PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

GESTION DE LA TECNOLOGÍA

GRUPO ÁREA DE SISTEMAS

INSTITUTO NACIONAL DE CANCEROLOGÍA ESE

2018

TABLA DE CONTENIDO

1. OBJETIVOS

El presente documento se enmarca dentro de la política establecida por el Gobierno Nacional que pretende la inclusión social y la competitividad a través de la apropiación y el usos de las Tecnologías de la Información y las Comunicaciones (TIC), tanto en la vida cotidiana como productiva de los ciudadanos, empresas, academia y estado. Su desarrollo se ha enmarcado dentro de la Estrategia de Gobierno en Línea que contribuye a la construcción de un Estado eficiente, transparente, participativo y que preste mejores servicios a los ciudadanos.

El Plan de tratamiento de riesgos de seguridad y privacidad de la información define las estrategias del Instituto nacional de Cancerología en cuanto a la identificación, valoración, mitigación y monitoreo del riesgo con el fin de controlar y salvaguardar sus activos de información durante todo el ciclo de vida dentro y fuera del INC.

2. ALCANCE

Estructurar el plan de trabajo de tratamiento de riesgo de seguridad y privacidad de la información para los procesos críticos del INC, validando los recursos con los que se cuentan actualmente en el instituto, y alineándolo a las metodologías DAPF e ISO respectivamente en seguridad y riesgo de la información. El alcance limita al proyecto en el primer año a la revisión de controles como base para la ejecución del plan de seguridad y privacidad de la información, la implantación del SGSI, y la formalización de planes de contingencia (DRP) y para segundo año se amplía el alcance para desarrollar un análisis de impacto de negocio (BIA) y la construcción del plan de continuidad de negocio.

3. NORMATIVIDAD

Decreto 612 de 2018: Por el cual se fijan las directrices para la integración de los planes institucionales y estratégicos al plan de acción por parte de las entidades del estado.

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.

Ley Estatutaria 1581 de 2012 y Reglamentada Parcialmente por el Decreto Nacional 1377 De 2013: Por la cual se dictan disposiciones generales para la protección de datos personales

Decreto 2693 de 2012: Lineamientos generales de la Estrategia de Gobierno en línea de la República de Colombia que lidera el Ministerio de las Tecnologías de Información y las Comunicaciones, se reglamentan parcialmente las Leyes 1341 de 2009 y 1450 de 2011, y se dictan otras disposiciones.

Decreto 2578 de 2012: Por medio del cual se reglamenta el Sistema Nacional de Archivos. Incluye “El deber de entregar inventario de los documentos de archivo a cargo del servidor público, se circunscribe tanto a los documentos físicos en archivos tradicionales, como a los documentos electrónicos que se encuentren en equipos de cómputo, sistemas de información, medios portátiles” entre otras disposiciones.

Decreto 2609 de 2012: Por medio del cual se reglamenta el Título V de la Ley General de Archivo del año 2000. Incluye aspectos que se deben considerar para la adecuada gestión de los documentos electrónicos.

Ley 1437 de 2011: Por la cual se expide el Código de Procedimiento Administrativo y de lo Contencioso Administrativo**.**

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

Ley 1341 DE 2009: Por medio de la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la información y comunicaciones - TIC, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones.

Ley 1150 DE 2007: Por medio de la cual se introducen medidas para la eficiencia y la transparencia en la Ley 80 de 1993 y se dictan otras disposiciones generales sobre la contratación con Recursos Públicos contenidos de la norma

ISO/IEC 27001:2013: Es la evolución certificable del código de buenas prácticas ISO 17799. Define cómo organizar la seguridad de la información en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande. Es posible afirmar que esta norma constituye la base para la gestión de la seguridad de la información

Ley 962 DE 2005: Por la cual se dictan disposiciones sobre racionalización de trámites y procedimientos administrativos de los organismos y entidades del Estado y de los particulares que ejercen funciones públicas o prestan servicios La elaboración de la política de seguridad informática, está fundamentado bajo las normas: ISO/IEC 27001:2005. Information technology - Security techniques - Information security management systems - Requirements

4. GLOSARIO

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

Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC 27000).

Activo de Información: En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controlar en su calidad de tal.

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

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

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

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

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

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

Ciberseguridad: Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701).

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

Control: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

Datos Abiertos: Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos (Ley 1712 de 2014, art 6).

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

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

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

Datos Personales Mixtos: Para efectos de esta guía es la información que contiene datos personales públicos junto con datos privados o sensibles.

Datos Personales Sensibles: Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y

garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos. (Decreto 1377 de 2013, art 3).

Declaración de aplicabilidad: Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información – SGSI, de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001. (ISO/IEC 27000).

Derecho a la Intimidad: Derecho fundamental cuyo núcleo esencial lo constituye la existencia y goce de una órbita reservada en cada persona, exenta de la intervención del poder del Estado o de las intromisiones arbitrarias de la sociedad, que le permite a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural (Jurisprudencia Corte Constitucional).

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

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

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

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

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

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

Privacidad: En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de GEL la correlativa obligación de proteger dicha información en observancia del marco legal vigente.

Responsabilidad Demostrada: Conducta desplegada por los Responsables o Encargados del tratamiento de datos personales bajo la cual a petición de la Superintendencia de Industria y Comercio deben estar en capacidad de demostrarle a dicho organismo de control que han implementado medidas apropiadas y efectivas para cumplir lo establecido en la Ley 1581 de 2012 y sus normas reglamentarias.

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

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

Seguridad de la información: Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).

Sistema de Gestión de Seguridad de la Información SGSI: Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).

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

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

5. SITUACION ACTUAL

El instituto nacional de Cancerología se encuentra en etapa de planeación para la implementación del Sistema de gestión de seguridad de la información SGSI, que es uno de los lineamientos estratégicos claves que el INC debe adoptar teniendo en cuenta su visión como un proceso, ya que se realiza de manera transversal a varios procesos por su impacto en los mismos. Para apoyar este objetivo el INC realizo en junio de 2018 la contratación del Oficial de seguridad de la información, con el fin de tener el recurso humano adecuado con el conocimiento, la experiencia y la disponibilidad para logar el éxito del proyecto.

El INC tiene definida y operativa la metodología de gestión del riesgo emitida por el DAFP, por lo que la integración con MSPI (SGSI) se podrá realizar de manera natural y adecuada. Los ejercicios de identificación y tratamiento de riesgo se encuentran liderados por el área de calidad, mientras que la identificación y activos de información se encuentra liderados por el área de gestión Documental.

EL INC realizo su último ejercicio de identificación y clasificación de activos de información, y análisis de riesgos para todos sus procesos estratégicos, misionales y de apoyo en diciembre de 2017, el cual tiene una frecuencia de revisión anual. Como resultado se cuentan con 14 matrices de identificación de riesgo, una por cada proceso del Instituto.

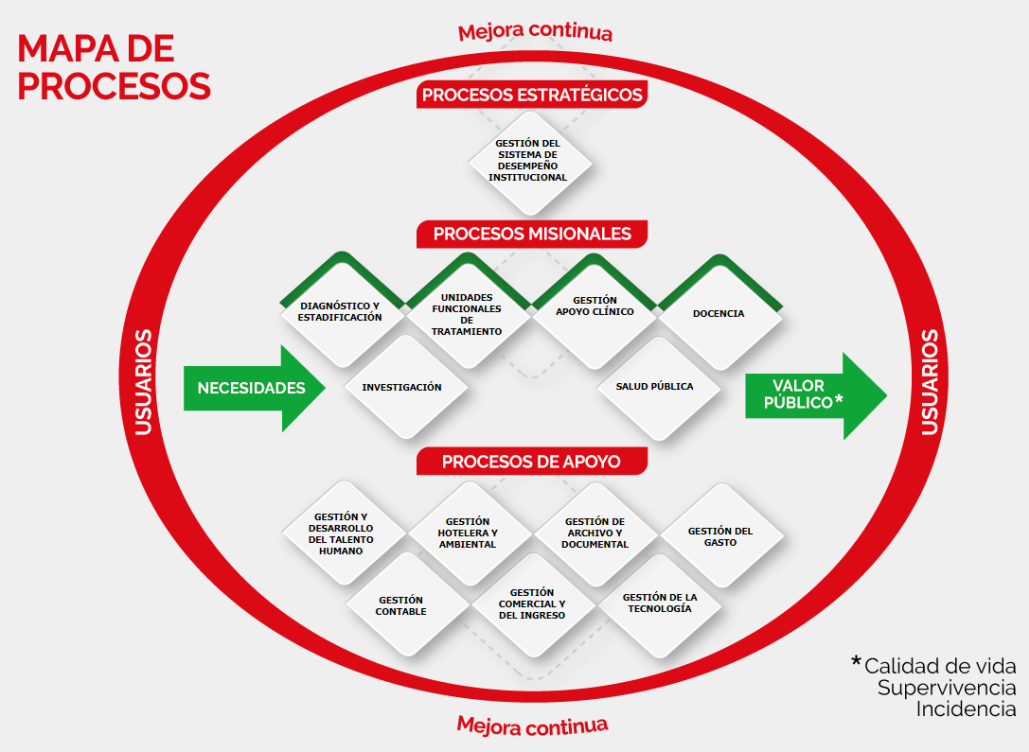

Imagen 1. Mapa de procesos del INC

Las matrices de riesgo actualmente no incluyen riesgos de seguridad y privacidad de la información para los procesos operativos misionales. Se evidencia análisis de riesgos operativos, de corrupción y solo en algunos casos de tipo tecnológico.

Los controles para mitigación de riesgo identificados dentro del proceso de apoyo de tecnología, y en conjunto con la política y manual de seguridad de la información fueron determinados e implantados de acuerdo a la norma ISO 27001:2005 por lo que se requiere una actualización a la norma ISO-27001:2013 y guías del MSPI de MINTIC.

La responsabilidad de identificación y administración de los riesgos de seguridad física sobre activos de información recaen sobre tres áreas distintas: Gestión Hotelera, Infraestructura y Vigilancia. El área de tecnología solo se encarga de la cobertura de riesgos de seguridad física sobre datacenter y equipos de cómputo. Se observa una baja cobertura para sistemas de detección y extinción de incendio, y CCTV.

La entidad cuenta con una póliza colectiva de seguros que cubre todos los activos propiedad de INC, pero no cuenta con una póliza de riesgo tecnológico para cubrir eventos sobre seguridad de la información y continuidad de negocio. El outsorcing de redes y tecnología cuenta con el cubrimiento de su propia póliza para los activos que pone a disposición para el INC.

En cuanto al cumplimento de la ley 1581 de 2012 y el decreto regulatoria 1377 de 2017 sobre protección de datos personales, el INC no ha formalizado el registro de bases de datos de información personal ante la SIC pero es consciente de la importancia del tratamiento de privacidad de sus activos de información por lo cual contrató una consultoría con la empresa Álzate y Asociados. La consultoría se encuentra en estado de planeación.

6. METODOLOGIA DE IMPLEMETACION

La implantación del plan de riesgo de seguridad y privacidad de la información se dividirá en (3) fases:

1era Fase: Diagnostico
En esta fase se realizara la ejecución de una consultoría externa para evaluar el estado actual del instituto e materia de protección de datos. El consultor, en conjunto con las áreas de Gestión documental y seguridad de la información evaluaran la completitud de los activos de información de los procesos, se ajustaran las tablas de retención de la información, y se diseñaran los manuales y clausulas y contratos requeridos. A la par de la consultoría el oficial de seguridad de la información realizara la identificación y levantamiento de amenazas y vulnerabilidades, y la documentación de los controles actuales implantados sobre los activos de información para todos los procesos.

2da Fase: Identificación y evaluación de riesgos de seguridad y privacidad de la información.

a) **Identificación y evaluación de riesgos de Tecnología:** Se evaluaran y se trataran los riesgos de seguridad del proceso de apoyo de tecnología, el cual tendrá una mayor visibilidad debido a que se valoraran los controles implantados de seguridad de la información, orientados al cumplimiento de la norma ISO27001:2013 y MSPI, para los principales contenedores de información que corresponden a los datacenter y a los sistemas de información misionales, bases de datos, redes y comunicaciones, y relación con los proveedores.

b) **Identificación y evaluación de riesgos de Procesos:** Se evaluaran y se trataran los riesgos de seguridad y privacidad inherentes al flujo de activos de información para cada uno de los 13 procesos restantes, enfocados en la identificación de los principales riesgos que afecten la triada de seguridad, y haciendo énfasis en la confidencialidad de la información de los pacientes.

c) **Aprobación de tratamiento de riesgos:** Se conseguirá aprobación del plan de tratamiento de riesgo y controles seleccionados por los dueños de cada proceso, y la aprobación de riesgo residual por el comité de riesgo y la dirección de INC. Luego se consolidaran los riesgos y su tratamiento en el formato **GSI-P07-F-02 Mapa de riesgo institucional** integrándose completamente con los sistemas de gestión, calidad y planeación del INC.

3ra Fase: Implementación y Comunicación

En fase ocurre la revisión y el despliegue de los controles aceptados sobre los activos de información, y el establecimiento de monitoreo y la revisión y redefinición de indicadores de seguridad de la información. En los casos necesarios se realiza acompañamiento y verificará la modificación de los flujos de información en los procesos operacionales con los líderes de áreas, y finalmente se ejecutan los planes de capacitación y concienciación en seguridad de la información para todo el personal del INC.

La última fase de mejora continua correspondiente al ciclo PVHA no se incluye dentro del plan de tratamiento de riesgo, sino que se incluye como un componente integrado en el Plan de seguridad y privacidad de la información.

7. CRITERIOS Y METODOLOGÍA DE EVALUACIÓN DE RIESGO.

Los criterios de evaluación de riesgo, criterios de impacto y criterios de aceptación del riesgo del Instituto Nacional de Cancerología están definidos en la guía **GSI-P07-I-01 INSTRUCTIVO PARA LA IDENTIFICACIÓN, ANÁLISIS, EVALUACIÓN, TRATAMIENTO, MONITOREO Y SEGUIMIENTO DE RIESGOS EN EL INSTITUTO NACIONAL DE CANCEROLOGÍA** y en la guía **GSI-P07-I-02 INSTRUCTIVO DE DILIGENCIAMIENTO DE LA**

MATRIZ PARA EL LEVANTAMIENTO DEL MAPA DE RIESGOS POR PROCESO Y DE CORRUPCIÓN. Las guías para la administración del riesgo del DAFP (Departamento Administrativo de la Función Pública) y la guía para la Gestión del Riesgos de Corrupción 2015, son las normas de referencia adoptadas por el Instituto

La metodología de valoración de riesgos de seguridad y privacidad en INC consta de 5 pasos y se describe a continuación:

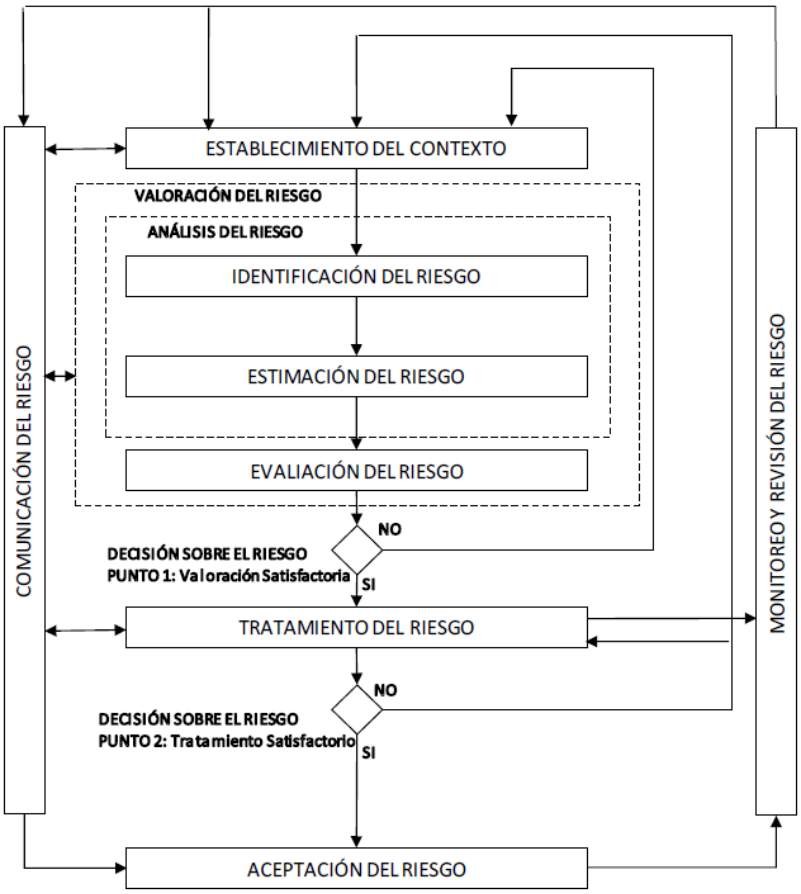

Imagen 2. NTC-ISO 31000 Metodología proceso de gestión de riesgo

7.1 Identificación del riesgo (Frecuencia Anual)

Tiene como principal objetivo conocer las fuentes de los riesgos, sus causas con base en los factores internos y/o externos y sus consecuencias. Para la identificación de los riesgos se realizan las siguientes actividades:

- Programar reunión de trabajo con los líderes de los procesos y/o coordinadores de grupo área o su designado y dejar constancia en SIAPINC, o en su defecto el formato de acta institucional **GSI-P02-F-21 Acta institucional**.
- Identificar y escribir los posibles hechos o amenazas de seguridad y privacidad (lo que puede suceder) que podrían generar consecuencias no deseadas para para cada activo de información identificado en la operación del proceso.

- Determinar las causas internas y externas, aplicando metodología de análisis causal como las que se mencionan a continuación con el fin de establecer el origen del riesgo.

  - Lluvia de Ideas
  - Cinco (5) Porqués?
  - Diagrama de espina de pescado (**Ishikawa**)
  - Protocolo de Londres
  - Otra, de ser necesario.

- Definir los posibles efectos o consecuencias de materializase los riesgo de seguridad y privacidad (Lo que podría ocasionar).

7.2 Análisis y evaluación de los riesgos (Frecuencia Anual)

Realizar calificación según los 4 criterios que se encuentran en la matriz **"GSI-P07-F-01 Matriz Para El Levantamiento del Mapa de Riesgos Por Proceso y de Corrupción",** (acción u omisión, uso del poder, desviación de la gestión de lo público y beneficio privado) y diligenciándolo según el **"GSI-P07-I-02 Instructivo Para El Diligenciamiento De La Matriz Para El Levantamiento Del Mapa De Riesgos Por Proceso Y De Corrupción"** para determinar si el riesgo de seguridad y privacidad es de proceso o de corrupción.

- Realizar la descripción características generales o las formas en que se observa o manifiesta cada uno de los riesgos de seguridad y privacidad identificados.

- Realizar análisis y determinando la calificación de los riesgos de seguridad y privacidad de la información teniendo en cuenta las variables de probabilidad e impacto, basándose en las tablas de criterios de análisis riesgos por proceso y por corrupción que se encuentra en la matriz **"GSI-P07-F-01 Matriz Para El Levantamiento Del Mapa De Riesgos Por Proceso y de Corrupción".**

- Cuando el riesgo sea de **corrupción** aplique las 17 preguntas que se encuentran en la matriz en la etiqueta denominada **"Formato para determinar el impacto en corrupción**" y según el resultado califique el impacto en la etiqueta Análisis-Evaluación diligenciándolo según el **"GSI-P07-I-02 Instructivo Para El Diligenciamiento De La Matriz Para El Levantamiento Del Mapa De Riesgos Por Proceso Y De Corrupción"**

- Establecer el tipo de impacto por categoría y subcategoría, según las características del riesgo definidas en la identificación; teniendo en cuenta la clasificación del riesgo previamente realizada y que se relacionan con las consecuencias potenciales del riesgo identificado.

La matriz mostrara automáticamente la zona de riesgo y la posición en la gráfica antes de controles.

- Registrar los controles de seguridad que se ejecutan en la actualidad (máximo 3 principales) y valorarlos según el **"GSI-P07-I-02 Instructivo Para El Diligenciamiento De La Matriz Para El Levantamiento Del Mapa De Riesgos Por Proceso Y De Corrupción**".

La matriz mostrara automáticamente los campos de calificación del control, control del riesgo y control del proceso.

- Realizar la valoración del riesgo, teniendo como base los controles anteriormente descritos y establezca si con los controles mitigan la posibilidad de ocurrencia (Probabilidad) o las consecuencias (Impacto) si se materializara.

7.3 Tratamiento del riesgo

Se tratarán los riesgos extremos y los altos en primer lugar, a los riesgos moderados y bajos se les realizarán seguimiento.

- Establecer la medida de mitigación de acuerdo al listado de controles ANEXO A de la Norma ISO 27001:2013, determinando las opciones de tratamiento del riesgo así:

  - **Zona de riesgo baja:** asumir el riesgo
  - **Zona de riesgo moderada:** asumir el riesgo, reducir el riesgo
  - **Zona de riesgo alta:** reducir el riesgo, evitar, compartir o transferir
  - **Zona de riesgo extrema:** reducir el riesgo, evitar, compartir o transferir

- Definir la acción clasificándola en corrección, acción preventiva o acción Correctiva
- Establecer el producto o meta generado de la ejecución de la acción.
- Establecer el tiempo de inicio y de terminación de la ejecución de la acción.
- Definir el responsable de la implementación de las acciones de tratamiento y del seguimiento a los controles.
- Definir el indicador y la medida del indicador. Puede utilizar indicadores que se encuentran creados o crear uno según su pertinencia.
- Elaborar el plan de tratamiento para aquellos riesgos que quedaron en zona alta o extrema posterior a los controles en el SIAPINC.
- Aprobar el plan de tratamiento de riesgo y la aceptación de riesgo residual por la Dirección de INC y Comité de seguridad de la información.

7.4 Monitoreo y seguimiento

La periodicidad de seguimiento de acuerdo a los niveles de riesgo residual, serán realizados de la siguiente manera:

- Los riesgos determinados como extremos y altos se les realizará monitoreo y seguimiento cada 4 meses sobre los controles operacionales y de seguridad de la información de los procesos, y se recomienda un monitoreo a controles del proceso de tecnología de tipo diario a mensual dependiendo de la importancia del control o del activo de información , con seguimiento específico mensual dejando evidencia de dicha verificación en la matriz en el campo de “seguimientos trimestral y monitoreo líder proceso, la oficina de control interno realiza seguimiento a los mapas de riesgos de los procesos y evalúa la efectividad de los controles dejando como evidencia en formato GSI-P10-F-12.
- Los riesgos determinados como moderados y bajos se les realizará monitoreo para procesos de operación una vez cada año con enfoque principal de seguimiento a los controles, y se recomienda un seguimiento semestral en específico para el proceso de tecnología también dependiendo de la importancia del control y del activo.
- El responsable de la implementación de las acciones de tratamiento y/o el líder del proceso debe hacer seguimiento al Plan de mejora de tratamiento a riesgos de ser necesario, cargue al SIAPINC la

información necesaria que evidencie la ejecución de las acciones propuestas para tratar los riesgos en zona alta o extrema.

- Verificar e informar aquellos riesgos que se materialicen. Los incidentes o eventos se registraran en el aplicativo de mesa de ayuda, según el manual de incidentes de seguridad del outsourcing de helpdesk (COLSOFT), y se dispone de una bitácora ampliada para construir una base de conocimiento específica para el análisis y mejora en seguridad de la información.

.

8. STAKEHOLDERS Y RECURSOS

Se identifican los siguientes stakeholders para el plan de tratamiento de riesgos y privacidad de la información

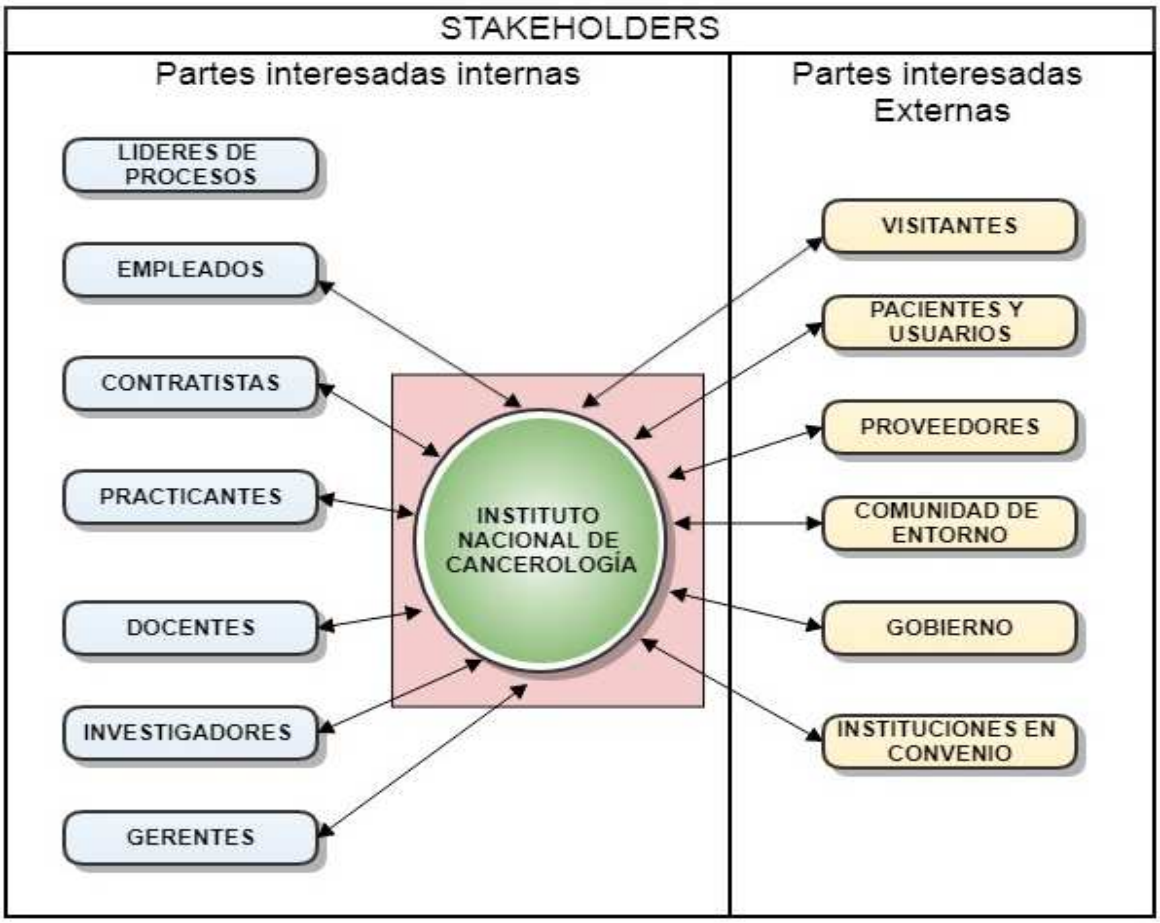

Imagen 3. Identificación de stakeholders para plan de tratamiento de riesgo

Para la ejecución de dicho plan se requieren los siguientes **Recursos Humanos** por fase de proyecto:

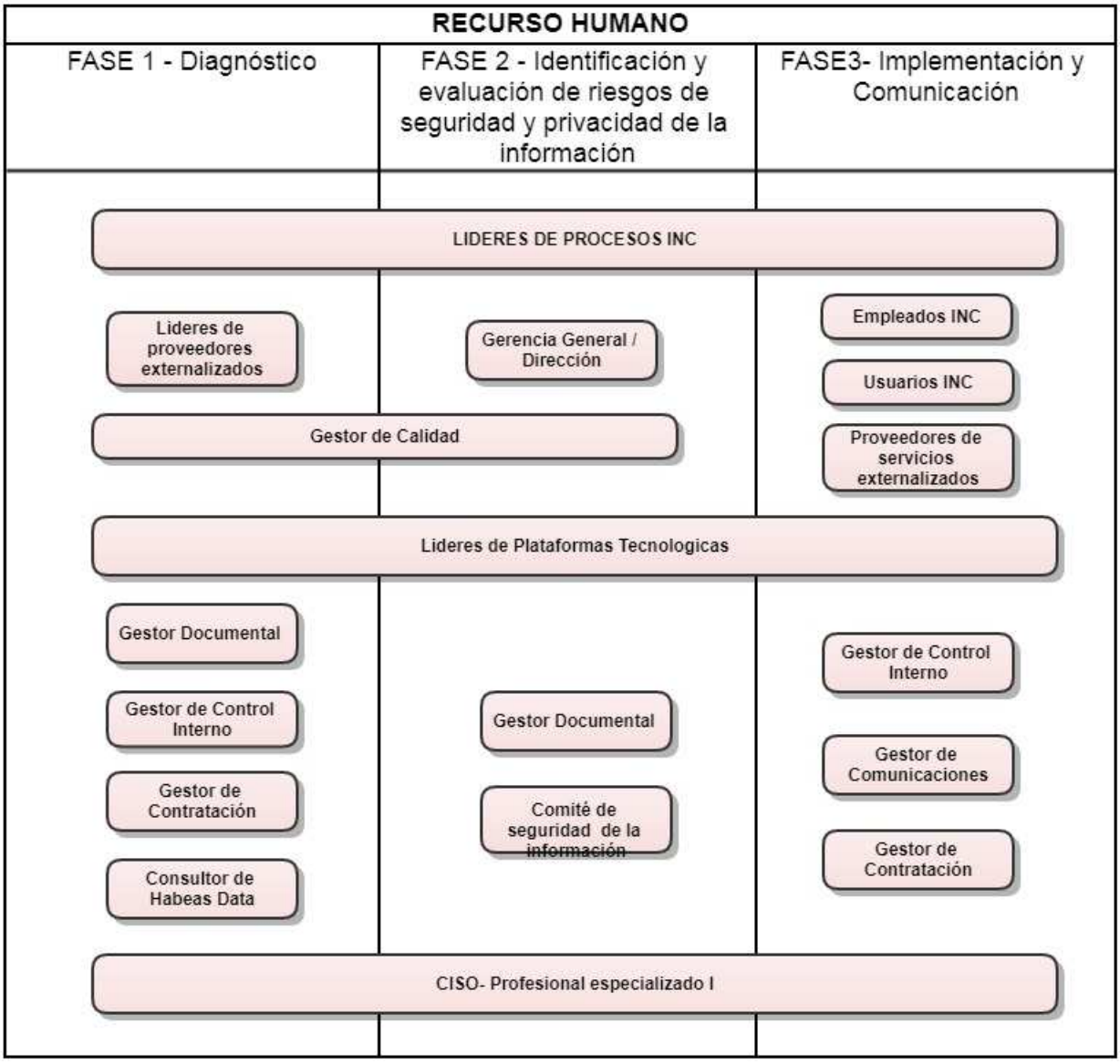

Imagen4. Recursos Humano necesario para plan de tratamiento de riesgo

Para la ejecución de dicho plan se requieren los siguientes **Recursos Físicos** y documentales por fase de proyecto:

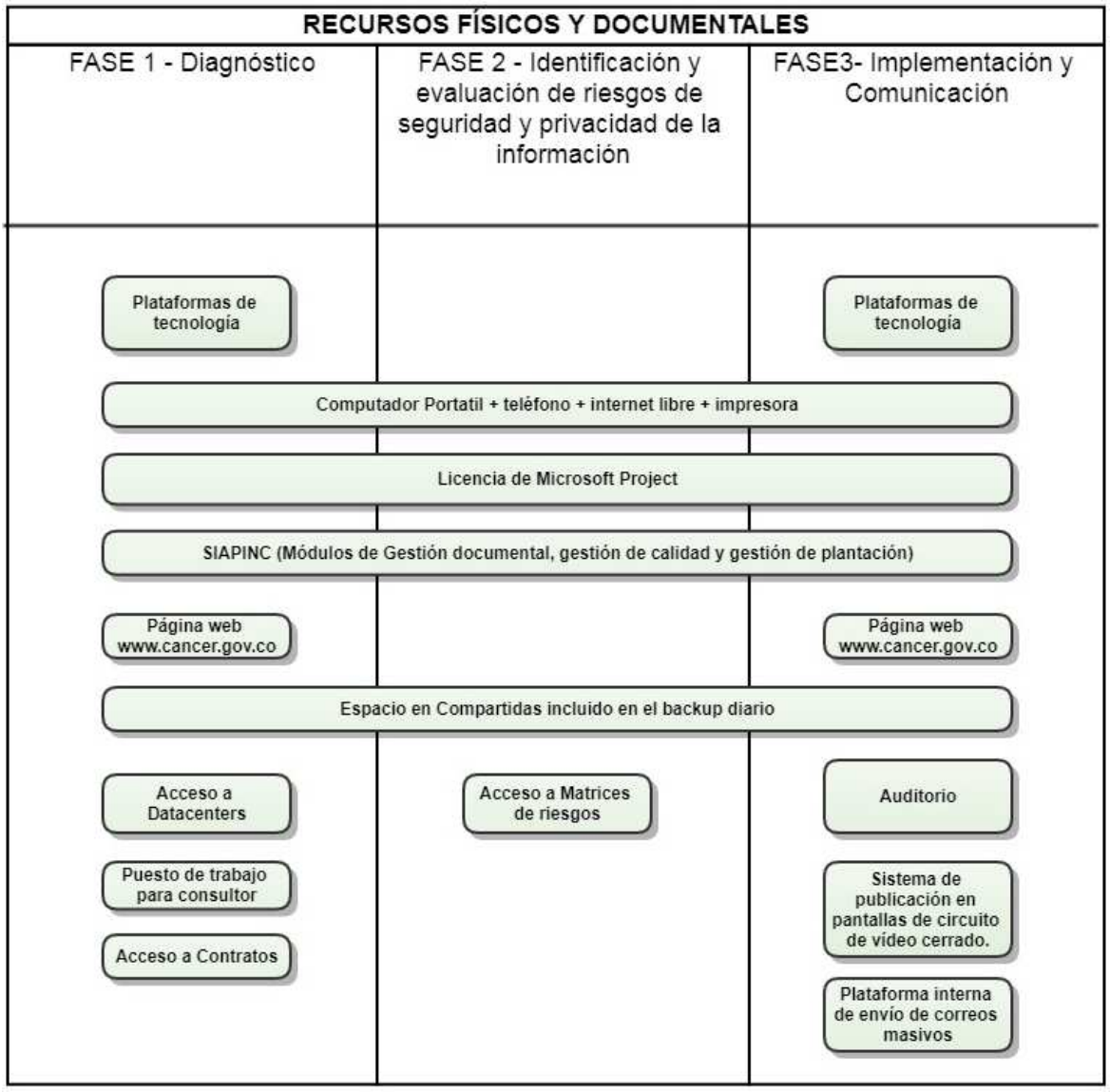

Imagen 5. Recursos Físicos y documentales necesarios para plan de tratamiento de riesgo

Para la ejecución de dicho plan se requieren inicialmente los siguientes **Recursos Financieros** para la ejecución del proyecto:

ITEM	Capacidad	Tipo de Soporte	Valor Mensual	Valor Anual
Oficial seguridad de la información	N/A	N/A	$ 5.200.000,00	$ 96.096.000,00
Consultoría protección de datos personales	N/A	N/A	N/A	$ 15.624.819,00
TOTAL				**$ 111.720.819,00**

Imagen 6. Recursos Físicos y documentales necesarios para plan de tratamiento de riesgo

En la tercera fase de implementación del plan de tratamiento de riesgos el comité de riesgo puede determinar la asignación de un presupuesto adicional para la mitigación de riesgo en el caso de que sean necesarias herramientas adicionales de seguridad, nuevos controles o cambios en los controles actuales que requieran inversión. El resultado de la tercera fase es la aprobación de los riesgos a ser tratados y el presupuesto que se requiere para alcanzar este objetivo. El presupuesto de controles se incluye en el plan se seguridad y privacidad de la información del INC.

9. CUMPLIMIENTO DE IMPLEMENTACIÓN

De acuerdo a las fases mencionadas anteriormente, se describe a continuación los dominios que se deben desarrollar y los plazos de implementación de acuerdo a lo establecido por el INC.

- Gestión de Activos de Información
- Análisis de Riesgos de Seguridad de la Información
- Arquitectura de Seguridad (En sitio y en la nube)
- Relación con Proveedores
- Seguridad Física y ambiental
- Seguridad de las Operaciones
- Seguridad de los Recursos Humanos
- Seguridad de las Comunicaciones
- Control de Accesos
- Criptografía

10. CRONOGRAMAS

Fases 1 y 2 - Año 2018 (Diagnostico, identificación y valoración de riesgo de seguridad y privacidad)

Sub-Proceso	MSPI (Mintic)	Dominio ISO 27001:2013	Actividad	Responsable	Avan	Julio				Agosto				Septiem				Octubre				Noviemb				Diciembr			
						1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
	GUIA 5	8. Gestión de Activos de Información	Actualizar el procedimiento definido para la identificación y gestión de activos de información	CISO, CALIDAD	0																								
			Actualizar el Inventario de Activos de Información y clasificación (anual nov-dic2018)	GESTION DOCUMENTAL, CISO	0																								
	GUIA 7 Y 8	Análisis de Riesgos de Seguridad de la Información	Actualizar el procedimiento para la Gestión de Riesgos de INC incluyendo el analisis de riesgo de seguridad de la informacion para cada uno de los procesos operativos .	CISO, GESTOR DE CALIDAD	0																								
			Realizar el análisis de riesgos de Seguridad de la Información, identificados por el area de calidad, definiendo oportunidades de mejora en los controles implementados o definición de nuevos.	CISO, GESTOR DE CALIDAD	0																								

Fase 3. Implementación y Comunicación año 2018

Sub-Proceso	MSPI (Mintic)	Dominio ISO 27001:2013	Actividad	Responsable	Avan	Julio				Agosto				Septiem				Octubre				Noviemb				Diciembr			
						1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
Gestión de Riesgos de Seguridad de la Información	GUIA 11	Arquitectura de Seguridad (En sitio y en la nube)	Definir el procedimiento para la arquitectura de Seguridad de la Información	CISO,ARQUITECTO EMPRESARIAL	0																								
			Crear la matriz de arquitectura de red segura	CISO,ARQUITECTO EMPRESARIAL																									
			Validar y documentar arquitectura y controles de servcio de datacenter para DRP en la nube con TIVIT. (Acceso , cifrado, datos en transito, monitoreo)	CISO,ARQUITECTO EMPRESARIAL, PROVEEDOR	0																								
	GUIA 15	A15. Relación con Proveedores	Revisar y ajustar politicas de contratacion, acuerdos de privacidad y confidencialidad establecidos con los suministradores	CISO, GESTION CONTRACTUAL	0																								
			Revisar y ajustar contoles de cambios en el suministro de servico por parte de los proveedores	CISO, GESTION CONTRACTUAL	0																								
			Definir plan de entrevistas de Seguridad de la Información a los proveedores críticos para la	CISO, CONTROL INTERNO	0																								
	GUIA 3 (Procedimientos) GUIA 8 (Controles)	A.11 Seguridad Fisica y ambiental	Evaluar situacion actual de seguridad fisca y ambiental para areas seguras y equipos	CISO,GESTION ADMINISTRATIV	0																								
			Crear el procedimiento para Seguridad física y del entorno	CISO	0																								
			Obtener Certificados ISAE o de audiotria ISO 27001:2013 del proveedor de datacenter, y en su defecto programar y ejecutar auditorias internas a datacenter	CISO, CONTROL INTERNO	0																								
			Analizar y validar los controles implementados a nivel de Seguridad fisica y ambiental, dando cumplimiento a la norma ISO 27001:2013	CISO, VIGILANCIA, GESTION ADMINISTRATIVA, RECURSOS	0																								
			Revisar y ajustar controles establecidos sobre equipos de computo y cableado.	CISO	0																								
			Establecer, configurar y promover politicas de escritorio y pantalla limpia	CISO																									
		A.12 Seguridad de las Operaciones	Afinamiento y administración en la configuración de las herramientas de Seguridad para mejorar y oprtimizar el monitoreo	CISO	0																								
			Valida toma y resplado de logs para sistemas de infromación y plataformas criticas, y toma de logs de auditoria para roles de usuarios administadores y operadores de sistemas	CISO	0																								
			Evaluar proyecto sobre herramienta para analisis de log y correlacion de eventos	CISO,COORDINADOR DE AREA	0																								
			Revisar y ajustar procedimiento de backup , frecuencias de backup y pruebas periodicas de medios de backup	CISO	0																								
			Programar y acordar la ejecución de pruebas de vulnerabilidades y hacking ético	CISO	0																								
			Validar separcion de entornos de desarrollo de sistemas de infromacion, con sus correspondientes roles y permisos, logs y manejo de data de prueba	CISO, COODINADOR DE	0																								
			Validar controles de instalacion de software y restricciones de herramientas system 32 en equipos de computo	CISO	0																								
			Asegurar Sincronizacion de relojes para servidores y equipos de computo	CISO	0																								
	GUIA 3	A.7 Seguridad de los Recursos Humanos	Analizar y validar los controles implementados a nivel de Seguridad de los Recursos Humanos, dando cumplimiento a la norma ISO 27001:2013.	CISO, RRHH	0																								
			Modificar los procedimientos para la Seguridad de los Recursos Humanos , antes y durante la contratacion, y al cese o cambio de puesto de trabajo	CISO, RRHH	0																								
	GUIAS 19 Y 20	A.13 Seguridad de las Comunicaciones	Crear la politica y el procedimiento para la Seguridad de las redes y las Comunicaciones	CISO	0																								
			Revisar la arquitectura de red de la Entidad para identificar oportunidades de mejora	CISO, COORDINADOR DE AREA DE	0																								
			Evaluar proyecto para administracion segura de puertos de red y aplicación de politicas BYOD	CISO, COORDINADOR DE AREA DE	0																								
			Evaluar proyecto de implantacion de herramientas IDS, IPS y WAF para deteccion y restricción proactiva de trafico sospechoso de red y portal web	CISO, LIDER DE REDES	0																								
			Realizar revisión y emitir la politica y recomendaciones para la transferencia de	CISO	0																								
			Identificar riesgos y requerimientos de seguridad para el proyecto de Transicion y Aseguramiento de protocolo IPV6	CISO, ARQUITECTO EMPRESARIAL, LIDER DE REDES	0																								
		A.9 Control de Accesos	Definir procedimiento estandar para el control de accesos	CISO	0																								
			Revisar, definir y gestionar las mejoras correspondientes para la administración de usuarios en las diferentes aplicaciones y plataformas.	CISO, COORDINADOR DE	0																								
			Crear y documentar las matrices de cargos vs roles	CISO	0																								
			Socializar la creación y uso de matrices a líderes de proceso	CISO	0																								
		A.10 Criptografía	Documetar la administración de las llaves de cifrado para VPN.	CISO	0																								
			Evaluar y desplegar herramienta para la administración centralizada y cifrada de contraseñas	CISO,COORDINADOR DE AREA	0																								
			Verificar y desplegar cifrado de volumenes en la nube	CISO, COORDINADOR DE	0																								
			Validar la compra e instalcion de certificado digital para el portal web, servcio de correo webmail, pagos virtuales (donaciones), intranet y SIAPINC	CISO,COORDINADOR DE AREA SISTEMAS, COORDINADOR DE	0																								

Alcance limitado para siguiente año (2019): Plan de Continuidad de negocio

Sub-Proceso	MSPI (Mintic)	Dominio ISO 27001:2013	Actividad	Responsable	% de Avance	Enero 1	2	3	4	Febrero 1	2	3	4	Marzo 1	2	3	4	Abril 1	2	3	4
	GUIA 10	A.17 Continuidad de Seguridad de la información	Revisar y documetar los sistemas de redundancia de las instalaciones de procesamiento.	CISO, LIDERES DE PLATAFORMAS	0																
			Realizar y socializar el BIA (Analisis de impacto de negocio)	CISO, LIDERES DE PROCESOS	0																
			Construir e implementar el plan de continuidad de negocio para los procesos criticos del INC, y diseño de formato de pruebas (Evaluar Consultoria)	CISO, LIDERES DE PROCESO	0																
			Programar y ejecutar primeras pruebas de continudad de negocio	CISO, LIDERES DE PLATAFORMAS, COORDINADOR DE AREA DE SISTEMAS	0																
			Definir los controles a implementar en el ambiente de contingencia.	CISO	0																
			Definir el plan de monitoreo de Usuarios y plataformas en ambiente de contingencia.	CISO	0																

11. ENTREGABLES

Para el plan de riesgos y privacidad de la información del INC se identifican los siguientes entregables:

- Plan de tratamiento de riesgo aprobado por Dirección
- Matrices de riesgos actualizadas incluyendo riesgo de seguridad
- Diseño de arquitectura de seguridad de la información
- BIA (Análisis de impacto de negocio) en su capítulo de sistemas y tecnología

12. IDENTIFICACION DE RIESGOS DEL PLAN

- **Ocupación de recursos claves**
  Impacto: Alto
  La no disponibilidad u ocupación de recursos claves, y la ocupación del día a día con prioridad sobre las tareas del proyecto impacta el tiempo y cronograma del plan.

- **Cambios de proveedores de tecnología**
  Impacto: Medio
  Los cambios de proveedores de tecnología por política de sector gobierno se constituye en un riesgo que impacta el tiempo de proyecto debido a la necesidad de capacitación y adaptación de personal externo en los procesos del instituto, y requiere reproceso y revisión de los controles, la documentación de SGSI y entregables del plan.

- **Cambios de tecnología**:
  Impacto: Medio
  Aunque se observa una tendencia estable sobre los sistemas de información críticos, los cambios de tecnología debido a los cambios de proveedores por política de sector gobierno se constituye en un riesgo que impacta el recurso humano y tiempos de proyecto, ya que se requieren nuevos procesos de adopción y curva de aprendizaje del personal interno, contratistas y proveedores del INC a estos cambios, y se requiere revisión de los controles, la documentación de SGSI y entregables del plan.

13. CONTROL DE CAMBIOS

ELABORÓ		**REVISÓ**		**APROBÓ**	
Cargo:	Profesional especializado I	Cargo:	Coordinador	Cargo:	MIPG - Comité institucional de gestión y desempeño
Nombre	Carlos Andres Guerrero	Nombre	Luis Eduardo Martínez	Cargo:	Coordinador Grupo Área Sistemas
Dependencia:	Grupo Área de Sistemas	Dependencia:	Grupo Área de Sistemas	Dependencia:	Comité institucional de gestión y desempeño con acta No 09 de 12 de julio de 2018
Fecha:	04-07-2018	Fecha:	06-07-2018	Fecha:	12-07-2018

INDICE DE MODIFICACIONES				
Versión	Responsable	Cargo	Fecha	Descripción
1.0	Carlos Andres Guerrero	Profesional especializado I – oficial de seguridad de la información	04/07/2016	Creación del documento