PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

GESTION DE LA TECNOLOGIA

GRUPO ÁREA DE SISTEMAS

INSTITUTO NACIONAL DE CANCEROLOGÍA ESE

2019

TABLA DE CONTENIDO

1. INTRODUCCION

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 Digital que contribuye a la construcción de un Estado eficiente, transparente, participativo y que preste mejores servicios a los ciudadanos.

Teniendo en cuenta lo anterior, se actualiza el presente documento dando cumplimiento a lo establecido en el Decreto 612 de 2018, actualizando el Plan de implementación de Seguridad y Privacidad de la Información al interior del Ministerio de Tecnologías de la Información y las Comunicaciones, aprobado mediante acta de comité de tecnología del 05 de septiembre de 2019.

2. OBJETIVO DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

Establecer las actividades que están contempladas en el Modelo de Seguridad y Privacidad de la Información (MSPI) de MINTIC, alineadas con la NTC/IEC ISO 27001:2013, la Política de Seguridad Digital y Continuidad del servicio, que conducen a la preservación de la confidencialidad, integridad, y disponibilidad de los activos de información del INSTITUTO NACIONAL DE CANCEROLOGÍA –E.S.E.

3. OBJETIVOS ESPECIFICOS DE PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

- Identificar, reformular y formalizar las necesidades y requerimientos del Instituto Nacional de Cancerología ESE en cuanto a normatividad a tener en cuenta en la implantación del SGSI.
- Establecer el estado actual y nivel de madurez de los procesos de seguridad y privacidad de la información.
- Actualizar los controles, las políticas, y definir los planes de mejoramiento necesarios para Gestionar los riesgos de seguridad y privacidad de la información, Seguridad Digital de manera integral.
- Establecer y documentar el gobierno de gestión de seguridad de la información, alineado con el gobierno de TI
- Evaluar y alinear el SGSI para dar cumplimiento a los marcos regulatorios identificados.
- Planear programas y planes de auditoria para el monitoreo y mejora continua del SGSI.

4. ALCANCE DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Establecimiento del sistema de gestión de seguridad de la información (SGSI) para las áreas de tecnología de información y las comunicaciones, utilizando como guía la norma ISO-IEC- 27001:2013 y la metodología MSPI de MINTIC, en un periodo de 2 años .(Fase I -2019, Fase 2 -2020)

5. OBJETIVO DEL SISTEMA DE GESION DE SEGURIDAD DE LA INFORMACION SGSI

Lograr procesos internos seguros y eficientes a través del fortalecimiento de las capacidades de gestión de tecnologías de información por medio de la incorporación de esquemas de manejo seguro de la información

y de la alineación con la arquitectura institucional de la entidad, a fin de apoyar el logro de las metas y objetivos de la entidad

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

Aplica a todos los niveles del INSTITUTO NACIONAL DE CANCEROLOGIA E.S.E, a todos sus funcionarios, contratistas, proveedores, operadores y aquellas personas o terceros que en razón del cumplimiento de sus funciones y las del Ministerio 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, aplica a toda la información creada, procesada o utilizada por el INC, sin importar el medio, formato o presentación o lugar en el cual se encuentre.

7. RESUMEN DE POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN, SEGURIDAD DIGITAL Y CONTINUIDAD DE LOS SERVICIOS DEL INSTITUTO NACIONAL DE CANCEROLOGIA E.S.E.

El INSTITUTO NACIONAL DE CANCEROLOGIA E.S.E, mediante la adopción e implementación del Modelo de Seguridad y Privacidad de la Información (MSPI) enmarcado en el Sistema de Gestión de Seguridad de la información, protege, preserva y administra la confidencialidad, integridad, disponibilidad, autenticidad y no repudio de los activos de información del Instituto mediante una gestión integral de riesgos y la implementación de controles físicos y digitales previniendo así incidentes y dando cumplimiento a los requisitos legales y reglamentarios, orientados a la mejora continua y al alto desempeño del Sistema de Gestión de Seguridad de la Información, propendiendo así por el acceso, uso efectivo y apropiación de las TIC para el trabajo en el control integral del cáncer en el país.

8. OBJETIVOS ESPECIFICOS DE SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION SGSI

Objetivos PDI	Objetivos SGSI	INSTITUTO NACIONAL DE CANCEROLOGIA (ICN)				
		Plan de Desarrollo Institucional 2019 -2022	Plan Sectorial Salud	Plan Nacional de Cancer	Generación de Impacto	Excelencia Organizacional
Diseñar e implementar al 100% anual el plan de la seguridad y privacidad	Cumplir con normatividad y reglamentación legal vigente relacionada con Seguridad de la Información que aplique al INC, tomando las medidas necesarias de acuerdo a la gestión de cada proceso.	X	X			X

de la información.	Gestionar los riesgos de Seguridad de la Información de manera eficiente, permitiendo una armonización entre operatividad de los procesos y la seguridad de la información, alineados con las mejores prácticas del estándar ISO27001:2013	X	X	X	X	X
	Asegurar que la forma en que se recopila, procesa, utiliza y almacena la información durante todo su ciclo de vida dentro del INC se trata de forma segura, confidencial, y siempre cuenta con el consentimiento y la finalidad que determina el paciente o interesado.	x	X	X	X	X
	Asegurar que todos los colaboradores, pacientes, contratistas y proveedores sean conscientes de las amenazas y riesgos de seguridad de la información, y se dé cumplimiento a las políticas y controles establecidos.	x	X		X	X
	Fortalecer las capacidades de Ciberseguridad y Ciberdefensa para proteger la infraestructura que se determine como critica en el Instituto.	x				X

9. ESTABLECIMIENTO DE COMITÉ DE SEGURIDAD DE LA INFORMACIÓN

Las funciones del comité de Seguridad de la Información serán asumidas por el comité institucional de gestión y desempeño – MIPG

10. NORMATIVIDAD

Ley 1952 de 2019. Por medio de la cual se expide el código general disciplinario

Circular externa 007 de 2018 Superfinaciera: Por la cual se Imparten instrucciones relacionadas con los requerimientos mínimos para la gestión del riesgo de ciberseguridad.

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.

CONPES 3854 de 2016. Política Nacional de Seguridad digital.

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

Decreto 1377 De 2013: Por el cual se reglamenta parcialmente la Ley 1581 de 2012, Derogado Parcialmente por el Decreto 1081 de 2015.

Ley 1581 de 2012: 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.

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

Ley 1474 de 2011. Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública.

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

Ley 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

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

Ley 594 de 2000. Por medio de la cual se expide la Ley General de Archivos

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

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

CONPES 3670 DE 2010. Lineamientos de política para la continuidad de los programas de acceso y servicio universal a las TICS.

Decreto 1404 de 2012 – Lineamientos para Interceptación legal de comunicaciones

Plan de protección y defensa de la infraestructura critica cibernética del sector salud y protección social. PSPICCN v1.0 Año 2019

Constitución Política de Colombia 1991. Artículo 15.

11. DEFINICIONES TÉCNICAS

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).

12. METODOLOGIA DE IMPLEMENTACIÓN DEL PLAN

El modelo de implementación e inicio de operación del SGSI basado en ISO 27001:2013 consta de 5 pasos, y está basado en el ciclo PHVA lo que permite que el sistema de gestión sea sostenible en el tiempo.

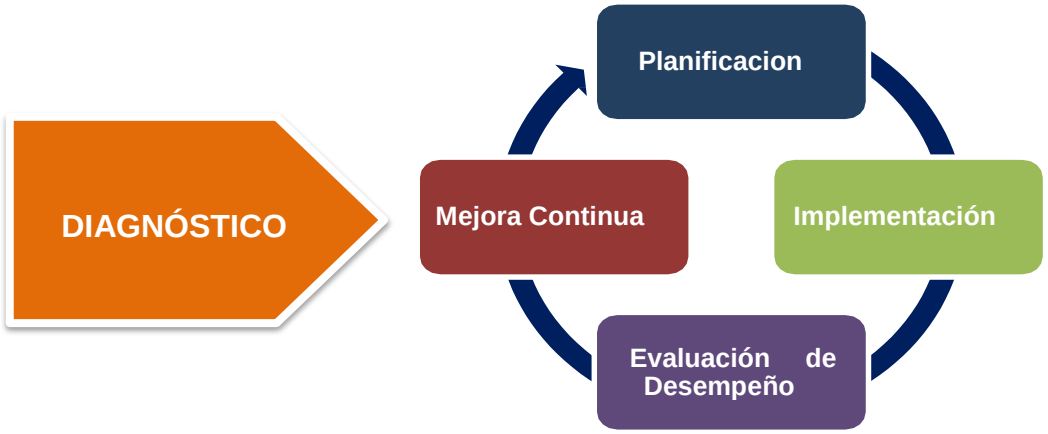


Imagen 1 – Ciclo de operación del Modelo de Seguridad y Privacidad de la Información

Año	AVANCE PHVA – Julio 2019		
	COMPONENTE	% de Avance Actual	% Avance Esperado
2018	Planificación	100%	100%
2019	Implementación Fase 1	49%	49%
2020	Implementación Fase 2	-	-
2019	Evaluación de desempeño	90%	90%
2019-2020	Mejora continua	Sin Iniciar%	N/A%
TOTAL		**58%**	**100%**

13. ACTUALIZACIÓN DE COMPONENTES PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Se identifican a continuación los dominios seleccionados de ISO 27001:2013 que se deben desarrollar para la implementación del SGSI en INC y para dar cumplimiento al plan de seguridad y privacidad de seguridad de la información exigida por MSPI de MINTIC. Se actualizan componentes para incluir los temas concernientes a Habeas data (Tratamiento de datos personales), Ciberseguridad y Ciberdefensa de las infraestructuras críticas y de la Gestión de Cumplimento interno y regulatorio.

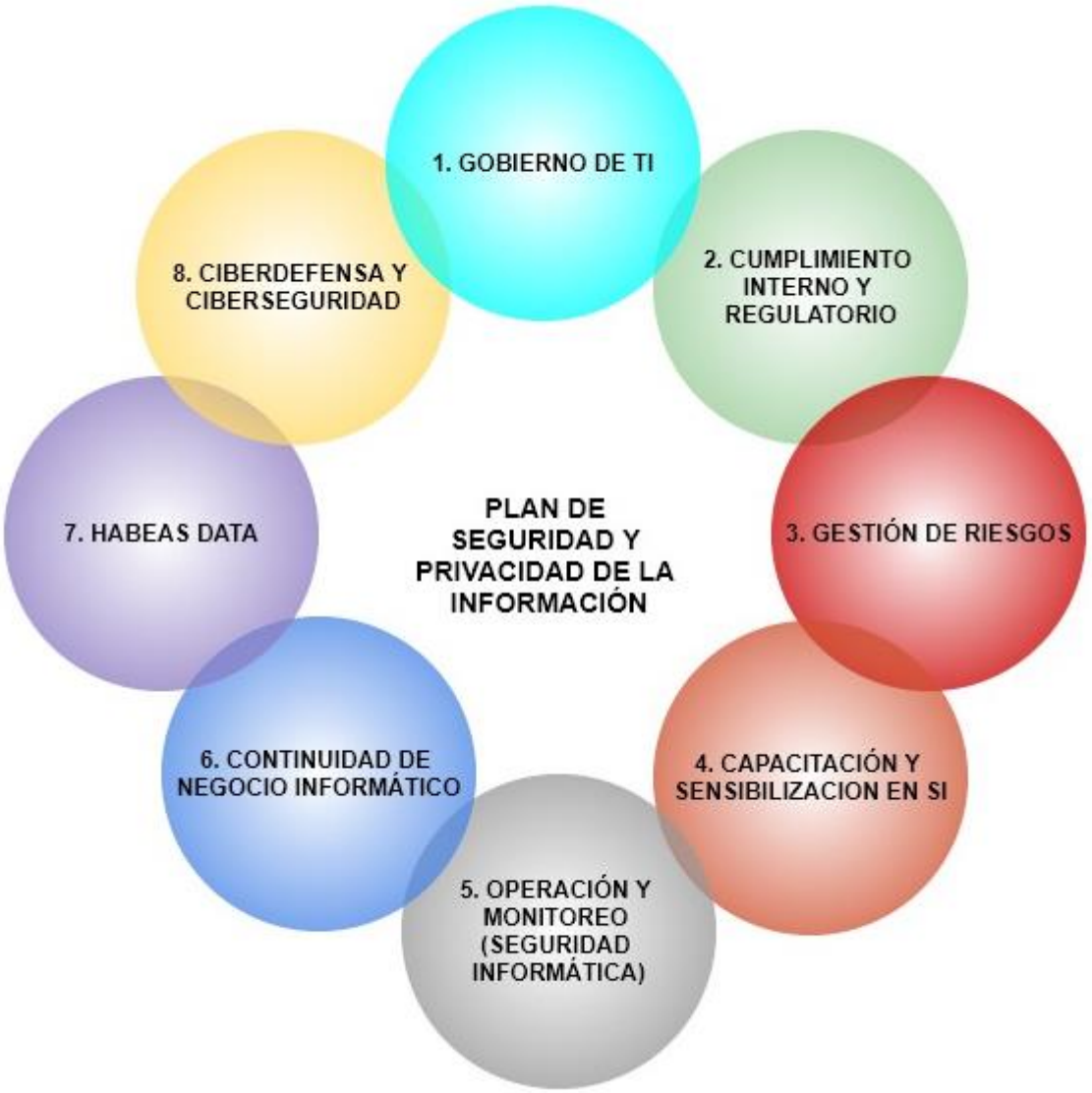


Imagen 2. Actualización de Componentes de Plan de Seguridad y privacidad de la información

14. ACTUALIZACIÓN DE PARTES INTERESADAS DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Para el Modelo de Seguridad y Privacidad de la Información (MSPI) de Gobierno Digital y el Sistema de Gestión de Seguridad de la Información (SGSI), las partes interesadas internas, pertinentes, están constituidas por los procesos misionales, estratégicos, de apoyo y de evaluación, definidos por el Sistema de Gestión de Calidad, de conjunto con las respectivas dependencias y/o áreas que garantizan su operación.

Para la implantación del plan se requieren la participación y ajustes de las siguientes partes interesadas por fase de proyecto:

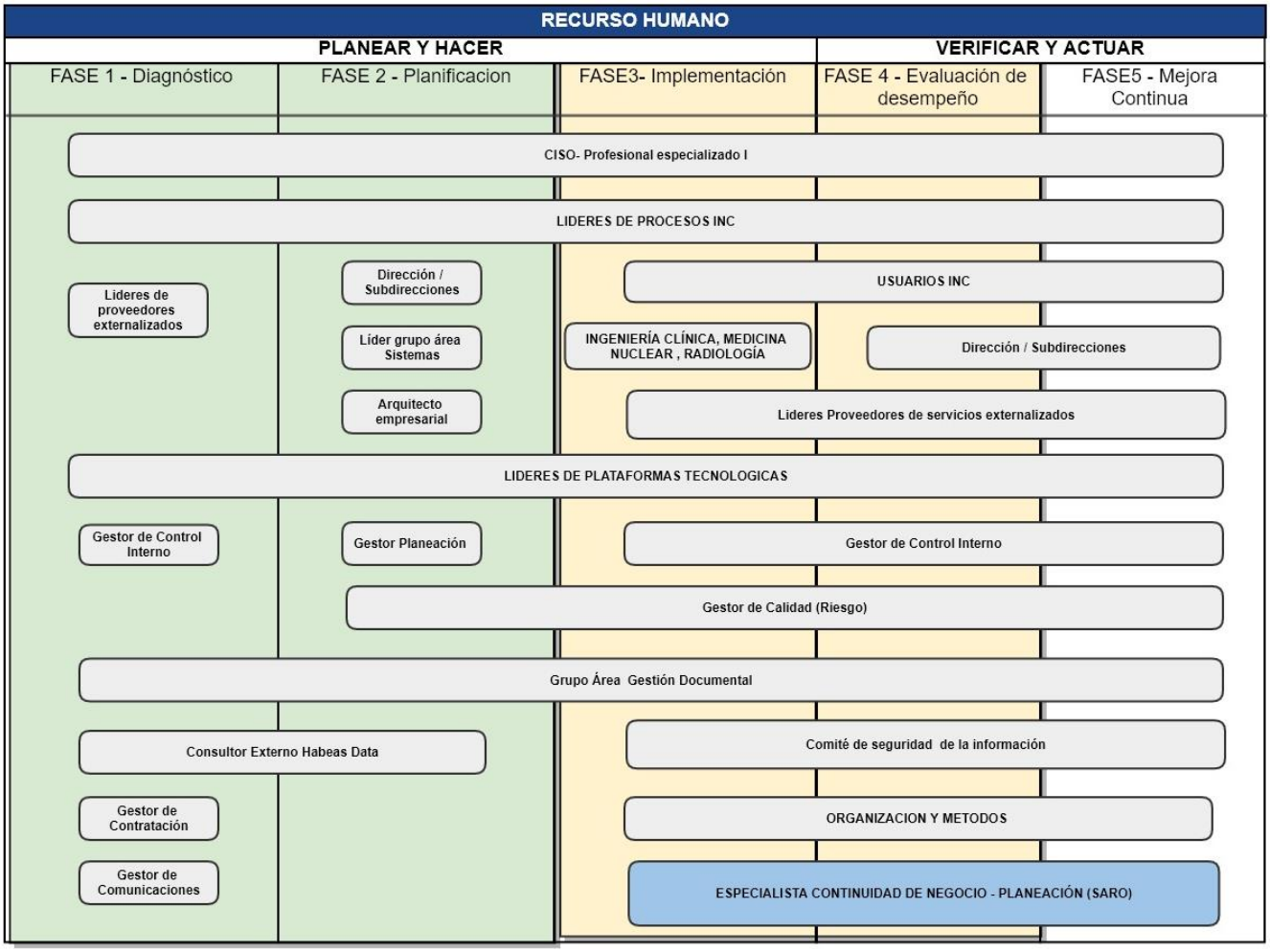


Imagen 3. Recursos Humano necesario para plan de seguridad y privacidad de la información.

Se incluye a los grupos Area Ingeniería Clínica, Medicina Nuclear y Radiología dentro de la implementación del componente de Ciberseguridad y Ciberdefensa, para el aseguramiento de sus sistemas debido a la determinación del impacto y riesgo de tipo ambiental.

Es importante contar con la inclusión de un Especialista de Continuidad de negocio gobernado por el grupo área de planeación, o por el área que lidere la administración de riesgo operativo SARO. Esta especialista en Continuidad se encargara de la prevención y atención de emergencia, la administración de la crisis, el análisis BIA, y liderar la construcción de los planes de continuidad para los procesos operativos del INC. El oficial de seguridad de la información y grupo de seguridad informática apoyara la gestión de contingencia tecnológica e informática.

15. IDENTIFICACIÓN NECESIDADES Y EXPECTATIVAS DEL SGSI

A continuación, se exponen con detalles, las actuaciones de las partes interesadas internas del MSPI de Gobierno Digital y el SGSI, con las respectivas necesidades identificadas:

PERFIL	NECESIDADES Y EXPECTATIVAS
DIRECTIVOS	• Comprometerse con la implementación, establecimiento, operación, monitorización, mantenimiento, revisión y mejora del Sistema de Gestión de Seguridad de la Información • Conocer y entender las leyes y directivas que forman la base del programa de seguridad. • Comprender el liderazgo y compromisos con la seguridad de la información que su rol tiene. • Efectuar actividad de identificación, análisis y valoración de riesgos de seguridad digital , para su proceso • Realizar actividad de clasificación y etiquetado de la información, en cuanto a confidencialidad, integridad y disponibilidad • Garantizar el correcto tratamiento a los datos personales, recolectados por las áreas que gestionan el proceso. • Revisión del Manual de Políticas de Seguridad y Privacidad de la Información, a intervalos planificados, para su validación •
RESPONSABLES DE PROCESOS ESTRATÉGICOS	• Participación activa en la determinación del alcance del MSPI de Gobierno Digital y el SGSI. • Participación activa en la identificación de las cuestiones internas y externas (debilidades, fortalezas, amenazas y oportunidades), pertinentes al MSPI de Gobierno Digital y al SGSI. • Participación activa en la identificación de las partes interesadas, pertinentes al MSPI de Gobierno Digital y al SGSI; sus necesidades y expectativas • Asegurarse que la política de seguridad de la información y los objetivos, son compatibles con la dirección estratégica de la organización. • Asegurar que los recursos requeridos para la implementación del MSPI de Gobierno Digital y el SGSI, se encuentren disponibles. • Dirigir y apoyar al recurso humano, encargado de implementar el MSPI de Gobierno Digital y el SGSI, para contribuir a la eficacia respectiva • Participación activa en la elaboración, aprobación e implementación de la política general de seguridad de la información.. • Liderar la gestión de Continuidad de Negocio • Realizar actividad de clasificación y etiquetado de los activos de información, en cuanto a confidencialidad, integridad y disponibilidad • Efectuar una actividad de identificación, análisis y valoración de riesgos de seguridad de la información satisfactoria, para el proceso. • Ofrecer un adecuado tratamiento a los datos personales, recolectados por las áreas que gestionan el proceso.
RESPONSABLES DE SEGURIDAD DE LA INFORMACION	• Verificar que la política general de seguridad de la información, los roles y responsabilidades se encuentren acorde a los requisitos de la norma NTC-ISO-IEC 27001:2013.

- Garantizar que los objetivos del Modelo de Seguridad y Privacidad de la Información y el Sistema de Gestión de Seguridad de la Información, se encuentren acorde a la norma NTC-ISO-IEC 27001:2013. y al plan de desarrollo institucional.
- Participación activa en la identificación de las cuestiones internas y externas (debilidades, fortalezas, amenazas y oportunidades), pertinentes al MSPI de Gobierno Digital y al SGSI.
- Liderar la Implementación del SGSI en cumplimiento del plan de seguridad y privacidad de la información
- Liderar la identificación de las partes interesadas, pertinentes al MSPI de Gobierno Digital y al SGSI; sus necesidades y expectativas.
- Elaborar e implementar un plan de tratamiento de riesgos de seguridad de la información, que permita mantener controlado y en niveles aceptables, los riesgos identificados en el proceso.
- Asignar y comunicar los roles y responsabilidades respectivas de la seguridad de la información
- Participación activa en la elaboración de los objetivos de la seguridad de la información y planes para lograrlos.
- Actualización de Manual de Políticas de Seguridad y Privacidad de la Información
- Implementación de modelos de ciberseguridad y Ciberdefensa al interior del instituto.
- Garantizar la adecuada implementación de controles de seguridad contra código malicioso
- Garantizar una adecuada identificación y gestión de vulnerabilidades y amenazas técnicas de sistemas y activos de información
- Elaboración y socialización de políticas de escritorio limpio,pantalla limpia e higiene de seguridad informática
- Garantizar la adquisición e implementación de certificados digitales para los sistemas de información.
- Garantizar la elaboración e implementación del plan de contingencia, recuperación y retorno a la normalidad.
- Elaborar el Plan de Sensibilización y Entrenamiento, en temas de seguridad de la información, garantizando su implementación al interior del Instituto
- Garantizar que el recurso humano, destinado a participar en tareas o actividades, relacionadas con seguridad de la información, tenga o adquiera las competencias respectivas, para el buen desempeño de la misma
- Participación activa en la elaboración de la estrategia de comunicación interna, para los temas referentes a seguridad de la información.
- Garantizar que toda documentación que sea de interés para el Sistema de Gestión de Calidad, se encuentre debidamente ingresada, acorde al procedimiento de control de documentos definido y aprobado
- Reaccionar ante la identificación de una no conformidad y tomar acciones para controlarla y corregirla, haciendo frente a cualquier consecuencia que pueda tener la misma, evaluando, además, la necesidad de generar acciones que permitan eliminar la causa.
- Articularse con las áreas respectivas para garantizar la elaboración y actualización de los inventarios de activos de información, y la clasificación y

	etiquetado de la información, en cuanto a confidencialidad, integridad y disponibilidad • Liderar la gestión para un adecuado tratamiento a los datos personales del instituto. • Ofrecer una adecuada protección a los equipos de usuarios desatendidos. • Cumplir con todo lo establecido por el habilitador transversal seguridad de la información, de Gobierno Digital.
LIDERES DE PROCESOS	• Conocer y entender su compromiso y el de su grupo con las políticas de seguridad de la información y Política de manejo de datos personales • Identificación de riesgo de seguridad digital sobre sus activos de información • Custodia de activos de información a cargo de su grupo de trabajo. • Efectuar una actividad de identificación, análisis y valoración de riesgos de seguridad de la información satisfactoria, para el proceso. • Elaborar e implementar planes de tratamiento de riesgos de seguridad digital, que permita mantener controlado y en niveles aceptables, los riesgos identificados en el proceso • Ofrecer una adecuada protección a los equipos de usuarios desatendidos • Ofrecer un adecuado tratamiento a los datos personales, recolectados por las áreas que gestionan el proceso • Garantizar una adecuada aplicación de controles de escritorio limpio y pantalla limpia. • Realizar una actividad de clasificación y etiquetado de la información, en cuanto a confidencialidad, integridad y disponibilidad • Garantizar que el recurso humano, destinado a participar en tareas o actividades, relacionadas con seguridad de la información, tenga o adquiera las competencias respectivas, para el buen desempeño de la misma • Garantizar que el recurso humano que gestiona el proceso, participe activamente en las charlas de sensibilización que convoca la el Grupo área de Gestión de sistemas. • Reaccionar ante la identificación de una no conformidad y tomar acciones para controlarla y corregirla, haciendo frente a cualquier consecuencia que pueda tener la misma, evaluando, además, la necesidad de generar acciones que permitan eliminar la causa.
ADMINISTRADORES DE PLATAFORMAS Y SISTEMAS DE INFORMACION	• Preparación y actualización a nivel técnico de seguridad (implementación y prácticas de seguridad efectivas) para soportar las operaciones críticas del INC de manera apropiada. • Capacitación avanzada sobre protocolo IPV6 • Conocer y entender su compromiso y el de su grupo con las políticas de seguridad de la información y Política de manejo de datos personales • Conocer sus responsabilidades con el SGSI. • Conocimientos avanzados sobre protección y administración de archivos en la nube. • Efectuar actividad de identificación, análisis y valoración de riesgos de seguridad de la información satisfactoria, para el proceso.

	• Elaborar e implementar un plan de tratamiento de riesgos de seguridad de la información, que permita mantener controlado y en niveles aceptables, los riesgos identificados en el proceso. • Garantizar que el recurso humano, destinado a participar en tareas o actividades, relacionadas con seguridad de la información, tenga o adquiera las competencias respectivas, para el buen desempeño de la misma • Contemplar la actividad de la seguridad de la información en la gestión de proyectos. • Participar activamente en la elaboración y actualización del inventario de activos de información tipo software, servicios y hardware. • Realizar una actividad de clasificación y etiquetado de la información, en cuanto a confidencialidad, integridad y disponibilidad. • Implementar el conjunto de políticas de control de acceso. • Implementar controles de seguridad para asignar los privilegios adecuados a los usuarios, para el acceso a la red institucional y sus servicios. • Garantizar un mantenimiento adecuado de equipo • Garantizar una adecuada protección a los equipos de usuarios desatendidos. • Garantizar la implementación de la política de escritorio limpio y pantalla limpia. • Garantizar la elaboración e implementación de un procedimiento de gestión de cambios. • Garantizar la separación de los ambientes de desarrollo, pruebas y producción. • Garantizar la implementación de soluciones de backup automático, para sistemas de información y usuarios del dominio. • Garantizar una adecuada sincronización de relojes para el registro de eventos de seguridad de la información. • Garantizar un adecuado control de la instalación de software, en los sistemas operativos. • Garantizar una adecuada gestión de tratamiento de las vulnerabilidades técnicas identificadas. • Garantizar la implantación de certificados digitales para los sistemas de información. • Implementar un marco de trabajo desarrollo seguro. • 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 técnica
RESPONSABLES DE INGRESO Y RETIRO DE PERSONAL	• Conocer y entender su compromiso y el de su grupo con las políticas de seguridad de la información y Política de manejo de datos personales. • Verificar de manera satisfactoria los antecedentes disciplinarios, fiscales y penales, de los candidatos a las vacantes ofertadas • Establecer la cláusula de confidencialidad, en la relación contractual, con los servidores públicos del proceso • Ofrecer un adecuado tratamiento a los datos personales, recolectados por las

	áreas que gestionan el proceso • Garantizar una adecuada aplicación de controles de escritorio limpio y pantalla limpia. • Realizar una actividad de clasificación y etiquetado de la información, en cuanto a confidencialidad, integridad y disponibilidad • Ofrecer una adecuada protección a los equipos de usuarios desatendidos • Garantizar que el recurso humano, destinado a participar en tareas o actividades, relacionadas con seguridad de la información, tenga o adquiera las competencias respectivas, para el buen desempeño de la misma • Garantizar que el recurso humano, destinado a participar en tareas o actividades, relacionadas con seguridad de la información, tenga o adquiera las competencias respectivas, para el buen desempeño de la misma.
RESPONSABLES DE CONTROL INTERNO Y PROCESOS DISCIPLINARIOS	• Revisar, a intervalos planificados, el MSPI de Gobierno Digital y el SGSI, para asegurarse de su conveniencia, adecuación y eficacia continua • Realizar auditorías internas a los procesos constituidos por el Sistema de Gestión de Calidad, donde se tengan en cuenta criterios normativos y de Gobierno, en temas de seguridad de la información • Realizar el respectivo seguimiento a los planes de mejora, relacionados con seguridad de la información, en todos los procesos internos, verificando la eficacia de las acciones tomadas. • Implementar de manera satisfactoria el procedimiento disciplinario correspondiente, con todo servidor público que viole lo referente a seguridad de la información. • Participación activa en la identificación de las cuestiones internas y externas (debilidades, fortalezas, amenazas y oportunidades), pertinentes al MSPI de Gobierno Digital y al SGSI. • Ofrecer una adecuada protección a los equipos de usuarios desatendidos • Ofrecer un adecuado tratamiento a los datos personales, recolectados por las áreas que gestionan el proceso • Garantizar una adecuada aplicación de controles de escritorio limpio y pantalla limpia. • Realizar una actividad de clasificación y etiquetado de la información, en cuanto a confidencialidad, integridad y disponibilidad • Garantizar que el recurso humano, destinado a participar en tareas o actividades, relacionadas con seguridad de la información, tenga o adquiera las competencias respectivas, para el buen desempeño de la misma
RESPONSABLES DE COMUNICACIONES	• Participación activa en la elaboración de la estrategia de comunicación interna, para los temas referentes a seguridad de la información. • Actualización de plan de comunicaciones incluyendo plan de capacitación y sensibilización de seguridad de la información. • Garantizar un manejo seguro y adecuado de los medios de comunicación • Ofrecer una adecuada protección a los equipos de usuarios desatendidos • Ofrecer un adecuado tratamiento a los datos personales, recolectados por las áreas que gestionan el proceso • Garantizar una adecuada aplicación de controles de escritorio limpio y pantalla limpia.

	• Realizar una actividad de clasificación y etiquetado de la información, en cuanto a confidencialidad, integridad y disponibilidad • Garantizar que el recurso humano, destinado a participar en tareas o actividades, relacionadas con seguridad de la información, tenga o adquiera las competencias respectivas, para el buen desempeño de la misma
RESPONSABLES DE LA GESTION DE INFRAESTRUCTURA FISICA	• Ofrecer una seguridad de recintos, oficinas, cajones y archivadores, CCTV y custodia satisfactoria, para de esta manera, preservar la confidencialidad, integridad y disponibilidad de la información almacenada • Garantizar una protección óptima de todos los equipos tecnológicos contra fallas de energía • Ofrecer una adecuada protección al cableado de energía eléctrica y de datos, para minimizar el riesgo de interceptación, interferencia o daño • Ofrecer una adecuada protección a los equipos de usuarios desatendidos • Ofrecer un adecuado tratamiento a los datos personales, recolectados por las áreas que gestionan el proceso • Garantizar una adecuada aplicación de controles de escritorio limpio y pantalla limpia. • Realizar una actividad de clasificación y etiquetado de la información, en cuanto a confidencialidad, integridad y disponibilidad • Garantizar que el recurso humano, destinado a participar en tareas o actividades, relacionadas con seguridad de la información, tenga o adquiera las competencias respectivas, para el buen desempeño de la misma
RESPONABLES DE GESTION DOCUMENTAL	• Garantizar un adecuado transporte, tratamiento y custodia de los medios físicos que contengan información • Establecer la política de manejo de Gestión Documental en Físico y electrónico • Establecer las políticas de clasificación de activos • Liderar y Realizar actividades de clasificación y etiquetado de la información, en cuanto a confidencialidad, integridad y disponibilidad. • Ofrecer una adecuada protección a los equipos de usuarios desatendidos • Ofrecer un adecuado tratamiento a los datos personales, recolectados por las áreas que gestionan el proceso • Garantizar una adecuada aplicación de controles de escritorio limpio y pantalla limpia. • Garantizar que el recurso humano, destinado a participar en tareas o actividades, relacionadas con seguridad de la información, tenga o adquiera las competencias respectivas, para el buen desempeño de la misma
RESPONSABLES DE SISTEMAS DE GESTION DE CALIDAD Y DE ORGANIZACIÓN Y METODOS	• Controlar la documentación del Modelo de Seguridad y Privacidad de la Información del Gobierno Digital y el Sistema de Gestión de Seguridad de la Información, que son de interés para el Sistema de Gestión de Calidad • Participación activa en la identificación de las cuestiones internas y externas (debilidades, fortalezas, amenazas y oportunidades), pertinentes al MSPI de Gobierno Digital y al SGSI • Ofrecer una adecuada protección a los equipos de usuarios desatendidos • Ofrecer un adecuado tratamiento a los datos personales, recolectados por las áreas que gestionan el proceso • Garantizar una adecuada aplicación de controles de escritorio limpio y

	pantalla limpia. • Realizar una actividad de clasificación y etiquetado de la información, en cuanto a confidencialidad, integridad y disponibilidad • Garantizar que el recurso humano, destinado a participar en tareas o actividades, relacionadas con seguridad de la información, tenga o adquiera las competencias respectivas, para el buen desempeño de la misma
PROCESOS RESPONSABLES DE CONTRATACIÓN Y ADQUISICIONES DE ACTIVOS DE INFORMACIÓN	• Establecer todos los requisitos de seguridad de la información, en la relación con los proveedores (cláusulas de confidencialidad, deber de secreto y acuerdos de niveles de servicios) • Identificar los riesgos de seguridad de la información, relacionados con la cadena de suministro de tecnología de información y comunicación, y en las relacionas con activos de información críticos para el instituto. • Evaluar la calidad en la prestación de servicios en los proveedores. 5- Gestionar, de manera óptima, los cambios en el suministro de servicios, por parte de los proveedores. • Efectuar una actividad de identificación, análisis y valoración de riesgos de seguridad de la información satisfactoria, para el proceso. • Ofrecer una adecuada protección a los equipos de usuarios desatendidos • Ofrecer un adecuado tratamiento a los datos personales, recolectados por las áreas que gestionan el proceso • Garantizar una adecuada aplicación de controles de escritorio limpio y pantalla limpia. • Realizar una actividad de clasificación y etiquetado de la información, en cuanto a confidencialidad, integridad y disponibilidad • Garantizar que el recurso humano, destinado a participar en tareas o actividades, relacionadas con seguridad de la información, tenga o adquiera las competencias respectivas, para el buen desempeño de la misma
PROVEEDORES Y TERCERIZADOS	• El deben tener un buen nivel de preparación y actualización a nivel técnico de seguridad (implementación y prácticas de seguridad efectivas) para soportar las operaciones críticas del INC de manera apropiada. • Conocer y entender su compromiso y el de su grupo con las políticas de seguridad de la información y Política de manejo de datos personales • Conocer y cumplir sus responsabilidades con el SGSI del INC. • Armonizar sus acuerdos de confidencialidad y deber de secreto con las políticas de seguridad, privacidad y manejo de datos personales del instituto. • Firmar acuerdos de confidencialidad para el manejo de los activos de información del instituto con todos sus empleados y subcontratistas • Implementar buenas prácticas de seguridad de protocolo IPV6 • Ofrecer una adecuada protección a los equipos de usuarios desatendidos • Ofrecer un adecuado tratamiento a los datos personales, recolectados en su gestión para la relación laboral, contractual o motivo de convenio • Garantizar una adecuada aplicación de controles de escritorio limpio y pantalla limpia. • Realizar una actividad de clasificación y etiquetado de la información, en cuanto a confidencialidad, integridad y disponibilidad • Garantizar que el recurso humano, destinado a participar en tareas o actividades, relacionadas con seguridad de la información, tenga o adquiera

	las competencias respectivas, para el buen desempeño de la misma
USUARIOS FINALES	• Requieren de un alto grado de sensibilización sobre la seguridad de la información y las reglas de comportamiento adecuadas con los sistemas y servicios que tienen a disposición, de los derechos del ciudadano y sus deberes con el manejo de datos personales e información sensible en el INC. Abarca a los usuarios finales internos del INC, a estudiantes, docentes e investigadores, y al personal de proveedores, externos y tercerizados. • Deben vigilar constantemente los activos de información que fueron puestos a su disposición y responsabilidad. • Ofrecer una adecuada protección a sus equipos cuando se encuentren desatendidos • Reportar por los canales adecuados y de manera oportuna los incidentes de seguridad de la información. • Ofrecer un adecuado tratamiento a los datos personales, recolectados en su trabajo diario. • Cumplir y respetar cada uno de los controles de seguridad de la información implementados por el instituto. • Eliminar cualquier base de datos o activo intermedia que se genere durante su labor una vez se cumpla la finalidad para la cual fue generada • Garantizar una adecuada aplicación de controles de escritorio limpio y pantalla limpia. • Realizar una actividad de clasificación y etiquetado de la información, en cuanto a confidencialidad, integridad y disponibilidad • Participar en tareas o actividades, relacionadas con seguridad de la información
PACIENTE Y CIUDADANO	• Se requiere crear conciencia en la ciudadanía sobre la necesidad del buen uso de las TIC, impulsar el conocimiento de los usuarios en seguridad digital, y conocer la percepción del usuario en cuanto a la confianza digital en los servicios y sistemas del instituto. • Sensibilizar sus derechos de tratamiento de datos personales y darle a conocer los canales de comunicación con el INC. • Cumplir y permitir el cumplimiento de todos los controles de seguridad durante su estancia en el instituto.

16. PRESUPUESTO SGSI

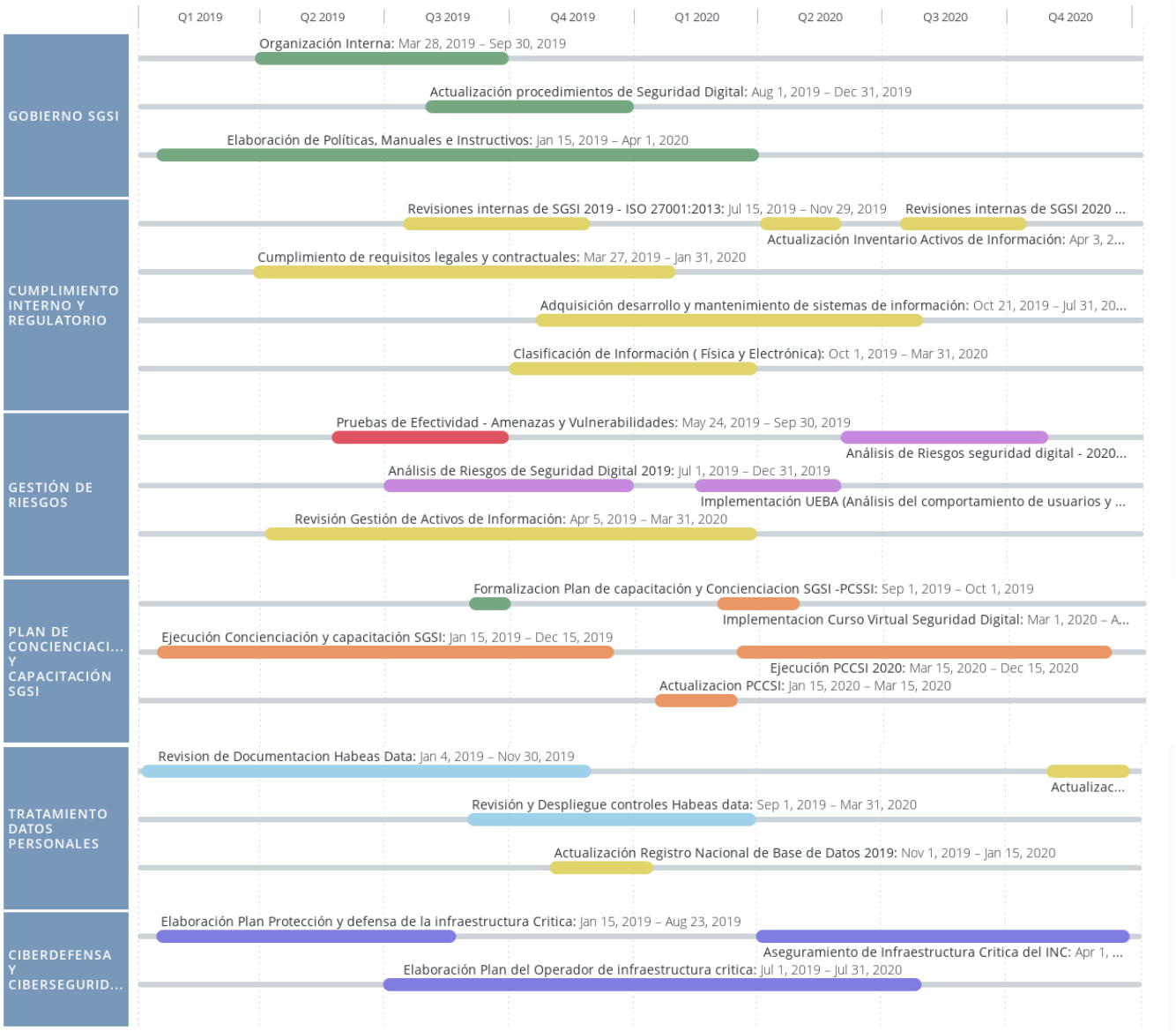
Se presenta a continuación el presupuesto para seguridad de la información para el año 2020

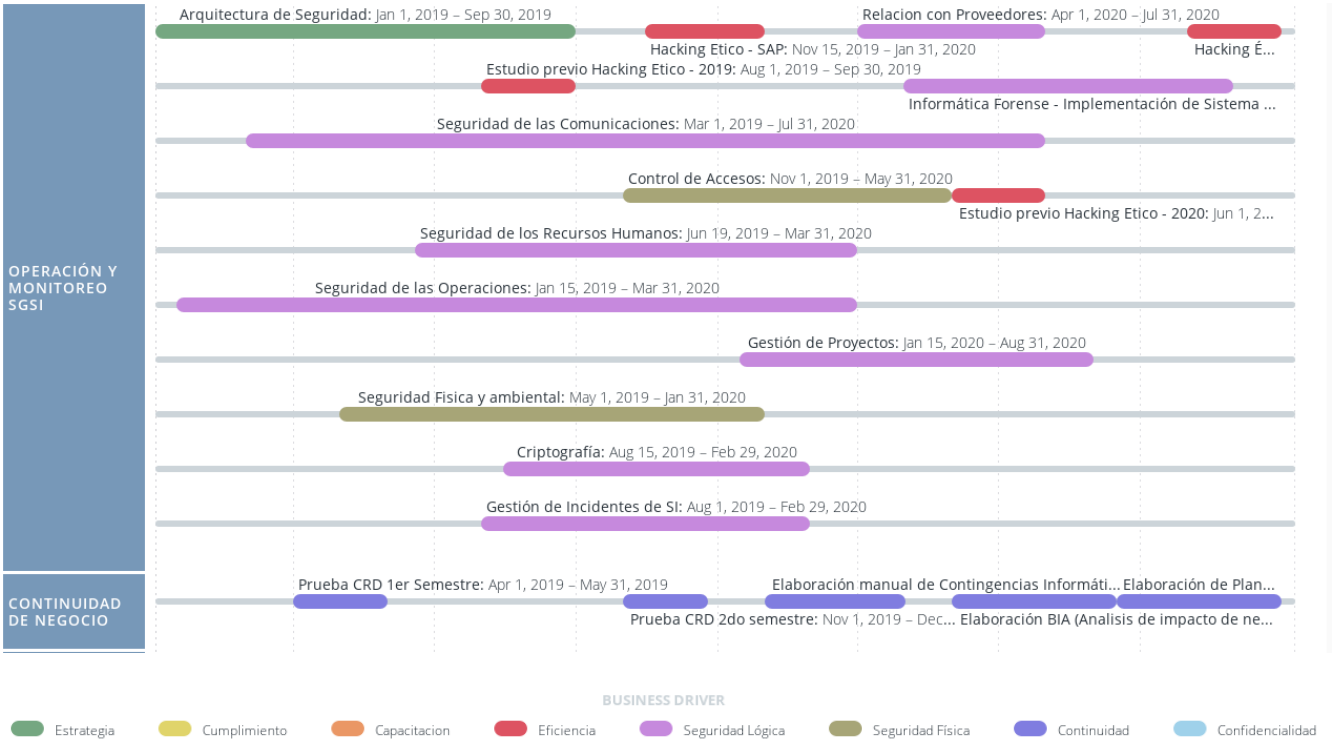
ITEM	Capacidad	Tipo de Soporte	Valor Mensual (Iva incluido)	Valor Anual (Iva incluido)
Oficial seguridad de la información	N/A	N/A	$ 5.700.000,00	$ 105.336.000,00
Especialista en continuidad de negocio (Planeación)	N/A	N/A	$ 5.700.000,00	$ 105.336.000,00
Appliance de Seguridad datacenter portal Web /campus Virtual (Firewall y antivirus)	Media	Oro	$ 630.065,00	$ 7.560.780,00
Web aplicación portal Web /campus Virtual	Media	Oro	$ 660.000,00	$ 7.920.000,00

ITEM	Capacidad	Tipo de Soporte	Valor Mensual (Iva incluido)	Valor Anual (Iva incluido)
IPS y DDos para Appliance portal Web /campus Virtual	Media	Oro	$ 1.454.460,00	$ 17.453.520,00
IPS y DDos para Appliance portal web / campus Virtual	Media	Oro	$ 630.065,00	$ 7.560.780,00
Desarrollo Curso Virtual de seguridad de la información (25 slides) Para inducción y Reinducción	N/A	N/A	N/A	$ 10.000.000,00
Servicio de Appliance de Seguridad (Firewall de nueva generación /Control de aplicaciones/ IPS/ DDos)	INCLUIDO EN SERVICIO DE OUTSOURCING		$ 8.537.060,00	$ 102.444.720,00
Servicio de analítica de eventos de amenazas y vulnerabilidades			$ 692.580,00	$ 8.310.960,00
Monitor de red y disponibilidad			$ 3.272.500,00	$ 39.270.000,00
Servicio de Antivirus con Consola centralizada			$ 2.658.788,00	$ 31.905.456,00
Data loss Prevention DLP para equipos + hw			$ 2.941.455,00	$ 35.297.460,00
Data loss Prevention Office 365			$ 8.385.000,00	$ 100.620.000,00
Servicio de Protección de correo electrónico			$ 17.224.691,00	$ 206.696.292,00
Administración técnica de seguridad informática (SOC+ Personal en sitio)			$ 10.350.246,00	$ 124.202.952,00
Servicio y herramienta de Backup			$ 2.541.014,00	$ 30.492.168,00
Ethical Hacking y Retesting	Caja gris		$ 10.000.000,00	$ 120.000.000,00
Certificado Digital 2 Dominios y Subdominios	Media	Oro	$ 2.333.333,33	$ 28.000.000,00
Servicio NAC (Network Access Control)	INCLUIDO EN EL PROYECTO DE REDES		$ 12.500.000,00	$ 150.000.000,00
Servicio análisis de comportamiento de entidades y usuarios UEBA basado en inteligencia artificial + Monitor de red	Media	Oro	$ 16.666.667	$ 200.000.000
Medios sanetizados y herramientas para informática forense			$ 600.000	$ 7.200.000
Auditoria externa protección datos personales (Gestión Documental- Sistemas)			$ 1.250.000	$ 15.000.000
SUBTOTAL PRESUPUESTO				**$ 1.460.607.088,00**

17. HOJA DE RUTA

A continuación se presenta la hoja de ruta de proyecto para la ejecución del plan de seguridad y privacidad de la información.





La siguiente tabla presenta el detalle de fechas de las principales actividades del ROADMAP para la implementación del plan de seguridad y privacidad de la información.

IMPLEMENTACION PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION 2019 -2020	Fecha 01/01/2019	Fecha 31/12/2020
GESTION DE GOBIERNO DE SEGURIDAD	**15/01/2019**	**01/04/2020**
Elaboración de Políticas, Manuales e Instructivos	15/01/2019	1/04/2020
Organización Interna	28/03/2019	30/09/2019
Actualización procedimientos de Seguridad Digital	01/08/2019	31/12/2019
GESTIÓN DE CUMPLIMIENTO INTERNO Y REGULATORIO	**27/03/2019**	**15/10/2020**
Revisiones internas de SGSI 2019 - ISO 27001:2013	15/07/2019	30/10/2019

IMPLEMENTACION PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION 2019 -2020	Fecha 01/01/2019	Fecha 31/12/2020
Revisiones internas de SGSI 2020 - ISO 27001:2013	15/07/2020	15/10/2020
Adquisición desarrollo y mantenimiento de sistemas de información	21/10/2019	31/07/2020
Cumplimiento de requisitos legales y contractuales	27/03/2019	31/01/2020
Revisión Gestión de Activos de Información	5/04/2019	31/03/2020
Clasificación de Información (Física y Electrónica)	01/10/2019	31/03/2020
PLAN DE CAPACITACIÓN Y CONCIENCIACIÓN SGSI -PCSSI	**15/01/2019**	**15/12/2020**
Formalización Plan de capacitación y Concienciación SGSI -PCSSI	01/09/2019	1/10/2019
Actualización PCCSI 2020	15/01/2020	15/03/2020
Ejecución PCCSI 2020	15/03/2020	15/12/2020
Implementación Curso Virtual Seguridad Digital	1/03/2020	30/04/2020
Ejecución Concienciación y capacitación SGSI 2019	15/01/2019	15/12/2019
GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN	**24/05/2019**	**31/12/2020**
Pruebas de Efectividad - Amenazas y Vulnerabilidades	24/05/2019	30/09/2019
Análisis de Riesgos de Seguridad Digital 2019	01/07/2019	31/12/2019
Hacking Ético - SAP	15/11/2019	31/01/2020
Hacking Ético - Red y Servicios de Apoyo	1/11/2020	31/12/2020
Implementación UEBA (Análisis del comportamiento de usuarios y entidades)	15/02/2020	1/06/2020

IMPLEMENTACION PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION 2019 -2020	Fecha 01/01/2019	Fecha 31/12/2020
Análisis de Riesgos seguridad digital - 2020	1/06/2020	31/10/2020
OPERACIÓN DE SEGURIDAD DE LA INFORMACIÓN	**01/01/2019**	**30/11/2020**
Arquitectura de Seguridad	01/01/2019	30/09/2019
Relación con Proveedores	01/04/2020	31/07/2020
Seguridad Física y ambiental	01/05/2019	31/01/2020
Seguridad de las Operaciones	15/01/2019	31/03/2020
Seguridad de los Recursos Humanos	19/06/2019	31/03/2020
Seguridad de las Comunicaciones	01/03/2019	31/07/2020
Control de Accesos	01/11/2019	31/05/2020
Criptografía	15/08/2019	29/02/2020
Gestión de Incidentes de Seguridad Digital	01/08/2019	29/02/2020
Gestión de Proyectos	15/01/2020	31/08/2020
Informática Forense - Implementación de Manual de cadena de custodia	01/05/2020	30/11/2020
CONTINUIDAD DE NEGOCIO	**01/04/2019**	**31/12/2020**
Prueba CRD 1er Semestre	01/04/2019	31/05/2019
Prueba CRD 2do semestre	01/11/2019	25/12/2019
Elaboración manual de Contingencias Informáticas - DRP	01/02/2020	1/05/2020

IMPLEMENTACION PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION 2019 -2020	Fecha 01/01/2019	Fecha 31/12/2020
Elaboración BIA (Análisis de impacto de negocio)	01/06/2020	15/09/2020
Elaboración de Plan de Continuidad de Negocio	16/09/2020	31/12/2020
HABEAS DATA (GESTION TRATAMIENTO DE DATOS PERSONALES)	**4/01/2019**	**31/12/2020**
Revisión de Documentación Habeas Data	4/01/2019	30/11/2019
Revisión y Despliegue controles Habeas data	1/09/2019	31/03/2020
Actualización Registro Nacional de Base de Datos 2019	01/11/2019	15/01/2020
Actualización Registro Nacional de Base de Datos 2020	01/11/2019	31/12/2020
CIBERDEFENSA Y CIBERSEGURIDAD DE INFRAESTRUCTURA CRITICA	**15/01/2019**	**31/12/2020**
Elaboración Plan Protección y defensa de la infraestructura Critica	15/01/2019	23/08/2019
Elaboración Plan del Operador de infraestructura critica	1/07/2019	31/07/2020
Aseguramiento de Infraestructura Critica del INC	1/04/2020	31/12/2020

18. CRONOGRAMA DE PROYECTO

El cronograma detallado y actualizado de actividades y responsables de proyecto del plan de seguridad y privacidad de la información se presenta a continuación, por cada uno de los subprocesos definidos en la hoja de ruta.

Nombre de tarea	Comienzo	Fin	Nombres de los recursos
PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION	**01/01/19**	**31/12/20**	
1. Gestión de Gobierno de seguridad	**15/01/19**	**01/04/20**	

A5. Política	**15/01/19**	**01/04/20**	
Actualización de documentos del SGSI como políticas, normas, procedimientos y manuales entre otros, alineándolas al marco de trabajo de ISO27001:2013 y MSPI	2/04/19	30/01/20	CISO
Realizar actividades de sensibilización de la política a los colaboradores de la Entidad	vie 1/11/19	vie 01/04/20	CISO, COMUNICACIONES
Revisar y ajustar los indicadores de seguridad del SGSI	mar 15/01/19	jue 24/01/19	CISO, CALIDAD;ARQUITECTO TI
A6. Organización Interna	**28/03/19**	**30/09/19**	
Estructurar Documentos y cadena de valor del SGSI (Objetivos , Alcance Roles y responsabilidades de SI)	28/03/19	30/09/19	CISO
Revisar y establecer separación de deberes para los roles de seguridad de la información.	22/04/19	30/09/19	CISO, COORDINADOR DE AREA DE SISTEMAS
Definir política BYOD (BRING YOUR Own DEVICE), para equipos para proveedores y empresas tercerizados que trabajan con el INC	22/04/19	10/05/19	CISO
Definir política BYOT, (Bring your own tecnology) para todos los usuarios y ciudadanos en el INC	28/03/19	1/05/19	CISO
Actualización procedimientos de Seguridad Digital	**1/08/19**	**31/12/19**	
Elaboración procedimiento incidentes Seguridad Digital	1/09/19	31/10/19	**CISO**
Identificación de necesidades y Expectativas de Seguridad de la información	1/08/19	31/08/19	**CISO**
Alineación de objetivos a Gobierno Digital y PDI	1/08/19	31/08/19	**CISO**
Integración de procedimiento de SGSI a procedimiento de Gestión de TI	01/11/19	31/12/19	**CISO, PLANEACION**
Alineación de Plan de Capacitación y sensibilización de seguridad a plan de comunicaciones	10/09/19	30/11/19	**CISO, COMUNICACIONES**
Gestión de Cumplimiento Interno y Regulatorio	**20/02/19**	**15/10/20**	
A.18 Revisiones de seguridad de la información	**15/07/19**	**29/11/19**	

Aplicar instrumento de medición de desempeño de SGS (Periódico) del MSPI y de ISO27001:2013	26/08/19	13/09/19	CISO, CONTROL INTERNO
Elaborar plan de trabajo y validar solución de los hallazgos de revisoría fiscal relacionados con seguridad de la información.	2/10/19	29/11/19	CISO, LIDER DE OUTSOURCING SISTEMAS, LIDERES DE PLATADORMAS
Evaluar, contratar revisión independiente del SGSI (Anual)	15/07/19	31/08/19	CISO, COORDINADOR DE TECNOLOGIA
A.14 Adquisición, desarrollo y mantenimiento de sistemas de información	**21/10/19**	**31/07/20**	
Validar prácticas en desarrollo seguro de proveedores tercerizados (TMS, NEORIS y BISA).	19/03/20	30/04/20	CISO;COORDINADOR DE APLICACIONES;PROVEEDORES DE APLICACIONES
Definir política de desarrollo seguro (requerimientos mínimos de cumplimiento para proveedores de desarrollo)	1/04/20	21/04/20	CISO;COORDINADOR DE APLICACIONES
Establecer especificaciones y requisitos de seguridad de la información para nuevos sistemas de información , y para mejora de sistemas existentes	21/10/19	31/12/19	CISO;COORDINADOR DE APLICACIONES
Analizar y validar los controles a implementar a nivel de Adquisición, control de cambio, versiónamiento y mantenimiento de los sistemas de información dando cumplimiento a la norma ISO 27001:2013.	2/05/20	31/07/20	CISO;COORDINADOR DE APLICACIONES;LIDER CONTRATACION
A.18.1 Cumplimiento de requisitos legales y contractuales	**20/02/19**	**31/01/20**	
Revisar procedimientos sobre derechos de propiedad intelectual.	vie 1/11/19	31/01/20	CISO;OFICINA ASESORIA JURIDICA
Revisión de Documentación y socialización de manejo datos personales y privacidad de la información, incluyendo actualización de registro de base de datos ante la SIC	1/10/19	7/02/19	GESTION DOCUMENTAL;CISO
Revisar cubrimiento de Pólizas de seguros, y evaluar adquisición de póliza de riesgo tecnológico	20/02/19	22/02/19	CISO;COORDINADOR GRUPO AREA SISTEMAS;INFRAESTRUCTURA
Concienciación SGSI	**15/01/19**	**31/12/20**	
Elaboración Plan de Capacitación y Sensibilización en Seguridad de la Información	1/05/19	15/08/19	CISO
Ejecutar Plan de Capacitación y sensibilización en seguridad de la Información 2019 -2020	15/01/19	31/12/20	CISO, COMUNICACIONES;CISO;OFICINA

			ASESORA COMUNICACIONES;TALENTO HUMANO
Diseño e implantación de Curso de seguridad de la información sobre plataforma virtual de capacitación	15/03/20	30/06/20	CISO, COMUNICACIONES;CISO;OFICINA ASESORA COMUNICACIONES;TALENTO HUMANO
Gestión de Riesgos de Seguridad de la Información	**05/04/19**	**31/12/20**	
Gestión de Activos de Información	**05/04/19**	**30/09/19**	
Actualizar el Inventario de Sistemas de Información y clasificación año 2019	1/04/19	31/07/19	OEM;CISO
Ajuste de nuevos requerimientos de Seguridad Digital para activos de información.	31/08/19	30/09/19	CISO;OEM
Clasificación de Activos de Información	1/10/19	31/12/19	CISO;OEM;GESTION DOCUMENTAL
Análisis de Riesgos de Seguridad Digital - 2019	**01/07/19**	**31/12/19**	
Participación en el desarrollo de la herramienta Ficha integral de riesgos	01/07/19	31/07/19	CISO;MESA DE TRABAJO MINSALUD
Actualizar el procedimiento para la Gestión de Riesgos de INC incluyendo el análisis de riesgo de seguridad de la información para cada uno de los procesos operativos.	01/08/19	1/09/19	CISO, GESTOR DE CALIDAD;PLANEACION
Ejecución análisis de riesgos de Seguridad de la Información, identificados por el área de calidad, definiendo oportunidades de mejora en los controles implementados o definición de nuevos.	1/09/19	31/12/19	CISO, GESTOR DE CALIDAD;GESTOR PLANEACION;CISO;GESTOR CALIDAD; Lideres Grupo Area
Pruebas de Efectividad: Análisis de Vulnerabilidades y Amenazas	**24/05/19**	**30/09/19**	
Identificación de amenazas y vulnerabilidades usando Metodología basada en sniffer x firmas	sáb 1/06/19	7/08/19	CISO
Identificación de amenazas y vulnerabilidades usando Metodología basada en inteligencia artificial basada en comportamientos	24/05/19	30/09/19	CISO
Operación de Seguridad de la información	**01/01/19**	**4/09/20**	

Arquitectura de Seguridad	**01/01/19**	**30/09/19**	
Diseñar de arquitectura básica de red segura	01/01/2019	25/01/19	CISO,ARQUITECTO EMPRESARIAL
Elaborar estudios previos para implementar nueva infraestructura de seguridad basada en las mejores prácticas del mercado y en ejercicios de identificación de vulnerabilidades de IPV6 y proyecto redes	28/01/19	28/03/19	CISO,ARQUITECTO EMPRESARIAL, ADMINISTRADORES DE PLATAFORMAS
Validar y documentar arquitectura y controles de servicio de datacenter para DRP en la nube con TIVIT. (Acceso , cifrado, datos en tránsito, monitoreo)	5/08/19	30/09/19	CISO,ARQUITECTO EMPRESARIAL, PROVEEDOR DATACENTER
A15. Relación con Proveedores	**1/04/20**	**31/07/20**	
Revisar y ajustar políticas de contratación, acuerdos de privacidad y confidencialidad establecidos con los suministradores	1/04/20	30/05/20	CISO, GESTION CONTRACTUAL
Validar y ajustar controles de cambios en el suministro de servicio por parte de los proveedores	1/06/20	31/07/20	CISO, CONTROL INTERNO
A.11 Seguridad Física y ambiental	**1/05/19**	**31/01/20**	
Evaluar situación actual de seguridad física y ambiental para áreas seguras y equipos	1/05/19	22/08/19	CISO,GESTION ADMINISTRATIVA
Crear el procedimiento para Seguridad física y del entorno	1/12/19	31/01/20	CISO
Analizar y validar los controles implementados a nivel de Seguridad física y ambiental, dando cumplimiento a la norma ISO 27001:2013	1/12/19	31/01/20	CISO, VIGILANCIA, GESTION ADMINISTRATIVA, RECURSOS HUMANOS
Revisar y ajustar controles establecidos sobre equipos de cómputo y cableado.	16/09/19	30/11/19	CISO
Establecer, configurar y promover políticas de escritorio y pantalla limpia	16/09/19	30/11/19	CISO;ADMINISTRADOR ACTIVE DIRECTORY
A.12 Seguridad de las Operaciones	**15/01/19**	**31/03/20**	
Afinamiento y administración en la configuración de las herramientas de Seguridad para mejorar y optimizar el monitoreo	12/04/19	12/04/19	CISO
Valida toma y respaldo de logs para sistemas de información y plataformas críticas, y toma de logs de	2/09/19	31/12/19	CISO

auditoria para roles de usuarios administradores y operadores de sistemas			
Evaluar proyecto sobre herramienta para análisis de log y correlación de eventos	1/03/19	28/03/19	CISO,COORDINADOR DE AREA SISTEMAS
Revisar y ajustar procedimiento de backup , frecuencias de backup y pruebas periódicas de medios de backup	1/12/19	31/01/20	CISO
Validar separación de entornos de desarrollo de sistemas de información, con sus correspondientes roles y permisos, logs y manejo de data de prueba	10/06/19	15/08/19	CISO, COODINADOR DE APLICACIONES
Validar controles de instalación de software y restricciones de herramientas system 32 en equipos de computo	1/02/19	28/02/19	CISO
Implementar Cambio de Antivirus	2/09/19	31/12/19	CISO
Implementar DLP para equipos de usuario Final	1/11/19	31/01/20	CISO
Implementar DLP para Office 365	1/11/19	28/02/20	CISO
Implementar Nueva Herramienta Antispam	1/12/18	31/01/19	CISO
Asegurar Sincronización de relojes para servidores y equipos de computo	1/03/20	31/03/20	CISO
Hacking Ético	**1/08/19**	**31/12/20**	
Elaborar Estudios Previos de ejercicios de hacking Ético 2019	1/08/19	31/09/19	CISO
Ejecución hacking ético SAP	15/11/19	31/01/20	CISO
Elaborar Estudios Previos de ejercicios de hacking Ético 2020	1/06/20	31/07/20	CISO
Ejecución hacking ético: Redes y Servicios de Apoyo + retesting SAP	01/11/20	31/12/20	CISO
A.7 Seguridad de los Recursos Humanos	**19/06/19**	**31/03/20**	
Analizar y validar los controles implementados a nivel de Seguridad de los Recursos Humanos, dando cumplimiento a la norma ISO 27001:2013.	19/06/19	30/08/19	CISO, RRHH
Adecuar los procedimientos para la Seguridad de los Recursos Humanos , antes y durante la contratación,	1/09/19	31/03/20	CISO, RRHH

y al cese o cambio de puesto de trabajo, con la puesta en marcha de aplicativo prodata			
A.13 Seguridad de las Comunicaciones	**28/01/19**	**31/07/20**	
Crear la política y el procedimiento para la Seguridad de las redes y las Comunicaciones	1/11/19	31/12/19	CISO; Outsourcing Sistemas
Revisar la arquitectura de red de la Entidad para identificar oportunidades de mejora	1/02/19	7/03/19	CISO, COORDINADOR DE AREA DE SISTEMAS
Evaluar proyecto para administración segura de puertos de red y aplicación de políticas BYOD	1/02/19	7/02/19	CISO, COORDINADOR DE AREA DE SISTEMAS
Evaluar proyecto de implantación de herramientas IDS, IPS y WAF para detección y restricción proactiva de trafico sospechoso de red y portal web	28/01/19	1/02/19	CISO, LIDER DE REDES
Implementar NAC (Network Access Control)	1/12/19	28/04/20	CISO;CONTRATISTA REDES
Implementación de Firewall de Nueva Generación	2/07/19	30/08/19	CISO;ESPECIALISTA OUTSOURCING
Implementación de Visibilidad y analítica de seguridad	24/05/19	15/09/19	CISO
Implantar IPS	1/08/19	14/10/19	CISO
IMPLANTAR DDOS	1/08/19	31/10/19	CISO
Implantar control de aplicaciones	15/09/19	31/12/19	CISO
Realizar revisión y emitir la política y recomendaciones para la transferencia de información	1/01/20	1/03/20	CISO
Revisión e implantación de nuevas restricciones de navegación	31/07/19	30/09/19	CISO;COMITE TECNOLOGIA
Diseño de nueva estructura de Active Directory	1/07/19	27/08/19	CISO
Identificar riesgos y requerimientos de seguridad para el proyecto de Transición y Aseguramiento de protocolo IPV6	18/02/19	28/02/19	CISO, ARQUITECTO EMPRESARIAL, LIDER DE REDES Y COMUNICACIONES
Implantar Herramienta de Monitoreo de red y disponibilidad con 500 sensores	1/09/19	31/01/20	CISO;COORDINADOR DE REDES Y HARDWARE

Implantar Herramienta de Administración de redes y switches	1/02/20	31/04/20	CISO;COORDINADOR DE REDES Y HARDWARE
Migrar Vlans A Switchs Core implantando nueva arquitectura de Seguridad	1/02/19	31/03/19	CISO;COORDINADOR DE REDES Y HARDWARE;CONTRATISTA REDES
Implantación y Aseguramiento de Protocolo IPV6	1/02/20	31/07/20	CISO;ADMINISTRADOR ACTIVE DIRECTORY;ADMINISTRADOR DE SEGURIDAD INFORMATICA;CONTRATISTA REDES
A.9 Control de Accesos	**1/11/19**	**31/05/20**	
Definir procedimiento estándar para el control de accesos	1/11/19	31/01/20	CISO
Revisar, definir y gestionar las mejoras correspondientes para la administración de usuarios en las diferentes aplicaciones y plataformas.	1/02/20	30/04/20	CISO, COORDINADOR DE APLICACI0NES
Socializar la creación y uso de matrices a líderes de proceso	1/05/20	31/05/20	CISO; Lideres Grupo Area
A.10 Criptografía	**15/08/19**	**29/02/19**	
Crear el procedimiento para gestión de Criptografía	01/01/20	29/02/20	CISO
Documentar la administración de las llaves de cifrado para VPN.	1/09/19	30/12/19	CISO
Evaluar y desplegar herramienta para la administración centralizada y cifrada de contraseñas	15/08/19	31/10/19	CISO,COORDINADOR DE AREA SISTEMAS
Actualización de certificados digital para el portal web, servicio de correo webmail, pagos virtuales (donaciones), intranet y SIAPINC, redcap, SIAI, campus virtual y demás subdominios y aplicativos, incluyendo corrección de código para cada Sistema	01/11/19	31/12/19	CISO,COORDINADOR DE AREA SISTEMAS, COORDINADOR DE APLICACIONES
Implementar cifrado de discos para todo los equipos del instituto por medio de chip TPM	15/09/19	15/12/19	MESA DE AYUDA;CISO
Implantar nueva herramienta de cifrado y compresión licenciada en equipos de computo	23/09/19	15/12/19	MESA DE AYUDA;CISO
A.16 Gestion de Incidentes de seguridad de la información	**1/08/19**	**29/02/20**	

Definir y/o actualizar procedimiento definido para la Gestión y atención de Alertas para Incidentes y Eventos de seguridad y privacidad	1/08/19	30/09/19	CISO;LIDER MESA DE AYUDA;COORDINADOR DE REDES Y HARDWARE
Construir base de conocimiento de seguridad de la información, y establecer procesos de análisis periódico para generar lecciones aprendidas	1/08/19	31/12/19	MESA DE AYUDA;CISO
Diseñar y generar informes de vulnerabilidades y Amenazas como resultado del monitoreo de seguridad	1/08/19	30/09/19	CISO;PROVEEDORES
Evaluar y establecer procedimientos de identificación, recolección, adquisición y preservación de evidencia en casos de materialización de eventos de SI (Informática forense).	1/11/19	29/02/20	CISO;ADMINISTRADOR DE SEGURIDAD INFORMATICA
Gestion de Proyectos	**15/01/20**	**31/08/20**	
Elaborar manual de requerimientos de Seguridad de la Información para proyectos	15/01/20	30/04/20	CISO
Apoyo en la definición de conceptos, recomendaciones y aplicación de buenas prácticas de seguridad en para supervisión de proyectos del INC.	01/05/19	31/08/20	Líderes Grupo Area; GESTORES DE PROYECTOS;GESTION DEL GASTO;CONTRATACION;CISO
Informática Forense	**01/05/20**	**30/11/20**	
Implantación de sistema de cadena de custodia basado en manual de cadena de custodia de la Fiscalía General de la Nación	01/05/20	30/11/20	CISO, ADMINISTRADORES DE APLICACIONES;
Continuidad de Negocio	**1/12/19**	**7/07/20**	
Elaboración de manual de Contingencias Informáticas	**01/01/20**	**01/05/20**	
Revisar y documentar los sistemas de redundancia de las instalaciones de procesamiento.	1/01/20	1/02/20	CISO;ADMINISTRADOR DE SEGURIDAD INFORMATICA; Especialista Continuidad de Negocio; GRUPO APLICACIONES
Definir los controles a implementar en el ambiente de contingencia.	23/03/20	31/05/20	CISO; ADMINISTRADOR DE SEGURIDAD INFORMATICA; Especialista Continuidad de

			Negocio; GRUPO APLICACIONES
Definir el plan de monitoreo de Usuarios y plataformas en ambiente de contingencia.	23/03/20	31/05/20	CISO;ADMINISTRADOR DE SEGURIDAD INFORMATICA; Especialista Continuidad de Negocio; GRUPO APLICACIONES
Documentar y formalizar el plan de Contingencias Informáticas para los procesos críticos del INC , y diseño de formato de pruebas (Evaluar Consultoría)	1/02/20	01/05/20	CISO;ADMINISTRADOR DE SEGURIDAD INFORMATICA; Especialista Continuidad de Negocio; GRUPO APLICACIONES
Pruebas CRD	**01/04/20**	**25/12/20**	
Ejecutar pruebas de plan de contingencia 1er semestre 2019 de TI de sistemas tecnológicos – CRD SAP	1/04/19	31/05/19	CISO;GRUPO APLICACIONES
Ejecutar pruebas de plan de contingencia 2do semestre 2019 de TI de sistemas tecnológicos – CRD SAP	1/11/19	25/12/19	CISO;ADMINISTRADOR DE SEGURIDAD INFORMATICA;GRUPO APLICACIONES
Continuidad de Negocio	**01/06/20**	**31/03/21**	
Elaboración de BIA	1/06/20	15/09/20	PLANEACION; ESPECIALISTA DE CONTINUIDAD (PLANEACION); LIDERES DE AREA;SUBDIRECTORES;DIRECCION;CISO(DRP)
Elaboración de Plan de Continuidad de Negocio	16/09/20	31/03/21	PLANEACION; ESPECIALISTA DE CONTINUIDAD (PLANEACION); LIDERES DE AREA;SUBDIRECTORES;DIRECCION;CISO(DRP)
Habeas Data (Gestion Manejo de datos Personales)	**4/01/19**	**31/12/20**	

Revisión Documental de tratamiento de datos Personales	**04/01/19**	**20/12/19**	
Actualización Levantamiento de controles de Bases de datos y Sistemas de Información	04/01/19	28/02/19	GESTION DOCUMENTAL;CISO
Actualización / Publicación de política de tratamiento de manejo de datos personales	01/08/19	31/10/19	GESTION DOCUMENTAL;CISO
Revisión de Documentación Jurídica para blindaje de tratamiento de datos Personales	21/07/19	30/11/19	GESTION DOCUMENTAL;CISO;JURIDICA
Revisión de mecanismos de comunicación de manejo de datos personales	12/11/19	20/12/19	GESTION DOCUMENTAL;CISO
Despliegue Controles de Habeas Data	**01/09/19**	**31/01/20**	
Generación de Avisos de video vigilancia	01/10/19	15/11/19	CISO; COMUNICACIONES
Intervención / Actualización de recolección de autorizaciones para manejo de datos personales	01/10/19	31/12/19	GESTION DOCUMENTAL;CISO
Capacitación y despliegue de manual interno y herramientas de manejo de datos personales	01/09/19	30/12/19	GESTION DOCUMENTAL;CISO
Establecimiento de Acuerdos de Confidencialidad para empleados y terceros	01/11/2019	31/01/20	GESTION DOCUMENTAL;CISO;TALENTO HUMANO, COORDINADORES DE EMPRESAS TERCERIZADAS
Revisar aplicación de Circular externa Conjunta No -04 de 05 de sept de 2019 (SIC)	01/10/19	31/12/19	GESTION DOCUMENTAL;CISO
Actualizar Registro Nacional de Base de datos	**01/11/19**	**15/01/21**	**GESTION DOCUMENTAL;CISO**
Actualización Registro Nacional de Base de datos 2019	01/11/19	15/01/20	CISO;OEM; GESTION DOCUMENTAL
Actualización Registro Nacional de Base de datos 2020	01/11/20	15/01/21	CISO;OEM; GESTION DOCUMENTAL
Ciberdefensa y Cibersegruidad de infraestructura critica	**15/01/19**	**31/12/20**	
Participación elaboración Guía sobre ciberdefensa y ciberseguridad del sector Salud	15/01/19	23/08/19	CISO;MESA DE TRABAJO MIN SALUD
Identificación y Aseguramiento de Infraestructura critica en el INC	01/04/20	31/12/20	CISO;MESA DE TRABAJO MIN SALUD

Participación en elaboración de manual del operador de sector salud	01/07/19	31/07/20	CISO;MESA DE TRABAJO MIN SALUD

19. DIVULGACIÓN DEL SGSI

El Plan de capacitación y sensibilización en seguridad de la información para el Instituto Nacional de Cancerología ESE (INC) define las estrategias que conducen a la preservación de la confidencialidad, integridad, y disponibilidad de sus activos de información, por medio de la sensibilización capacitación y comunicación de las reglas de comportamiento adecuadas para el uso de los sistemas y de los activos de la información, y de la privacidad y del manejo de datos personales del ciudadano, paciente y cliente interno dentro y fuera del INC

Análisis DOFA (Debilidades, Amenazas, Fortalezas y Oportunidades) sobre divulgación de SGSI

FACTORES INTERNOS DE LA EMPRESA

	DEBILIDADES (-)
1	La entidad debe fortalecer los programas de divulgación y sensibilización a los Funcionarios y/o Contratistas, proveedores y terceros frente al SGSI.
2	La entidad carece de visibilidad para seguimiento y monitoreo de plan de sensibilización de seguridad para verificar la efectividad y eficacia del mismo.
3	La entidad debe fortalecer el plan de tratamiento de los riesgos que afecten el SGSI, incluyendo riesgos de seguridad digital, ciberdefensa y ciberseguridad.
4	Alta rotación del personal operativo responsable de los procesos
5	El instituto carece de seguimiento a los Funcionarios y/o contratistas, proveedores y terceros frente al cumplimiento del SGSI.
6	Rotación del personal operativo responsable de plataformas, debido a cambio de Outsourcing y cambio de tecnología de seguridad de la información.
7	Resistencia al cambio y al control
8	Baja penetración de los medios establecidos para la sensibilización, según registros de 2018

FACTORES EXTERNOS A LA EMPRESA

	AMENAZAS (-)
1	Apropiarse de los cambios normativos y legislativos vigentes que afecten el SGSI.
2	Mantenerse actualizado con las evoluciones tecnológicas en seguridad informática.
3	Dar cumplimiento a los requisitos de los entes de control.
4	Dar cumplimiento al Manual del SGSI y a las políticas de seguridad y privacidad de la información
5	Ataques cibernéticos a la infraestructuras criticas del Instituto
6	
7	
8	

	FORTALEZAS (+)
1	Personal calificado, rigurosidad técnica y con habilidades de liderazgo.
2	Programas de sensibilización y transferencia de conocimiento actualizados e implementados.
3	Se cuenta con Sistemas de Gestión Integrados, que permite comunicar varios procesos y hacerlos parte integral del mismo.
4	Implementación del SGSI que promueve la confidencialidad, Integridad y Disponibilidad de la información para los clientes internos (Funcionarios y/o Contratistas) y Externos (Entidades, proveedores, etc.).
5	Adecuaciones de redes y comunicaciones y seguridad para adopción de protocolo IPV6
	Se estableció plan de Adopción de protocolo IPV6

	OPORTUNIDADES (+)
1	Aprender de los incidentes conocidos ocurridos en otras Entidades y Organizaciones del sector.
2	Mantener comunicación activa con Organismos o Entidades Externas frente a temas de Seguridad que permite ampliar el panorama y la visión para la Entidad.
3	Lograr que los objetivos de la Entidad se cumplan con un alto nivel de Seguridad en el manejo de la Información.
4	Participar entre las Entidades Públicas que hayan adoptado la metodología MSPI e ISO 27001:2013 mediante la apropiación de una Cultura del SGSI.
5	

Cronograma de Implantación de Plan de Sensibilización y capacitación en Seguridad de la información

Id	Nombre de tarea	Comienzo	Fin
0	**PLAN DE CAPACITACION Y SENSIBILIZACION EN SEGURIDAD DE LA INFORMACION**	**vie 15/02/19**	**vie 6/12/19**
1	**PLANEACIÓN**	**2/07/19**	**vie 9/08/19**
2	**Identificación de necesidades de capacitación**	**2/07/19**	**vie 9/08/19**
3	Alineación de metodología con MSPI Minitic	lun 8/07/19	lun 8/07/19
4	Análisis Dofa	vie 12/07/19	vie 12/07/19
5	Definición de Perfiles y Necesidades	lun 15/07/19	vie 19/07/19
6	Definición de metas de capacitación	16/07/19	mié 17/07/19
7	Diseño de la estrategia	lun 22/07/19	vie 26/07/19
8	Definición de Metas	lun 29/07/19	lun 29/07/19
9	Definición de temáticas de capacitación y sensibilización	lun 29/07/19	30/07/19
10	Definición de medios y estrategias de Comunicación	2/07/19	2/07/19
11	Aprobación de la estrategia	30/07/19	mié 31/07/19
12	Elaboración de Cronograma de Implementación	vie 9/08/19	vie 9/08/19
13	Entregable: Estrategia de Implementación	vie 9/08/19	vie 9/08/19
14	**DISEÑO**	**jue 28/02/19**	**mié 14/08/19**
15	**Diseño de Material de Capacitación INC**	**jue 28/02/19**	**vie 2/08/19**
16	Diseño textos de campañas seguridad de la información	jue 28/02/19	dom 31/03/19

17	Creación de Piezas e imágenes	mié 1/05/19	mié 31/07/19
18	Validación de Piezas e imágenes	mié 31/07/19	vie 2/08/19
19	Entregable: Piezas con Imágenes corporativas para despliegue	vie 2/08/19	vie 2/08/19
20	**Creación de Piezas e imágenes Sensibilización Gestión de seguridad Outsourcing**	**mié 24/07/19**	**mié 14/08/19**
21	Diseños Personaje Seguridad Campaña Expectativa	mié 24/07/19	13/08/19
22	Validación de Piezas e imágenes	mié 14/08/19	mié 14/08/19
23	Entregable: Piezas con Imágenes corporativas para despliegue	mié 14/08/19	mié 14/08/19
24	**DESARROLLO**	**vie 15/02/19**	**vie 29/11/19**
25	**Capacitaciones Internas / Transmisión de conocimiento**	**vie 15/02/19**	**jue 29/08/19**
26	**Capacitación IPV6**	**vie 15/02/19**	**lun 25/02/19**
27	Jornada 1 - Capacitación Interna IPV6 -Password	vie 15/02/19	vie 15/02/19
28	Jornada 2 - Capacitación Interna IPV6 -Password	lun 25/02/19	lun 25/02/19
29	Sensibilización proyecto IPV6 para el INC + Phishing	19/02/19	19/02/19
30	**Workshop Fortinet - Fortiguard**	**jue 29/08/19**	**jue 29/08/19**
31	Jornada 1 workshop Fortigate	jue 29/08/19	jue 29/08/19
32	Jornada 2 workshop Fortigate	jue 29/08/19	jue 29/08/19
33	**Capacitación Usuario**	jue 11/04/19	vie 29/11/19
34	**GESTIÓN DEL CAMBIO - PROYECTO OUTSOURCING - CAMBIO PLATAFORMA SEGURIDAD**	**vie 19/07/19**	**vie 1/11/19**
39	Capacitación manejo de datos personales	jue 11/04/19	jue 11/04/19
40	Sensibilización para Dirección -Manejo datos Personales	vie 20/09/19	vie 20/09/19
41	**Despliegue en pantallas Multivisual - Capacitación Seguridad de la Información**	**lun 9/09/19**	**vie 15/11/19**
45	Qué hacer ante la pérdida de dispositivos móviles	mié 12/06/19	vie 14/06/19
46	Capacitación 5 Estafas Cibernéticas que todos deben Conocer en el INC	vie 26/07/19	lun 29/07/19
47	Capacitación en Estándar de Gerencia de la Información	6/08/19	6/08/19
48	**Sensibilizaciones SGSI**	**25/06/19**	**vie 29/11/19**
49	Jornada Sensibilización Seguridad de la información y Riesgo Digital	lun 25/11/19	vie 29/11/19
50	Sensibilización en seguridad Comité Administrativo	lun 15/07/19	vie 26/07/19
51	Sensibilización Nueva política de Seguridad de la información	vie 4/10/19	vie 11/10/19
52	Sensibilización para Jornada de Acreditación	25/06/19	mié 26/06/19
53	Despliegue de tapices de escritorio	15/10/19	jue 31/10/19
54	**SEGUIMIENTO**	**lun 2/12/19**	**vie 6/12/19**
55	Aplicación Encuesta- Estado de apropiación de seguridad de la información	lun 2/12/19	vie 6/12/19
56	Reevaluación de Material Creado	mie 15/01/20	vie 30/01/20

20. IDENTIFICACIÓN DE RIESGOS DE PROYECTO

- **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.

- **Rotación de personal de proyecto**
  Impacto: Medio
  La rotación de personal del personal clave impacta el tiempo de proyecto, ya que se requiere un tiempo prudencial para el entrenamiento y conocimiento de los procesos completos del cargo. El sistema de gestión de calidad mitiga pérdida de conocimiento ya que se observa un árbol documental y de procesos maduro

- **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.

- **Resistencia al cambio y al control**
  Impacto: Medio
  El cambio y fortalecimiento de controles puede representar una ruptura en la cultura para algunos empleados que se pueden negar a seguir los nuevos lineamientos, retrasando las labores y obstaculizando el trabajo seguro de los demás. Se requiere el apoyo de la dirección y el uso de mecanismos como resoluciones y seguimiento de control interno para asegurar el cumplimiento de política y controles.

- **Gestión de Transparencia de Gobierno vs seguridad**
  Impacto: Alto
  La publicación de información de contratación debido a la obligación de cumplimiento de normatividad de transparencia en sector gobierno se identifica como un riesgo de seguridad ya que los atacantes tienen disponible la información sobre las herramientas implementadas y el conocimiento sobre los módulos y requerimientos de configuración estándar realizados por Colombia Compra para sistemas relacionados con seguridad.

21. CONTROL DE CAMBIOS

ELABORÓ		REVISÓ		APROBÓ	
Cargo:	Profesional especializado I	Cargo:	Coordinador	Cargo:	
Nombre	Carlos Andres Guerrero	Nombre	Luis Eduardo Martínez	Comité	Comité de Tecnología
Dependencia:	Grupo Área de Sistemas	Dependencia:	Grupo Área de Sistemas	Dependencia:	Dirección General
Fecha:	12-07-2019	Fecha:	19--07-2018	Fecha:	05-09-2019

INDICE DE MODIFICACIONES				
Versión	**Responsable**	**Cargo**	**Fecha**	**Descripción**
1.0	Carlos Andres Guerrero	Profesional especializado I – oficial de seguridad de la información	09/07/2016	Creación del documento
2.0	Carlos Andres Guerrero	Profesional especializado I – oficial de seguridad de la información	09/07/2016	Actualización del plan 2019-2020