridad de la información en las relaciones con los proveedores. El INC establece los siguientes lineamientos para asegurar la protección de los activos de la organización que sean accesibles a los proveedores:

A.15.1.1 El INC a través de los Grupos Area Gestión TI, Grupo de Gestión Documental y Correspondencia, y la Oficina de Asesoría Jurídica definirán mecanismos de control que aseguren que la información a la que tenga acceso un tercero cuente con un nivel de protección adecuado, y que éstos cumplan con las políticas y procedimientos de seguridad de la información establecidos.

A.15.1.2 Se deben establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor en los estudios previos y contrato, para que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la organización

A.15.1.3 El Grupo Gestión de Compras y Contratación deben incluir en los acuerdos, convenios y contratos con proveedores, requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación.

A.15.2 Gestión de la prestación de servicios de proveedores: El INC debe garantizar que los proveedores cumplan los Acuerdos de Nivel de Servicio (ANS) y mantengan el nivel acordado de seguridad de la información. Para esto:

A.15.2.1 Cada uno de los supervisores de contrato en el INC deben hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores, asegurando el cumplimiento de los requisitos de seguridad de la información y los ANS. Los proveedores y su personal se deben acoger al cumplimiento de controles de seguridad de la información del instituto, y a las condiciones de licenciamiento, uso y monitoreo de las herramientas de seguridad que determine el INC.

A.15.2.2 Se deben gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de la información, sistemas y procesos del negocio involucrados, y la revisión de los riesgos de seguridad digital.

ARTICULO 18 (ANEXO A - A.16) Gestión de incidentes de seguridad de la información

A.16.1 Gestión de incidentes y mejoras en la seguridad de la información

El INC, a través del Grupo Área Gestión TI se encarga de definir, documentar, mantener publicar y aplicar los procedimientos para atender, valorar, clasificar y dar respuesta a los eventos de seguridad de la información. Para esto debe:

A.16.1.1 Establecer responsabilidades y procedimientos. Diseñar, construir y aplicar un protocolo referente al reporte de incidentes de seguridad de la información que defina claramente los roles y responsabilidades en la gestión de incidentes y requerimientos de seguridad.

A.16.1.2 Informar Eventos de Seguridad de la información. Todos los usuarios del INC deben realizar de manera obligatoria el reporte de eventos de seguridad de la información tan pronto como sea posible a la mesa de ayuda (línea 7000), para reducir la probabilidad e impacto del riesgo inherente a ellos.

Los eventos e incidentes de seguridad de la información serán evaluados e investigados y se les dará respuesta liderados por el grupo de seguridad de la información y los administradores de plataformas tecnológicas, de acuerdo con el manual interno de gestión de incidentes, es su capítulo de seguridad de la información.

A.16.1.3 Informar debilidades de seguridad de la información. Todos los usuarios de los servicios y sistemas de información del INC, deben observar e informar a la línea 7000 cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios. De igual forma deben reportar al Grupo área Gestión IT cualquier servicio tecnológico nuevo para que se realice una evaluación de riesgo sobre el mismo

A.16.1.4 Evaluar los eventos de seguridad. Los eventos de seguridad de la información se deben evaluar y se debe decidir si se van a clasificar como incidentes de seguridad de la información. Todos los eventos y su evaluación se deben registrar en una herramienta de gestión de incidentes. (Helpeople). Los eventos deben evaluarse siguiendo los lineamientos del Plan de protección y defensa de la infraestructura Critica Cibernética del sector salud.

A.16.1.5 Dar respuesta a los incidentes de seguridad de la información. Se debe dar respuesta a los incidentes de seguridad de la información de acuerdo con el procedimiento de gestión de incidentes de seguridad de la información, y utilizando la herramienta de gestión de conocimiento del instituto (Helpeople).

A.16.1.6 Aprender de los incidentes de seguridad. Se debe construir una base de conocimiento de seguridad de la información donde se registren las principales soluciones, las cuales deben estar disponibles para consulta del personal de seguridad de la información y seguridad informática. El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debe usar para reducir la posibilidad o el impacto de incidentes futuros.

A.16.1.7 Recolectar la evidencia de forma segura. La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia, de acuerdo con los lineamientos del Manual de Sistema de Cadena de Custodia de la Fiscalía General de la Nación. El Instituto debe adquirir las herramientas necesarias para poder recolectar evidencias de los sistemas informáticos, validas en cualquier proceso investigativo o penal, y mantener una cadena de custodia valida ante las autoridades competentes.

ARTICULO 19 (ANEXO A - 17.1) Gestión de continuidad de negocio, y recuperación ante desastres

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 Cancerologia Empresa Social del Estado

A.17.1 Continuidad de seguridad de la información

A.17.1.1 Planificación de la continuidad de la seguridad de la información. El INC, liderado por la Oficina Asesora de Planeación debe determinar los requisitos, realizar un análisis de impacto de negocio (BIA), y propender por la implementación de un plan de continuidad de negocio que le permita al INC continuar con sus operaciones, en caso de presentarse fallas o inconvenientes en sus sistemas críticos que le impidan el normal funcionamiento de los servicios críticos.

La oficina Asesora de Planeación y Sistemas destinará los recursos financieros suficientes para proporcionar una respuesta efectiva, para soportar los procesos claves de la entidad en caso de contingencia o eventos catastróficos que afecten la continuidad de su operación.

El grupo Área Gestión TI debe consolidar y documentar en un plan de recuperación de desastres (DRP) los procedimientos existentes de recuperación de las aplicaciones críticas, redundancias de procesamiento de instalaciones de procesamiento de información, y los roles/responsabilidades requeridos para responder ante un evento de interrupción de los servicios de TI.

Los grupos Área Gestión de Infraestructura e ingeniería hospitalaria y Grupo Área Gestión TI lideraran la identificación y protección de infraestructuras críticas para la ciberdefensa y Ciberseguridad del INC.

A.17.1.2 Implementación de la continuidad de la seguridad de la información. El INC debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.

A.17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información. El plan de continuidad de negocio una vez implementado, y los planes de contingencia y de recuperación de desastres (DRP) deben probarse y verificarse a intervalos regulares, con el fin de asegurar que los controles de continuidad de la operación y la seguridad de la información implementados son válidos y eficaces durante situaciones adversas o de desastre natural mayor.

A.17.2 Redundancias. El INC debe garantizar de la disponibilidad de instalaciones de procesamiento de información. Para esto debe:

A.17.2.1 Implementar redundancias. Las instalaciones de procesamiento de información se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad. La redundancia se debe evaluar para sistemas críticos de operación de Datacenter en sus controles eléctricos, ambientales, servidores, almacenamiento, Directorio Activo, DNS, DHCP, Firewalls, antivirus, Canales de Internet, y demás que considere el análisis BIATI del INC.

.

ARTICULO 20 (ANEXO A – A.18) Cumplimiento

A.18.1 Cumplimiento de requisitos legales y contractuales. El INC debe evitar violaciones de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información y de cualquier requisito de seguridad. Para esto debe:

A.18.1.1 Identificar la legislación aplicable y los requisitos contractuales. Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes y el enfoque de la organización para cumplirlos, se deben identificar y documentar explícitamente, y mantenerlos actualizados en la política de seguridad de la información y en la política de manejo de datos personales del instituto, y en el manual de requerimientos de seguridad de la información.

La Política de Seguridad y Privacidad del INC recoge todos los requisitos constitucionales, estatutarios, reglamentarios, contractuales y jurisprudenciales pertinentes, y el enfoque de la institución para cumplirlos. De igual manera en la Política de Privacidad y Confidencialidad para

el Tratamiento de Datos Personales se recogen los requisitos constitucionales, estatutarios, reglamentarios, jurisprudenciales y contractuales para el aseguramiento legal y la gestión de Habeas data del instituto.

Estos requerimientos legales y de cumplimiento se deben mantener actualizados para que den cubrimiento a cada sistema de información, servicio y proceso del instituto.

El Grupo Área Gestión TI en cabeza del líder de seguridad de la información, y la oficina de Asesoría Jurídica garantizarán la identificación, documentación y cumplimiento de la normatividad vigente y aplicable relacionada con la seguridad de la información.

A.18.1.2 Controlar derechos de propiedad intelectual. La propiedad intelectual en el INC se define como la disciplina jurídica que tiene por objeto la protección de bienes inmateriales, de naturaleza intelectual y de contenido creativo producto del ingenio del talento humano.

El INC implementará y mantendrá los controles necesarios para dar cumplimiento a las disposiciones legales sobre derechos de autor, propiedad intelectual, ley de transparencia y Estrategia de Gobierno en Línea.

Para todo el material que es desarrollado por una persona natural o física mientras tenga una vinculación como funcionario o como contratista con el INC, se debe considerar que los derechos patrimoniales son propiedad del INC y que es de uso exclusivo de la institución, por lo tanto, debe ser protegida contra un develado, descubrimiento o uso que menoscabe los intereses institucionales misionales, reputacionales, económicos y en general cualquier prejuicio contra el INC.

Las relaciones institucionales de los empleados deben incluir cláusulas que especifiquen los compromisos y cuidados que deben tener con la información susceptible de protección por parte del régimen de propiedad intelectual y en lo referente a la confidencialidad. Así mismo, los contratos de prestación de servicios deben incluir los compromisos y cuidados que deben tener con la información susceptible de protección por parte del régimen de propiedad intelectual y en lo referente a la confidencialidad por parte de los contratistas.

Los funcionarios, contratistas y proveedores que infrinjan los requisitos contenidos en esta norma pueden estar sujetos a medidas disciplinarias, penales y administrativas según el caso, relacionadas en el dominio de incumplimiento y sanciones de la presente política.

A.18.1.3 Proteger los registros de información. Los Grupos Área Gestión TI y Grupo área Gestión Documental y Correspondencia, implementarán y mantendrán los controles necesarios para proteger la información de funcionarios, contratistas, beneficiarios, proveedores y demás terceros de los cuales reciban y administre información contra fuga de información, acceso y modificación indebida, y de conformidad con la Ley de Protección de Datos Personales.

A.18.1.4 Garantizar la Privacidad y tratamiento de información con datos personales. Se deben asegurar la privacidad y la protección de la información de datos personales, como se exige en la legislación y la reglamentación pertinentes, cuando sea aplicable. Para esto el Instituto cuenta con una política de tratamiento de datos personales, cuyo cumplimiento se debe validar anualmente por medio de auditoría externa.

Se debe mantener actualizado el registro Nacional de bases de datos, exigido por la Superintendencia de Industria y Comercio

A.18.1.5 Reglamentar el uso de controles criptográficos. Se deben reglamentar el uso controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes, como se describe en el “ARTÍCULO 11 (ANEXO A – A.10) Criptografía” de la presente política.

A.18.2. Revisiones de seguridad de la información. Se espera que La Política de Seguridad de la Información se preserve en el tiempo. Sin embargo, se debe hacer una revisión anual o ante cambios estructurales, tecnológicos y de riesgos que afecten al INC, para asegurar que éste cumple con el cambio de las necesidades de seguridad del Instituto. El líder de Seguridad de la Información es responsable por esta tarea y debe llevarla a cabo considerando los lineamientos institucionales.

A.18.2.1 Revisión independiente de la seguridad de la información. El grupo asesor de control interno debe liderar la revisión independiente del enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir, los objetivos de control, los controles, las políticas, los procesos y los procedimientos para seguridad de la información). Esta revisión debe realizarse a intervalos planificados o cuando ocurran cambios significativos.

A.18.2.2 Cumplimiento con las políticas y normas de seguridad en los Grupos Área. Los Lideres de grupo área deben revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas, y cualquier otro requisito de seguridad.

A.18.2.3 Revisión del cumplimiento técnico. El responsable de seguridad de la información, y el grupo Asesor de control interno deben asegurarse de que se revisan con regularidad los sistemas de información para determinar el cumplimiento con las políticas y normas de seguridad de la información.

Cualquier miembro del INC puede identificar la necesidad de modificar la Política de Seguridad y Privacidad de la Información. Dichas inquietudes y sugerencias deben ser comunicadas al líder de Seguridad de la Información.

Ante la necesidad de una adición o cambio a la Política, el Líder de Seguridad de la información lo realizará, y se ajustará a las medidas aprobadas por el comité de seguridad de la información del INC. La formalización de la nueva Política de Seguridad y Privacidad de la Información será realizada mediante el procedimiento establecido por la Oficina Asesora de Planeación y Sistemas.

ARTICULO 21. Administración del riesgo para la seguridad de la información. La información del INC se debe proteger con base en su valor y en el riesgo en que se pueda ver comprometida. Por lo tanto, se debe realizar periódicamente el análisis respecto al impacto en seguridad de la información para determinar o actualizar el valor relativo de la información, el nivel de riesgo a que está expuesta y el respectivo responsable.

Establecidos el nivel de riesgo y el valor de la información se debe realizar una evaluación formal de riesgos de seguridad digital para que estos sean identificados, evaluados y se apliquen las acciones necesarias para subsanarlos o mitigarlos, acorde con los niveles de riesgo permitidos por el instituto.

Cada usuario de la información debe estar enterado de la política de riesgos y los procedimientos de reporte de riesgos que puedan tener impacto en la seguridad de la información del INC, y se requiere que reporten inmediatamente cualquier sospecha u observación de un incidente a la seguridad de la información.

CAPITULO 3
DISPOSICIONES FINALES

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 Cancerologia Empresa Social del Estado

COMUNIQUESE Y CUMPLASE

Dada en Bogotá D.C. a los

CAROLINA WEISNER CEBALLOS
Directora General

Proyectó: Carlos Andrés Guerrero -Profesional Especializado I
Revisó: Jorge Orlando Neira – Asesor Jurídico
Luis Eduardo Martínez – Coordinador grupo Area Gestión TI
Comité Directivo – Acta 011 de 2019

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 siguientes líneas estratégicas del Plan de Desarrollo Institucional PDI 2019-2022:

2.1.Línea estratégica:
Línea estratégica Gestión de la Tecnología

2.2 Objetivos estratégicos:

- Planear e implementar la transformación digital del Instituto Nacional de Cancerología ESE apoyado en la gestión de la arquitectura empresarial de Tecnologías de la Información - TI.

- Optimizar la respuesta tecnológica de la institución a nivel de ingeniería clínica (equipos biomédicos y relacionados) para la atención integral del paciente con cáncer.

3.JUSTIFICACIÓN

La política de alto nivel o política general aborda la necesidad de la implementación de un sistema de gestión de seguridad de la información (SGSI) en el Instituto Nacional de Cancerología ESE, planteado desde la descripción del quién, qué, por qué, cuándo y cómo, en torno al desarrollo de la implementación del SGSI. Es así como, teniendo en cuenta la importancia que tiene que la entidad defina las necesidades de sus grupos de interés, y la valoración de los controles precisos para mantener la seguridad de la información, se establece una política de seguridad y privacidad que tiene en cuenta el marco general del funcionamiento de la entidad, sus objetivos institucionales, sus procesos misionales, y que está adaptada a las condiciones específicas y particulares de los procesos de la institución, la cual es aprobada y guiada por la Dirección.

4.OBJETIVO (S) DE LA POLÍTICA

4.1.Objetivo general

Determinar los lineamientos que permitan proteger la Información y los datos personales que adopta el INSTITUTO NACIONAL DE CANCEROLOGÍA E.S.E (INC), a través de acciones de aseguramiento de la Información teniendo en cuenta los requisitos legales, operativos, tecnológicos, de seguridad y de la institución, alineados con el contexto de direccionamiento estratégico y de gestión del riesgo con el fin de asegurar el cumplimiento de la integridad, disponibilidad, confidencialidad y legalidad de la información. La Seguridad de la Información es una prioridad para el INC, por lo tanto, es responsabilidad de todos los funcionarios y contratistas de la Entidad vigilar por el continuo cumplimiento de las políticas definidas.

4.2. Objetivos específicos

El INSTITUTO NACIONAL DE CANCEROLOGÍA E.S.E (INC), para asegurar el cumplimiento de su misión, visión, y objetivos estratégicos alineados a sus valores institucionales, establece la compatibilidad de la política de seguridad de la información y los objetivos de seguridad de la información, estos últimos correspondientes a:

- Minimizar el riesgo de los procesos misionales de la entidad.
- Prevenir el daño antijurídico.
- Cumplir con los principios de seguridad de la información.

- Mantener la confianza de los funcionarios, contratistas y terceros.
- Apoyar la innovación tecnológica.
- Apoyar la interoperabilidad segura de la información entre entidades
- Implementar el sistema de gestión de seguridad de la información.
- Proteger los activos de información.
- Establecer los procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los servidores públicos, funcionarios, contratistas, estudiantes, pasantes, especialistas en entrenamiento, personal de proveedores, terceros y clientes del INC.
- Garantizar la continuidad del negocio frente a incidentes después de una interrupción no deseada o desastre.

5. DECLARACION GENERAL DE LA POLITICA

El INSTITUTO NACIONAL DE CANCEROLOGIA E.S.E garantizará la seguridad y privacidad de su información, realizando cumplimiento de la norma ISO27001:2013. Como consecuencia de lo anterior, tanto responsables como encargados, acogerán íntegramente esta política enmarcada dentro del sistema de Gestión de Seguridad de la Información (SGSI) de la entidad, junto con las obligaciones y procedimiento que de aquí se desprendan, velando por la implementación de esta al interior de la entidad, divulgando su contenido y efectos entre su personal, es decir, entre sus subordinados o dependientes (operadores), y vigilando su cumplimiento. Todo ello, en garantía de la confidencialidad, integridad y privacidad de la información de acuerdo con las disposiciones legales anteriormente citadas.

6. DESARROLLO DE LA POLITICA

6.1. Alcance

Esta política aplica a todo el Instituto Nacional de Cancerología ESE, sus funcionarios, contratistas, terceros, colaboradores y ciudadana en general, así como a todos los activos de información, servicios, procesos, las tecnologías de información incluida el hardware y el software, instalaciones y demás herramientas utilizadas por la entidad en el ejercicio de sus funciones.

6.2. Cumplimiento

Todas las personas cubiertas por el presente alcance, y las que se encuentran identificadas en el “Manual de políticas de seguridad y privacidad de la información” deberán dar cumplimiento un 100% de la política.

6.3. Declaraciones específicas de la política

La política de seguridad de la Información del INC establece que:

- El INC dará cumplimiento a los lineamientos de la Estrategia de Gobierno en Digital respecto a la Seguridad de la Información.
- Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, colaboradores, contratistas, proveedores, o terceros.
- El INC protegerá la información generada, procesada o resguardada por los procesos institucionales, su infraestructura tecnológica y activos del riesgo que se genera de los accesos otorgados a terceros (ej.: proveedores o clientes), o como resultado de un servicio interno en outsourcing.
- El INC protegerá la información creada, procesada, transmitida o resguardada por sus procesos institucionales en físico o digital, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta.

- El INC debe implementar los controles necesarios para dar manejo a los riesgos detectados en su Gestión de riesgos de Seguridad digital, y proveerá un nivel de protección de la información apropiado y consistente. El listado de controles que mitigan, evitan o transfieren los riesgos de seguridad de la información se encuentra consolidado en el formato de Declaración de Aplicabilidad con el fin dar cumplimiento a lo requerido en la Norma ISO 27001:2013.
- EL INC protegerá su información de las amenazas originadas por parte del personal.
- El INC ejecutará un plan de capacitación y sensibilización en seguridad de la información para que todos sus funcionarios, colaboradores, contratistas y terceros estén comprometidos con el uso adecuado de los activos de información, el cumplimiento de controles de seguridad y la medidas higiene de seguridad informática en la realización de sus funciones y actividades.
- EL INC protegerá las instalaciones de procesamiento y la infraestructura tecnológica física que soporta sus procesos críticos.
- EL INC controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.
- El INC implementará control de acceso a la información, sistemas y recursos de red.
- EL INC garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
- El INC garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.
- EL INC garantizará la disponibilidad de sus procesos institucionales y la continuidad de su operación basada en el impacto que pueden generar los eventos.
- EL INC garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.
- El INC informará a los terceros sobre la presente política de Seguridad de la Información y vigilará por su observancia en todos los actos jurídicos que suscriban con la entidad
- El INC protegerá los datos personales recolectados en ejercicio de sus actividades de acuerdo con la Ley 1581 de 2012 y la Ley 1755 de 2015 0 las normas que la modifiquen o adicionen.
- EL INC protegerá su infraestructura que identifique como critica para la Ciberdefensa y Ciberseguridad del Estado Colombiano.

6.4. Implementación

La política de Seguridad y Privacidad de la Información se desarrolla mediante el “Manual de políticas seguridad y privacidad de la información”, y se implementa mediante el “Plan de seguridad y privacidad de la información”, que se encuentran publicados en el portal web institucional cancer.gov.co

6.5. Indicadores

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

- Porcentaje de acciones realizadas para el tratamiento de programas maliciosos
- Porcentaje de disponibilidad del sistema SAP
- E-Disponibilidad de los Sistemas de información (7x24)
- Proporción de riesgos Tratados del proceso GTI.
- Porcentaje de actualizaciones críticas aplicadas y liberadas en el mismo periodo.
- Porcentaje de eventos e incidentes solucionados antes de una hora relacionados con la seguridad de la información.
- Porcentaje de implementación del plan de seguridad y privacidad de la información FASE II.

6.4. Revisión de la política

La Política de seguridad y privacidad de la información se debe revisar a intervalos planificados de 1 año, o cada vez que ocurran cambios significativos, para asegurar su conveniencia, adecuación y eficacia continúas

7.ANEXOS

Anexo 1 - Manual de Políticas de Seguridad y Privacidad de la información
Anexo 2 - Declaración de Aplicabilidad de controles de seguridad de la información

8. CONTROL DE ACTUALIZACIÓN DE LA POLÍTICA

Versión	Fecha de la actualización	Descripción de la actualización
3	23 de noviembre de 2020	Se separa Política General de Seguridad de la información de Manual de Políticas de Seguridad y privacidad. Se relacionan indicadores. Se referencia formato de Declaración de Aplicabilidad de controles, Se Agrega sección de implementación. Se Agregan ítems a las Declaraciones específicas de Política.

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 politica, 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

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:	22-09-2020	Fecha:	23-09-2020	Fecha:	23-09-2020