ANEXO. ESPECIFICACIONES TÉCNICAS MÍNIMAS

ELABORACIÓN DEL ANÁLISIS DEL ESTADO ACTUAL DEL SISTEMA DE SEGURIDAD DE LA INFORMACIÓN EN LA IMPRENTA NACIONAL DE COLOMBIA QUE INCLUYE LA ENTREGA DE LOS DOCUMENTOS TÉCNICOS INDICADOS EN EL ANEXO TÉCNICO E IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LOS PROCESOS DE GESTIÓN COMERCIAL, GESTIÓN DE PRODUCCIÓN, GESTIÓN FINANCIERA Y GESTIÓN INFORMÁTICA

1. ESPECIFICACIONES TECNICAS

Para permitir el cumplimiento de los objetivos trazados, el proyecto se desarrollará en etapas utilizando la metodología de implementación propuesta por la ISO (Organización Internacional de Normalización) para Sistemas de Gestión de Seguridad de la Información.

A continuación se encuentran las especificaciones técnicas mínimas para cada una de las etapas definidas:

E1 - Análisis GAP Diagnóstico ISO 27001 & ISO 27002	
El análisis GAP (análisis de brechas) es un estudio formal con respecto a los niveles de seguridad implementados actualmente por la entidad y aquellos hacia los cuales se desea llegar en un futuro cercano. ▪ Debe asegurar la revisión y medición del nivel de madurez de la entidad con respecto a la seguridad de la información. ▪ Provee un indicativo del esfuerzo, tiempo, dinero y recursos humanos que van a ser requeridos para obtener ese objetivo deseado. ▪ Constituye el punto de arranque de la definición de una estrategia de la arquitectura de seguridad de la información, perfectamente alineada con la visión de la entidad, dentro de su entorno de operación.	
Actividad	**Descripción**
	Realizar el análisis bajo tres perspectivas: procedimental, tecnológica y de talento humano y de esta manera se presentarán los resultados de esta actividad.

E1.1	Para ello debe emplear los criterios de cumplimiento establecidos en la norma 27001:2013 e ISO 27002:2013 establecidos por la organización internacional de estándares ISO, específicamente en los aspectos y mejores prácticas que deberían tener las organizaciones para tratar los temas de seguridad de la información.
E1.2	Realizar el levantamiento de información y el análisis de cumplimiento y diferencia con respecto a los controles y objetivos de control que se encuentran distribuidos en los catorce (14) dominios de la ISO/IEC 27002:2013.
E1.3	Realizar un análisis GAP de la documentación y procedimientos actuales de la Imprenta Nacional de Colombia para el manejo de su modelo de seguridad en cuanto: ▪ **Documentación de Nivel 1** ✓ Documentos de: Estructura de gestión, incluyendo la política de seguridad de la información, los objetivos de control y los controles procedimentales. ▪ **Documentación de Nivel 2** ✓ Procedimientos acotados para implantar al detalle los controles procedimentales necesarios. Describen quién, qué, cuándo y donde se localizan los procedimientos de seguridad y los controles. ▪ **Documentación de Nivel 3** ✓ Documentos con tareas o actividades específicas que incluyen mayor detalle en instrucciones de trabajo, formularios, flujogramas, normas de servicios y manuales de sistemas. ▪ **Documentación de Nivel 4** ✓ Registros de las actividades ejecutadas en conformidad con los niveles de la documentación de nivel 1, 2 y 3 y lo exigido para un SGSI.
E1.4	Hacer entrega de: ▪ Análisis de la información para el desarrollo de un informe de resultados de evaluación y diagnóstico, en donde se indican los resultados por cada dominio de la norma ISO/IEC 27002:2013, este informe incluye: ✓ Resultados por dominio de la norma y para cada objetivo de control (representados en gráficos y tablas de datos). ✓ Observaciones (Evidencias, hallazgos, comentarios). ✓ Recomendaciones (oportunidades de mejora). ▪ Análisis de la información para el desarrollo de un informe de resultados de evaluación y diagnóstico de revisión documental del modelo actual de seguridad de la información, este informe incluye: ✓ Nivel de cumplimiento de la documentación con respecto a la norma. ✓ Observaciones (Evidencias, hallazgos, comentarios).

	✓ Recomendaciones (oportunidades de mejora).
E2 – Gestión de Activos de Información (levantamiento, inventario y clasificación de activos de información, caracterización de Usuarios e índice de información clasificada y reservada)	
Mediante la definición de un Inventario se especifica y se reconocen los activos de información que se deben clasificar y proteger. El inventario debe permitir identificar los activos de información a los que se les debe brindar protección. Las actividades realizadas para obtener un inventario de activos son un prerrequisito de la gestión de riesgos de seguridad de la información. La clasificación de activos de información tiene como objetivo asegurar que la información recibe los niveles de protección adecuados. La información con base en su valor y de acuerdo a los requisitos de confidencialidad tiene diferentes grados de protección o manejo especial que se definen en la clasificación de activos de información, por lo cual es importante contar con una caracterización de usuarios. Se debe definir el esquema de clasificación para estipular los niveles de protección para cada activo de información y señalar así las consideraciones especiales de manejo, restricciones, esquema de publicación, almacenamiento y destrucción de la información. Se efectuara el inventario para los procesos que se encuentren aprobados al momento del inicio de la ejecución contractual. A la fecha son un total de catorce (14) procesos, discriminados así: Cinco (5) de Dirección, dos (2) misionales y siete (7) de apoyo.	
Actividad	**Descripción**
E2.1	Realizar un inventario de los activos de información que apoyan los diferentes procesos de negocio de la Imprenta Nacional de Colombia**.**
E2.2	Dar cumplimiento a los lineamientos definidos en la norma *ISO/IEC 27002* en el ítem de "*Gestión de Activos*".
	Realizar entrevistas con el personal de la Imprenta Nacional de Colombia y levantamiento de información de procesos del negocio, tablas de retención documental y procedimientos en general que permitan identificar la siguiente información: ▪ *Nombre del Activo*: Es un campo que define la manera como se va a reconocer el activo de información dentro de la Imprenta Nacional de Colombia con un nombre particular y diferenciable. ▪ *Tipo*: Se define el tipo al cual pertenece el activo, para este campo se utilizan los siguientes valores:

E2.3	✓ *Información*: Bases de datos y archivos de datos, contratos y acuerdos, documentación del sistema, información sobre investigación, manuales de usuario, procedimientos operativos o de soporte, planes para la continuidad del negocio, acuerdos sobre retiro, pruebas de auditoría e información archivada, entre otra información crítica que se encuentre en medio físico. ✓ *Software*: Software de aplicación, software del sistema, herramientas de desarrollo y utilidades de la Imprenta nacional de Colombia. ✓ *Físico*: Equipos de computación, equipos de comunicaciones, medios removibles y otros equipos. ✓ *Servicio*: Servicios de computación y comunicaciones. ✓ *Datos Personales*: De acuerdo con lo estipulado en la Ley 1581 incluir la clasificación de Dato Personal. ▪ *Ubicación*: Es la información acerca de donde se encuentra físicamente ubicado el activo de información, puede ser un archivo físico de oficina, archivo digital, sistema de información, computador, base de datos, o aplicación. ▪ *Propietario*: Es la persona que tiene la responsabilidad de disponer del activo de información de la Imprenta Nacional de Colombia, y de determinar cuáles son los requisitos para que el mismo se salvaguarde ante accesos no autorizados, modificación, pérdida de la confidencialidad o destrucción deliberada. ▪ *Custodio Técnico*: Es la persona encargada de administrar y hacer efectivos los controles de seguridad que el propietario del activo ha definido, con base en los controles de seguridad disponibles en la Imprenta nacional de Colombia. ▪ *Valor*: Es el valor del activo para el negocio. Su medición es cualitativa.
E2.4	Definir el Instructivo para el proceso de inventario de activos de información.
E2.5	Índice de información clasificada y reservada.
E2.6	Formular las recomendaciones para la revisión, gestión y actualización del inventario de activos de información.
E2.7	Definir los niveles de clasificación y de confidencialidad, y las recomendaciones de manejo asociadas en cuanto a : ▪ Acceso permitido. ▪ Esquema de publicación. ▪ Restricciones en la publicación electrónica. ▪ Almacenamiento y archivado. ▪ Disposición y destrucción.

	▪ Penalizaciones por revelación o alteración deliberada o inadvertida de la información.
E2.8	Definir el instructivo de clasificación de activos de información.
E2.9	Formular las recomendaciones para la revisión, gestión y actualización de la clasificación de la información.
E2.10	Hacer entrega de: ▪ Informe de resultados del levantamiento de información. ▪ Inventario de activos de información de la Imprenta Nacional de Colombia. ▪ Instructivo de clasificación de activos de información de la Imprenta Nacional de Colombia y su nivel de clasificación, incluyendo las recomendaciones en cuanto: ✓ Acceso permitido. ✓ Esquema de publicación. ✓ Restricciones en la publicación electrónica. ✓ Recomendaciones a cerca del Almacenamiento y/o archivado. ✓ Recomendaciones a cerca de su disposición y destrucción. ✓ Penalizaciones por la revelación, acceso no autorizado, alteración deliberada o inadvertida de la información clasificada (para los casos en que apliquen penalizaciones disciplinarias y/o legales por parte de la Imprenta Nacional de Colombia). ▪ Activos de información clasificados, según inventario e instructivo de clasificación. ▪ Caracterización de Usuarios. ▪ Índice de información Clasificada y Reservada.
E3 - Gestión de Riesgos (Análisis y Evaluación de Riesgos)	
La metodología de Análisis de Riesgos utilizada deberá basarse como mínimo en las normas ISO27005 (gestión del riesgo en la seguridad de la información) y acoger las recomendaciones de la ISO/IEC 27002 e ISO/IEC 27001 aplicables.	
Actividad	**Descripción**
E3.1	Determinar las amenazas potenciales asociadas a los sistemas de información de la Imprenta Nacional de Colombia, para determinar la probabilidad de que una amenaza se materialice en un ataque a los sistemas de información a través de una vulnerabilidad, y el impacto que esto puede tener en la Entidad.
E3.2	Identificar los controles necesarios para minimizar o transferir los riesgos identificados y priorizados. Controles a nivel de tecnología o procedimientos.

E3.3	Llevar a cabo el análisis de amenazas basado en un análisis cuidadoso de todos los actores que interactúan con los sistemas, las posibles vulnerabilidades de los sistemas, y de los controles de seguridad existentes. (Explicar actividades y/o metodología para realizar el análisis).
E3.4	Llevar a cabo un análisis de controles para identificar y medir de manera cualitativa, el desempeño y las capacidades de los controles de seguridad que han sido implementados o que se planean implementar en el sistema de información para minimizar o eliminar la probabilidad de que una amenaza se materialice a través de una vulnerabilidad del sistema, y definir los controles necesarios para protegerlo de manera adecuada. (Explicar actividades y/o metodología para realizar la etapa de análisis de controles).
E3.5	Para el Análisis de Controles se deberá incluir los catorce (14) dominios cubiertos por la norma, haciendo énfasis en: ▪ Definición del esquema de Autenticación, Autorización y Auditoria (AAA) para el control de acceso a los sistemas de información y plataforma tecnológica. ▪ Definición de seguridad perimetral para la conexión a Internet y conexiones a redes WAN. ▪ Definición de conectividad segura (Encripción, VPN, Acceso Remoto). ▪ Definición de controles de seguridad para la red interna. ▪ Definición del esquema de monitoreo de la seguridad en la infraestructura. ▪ Definición del sistema de administración Centralizada de controles de seguridad (procedimiento).
E3.6	Llevar a cabo un completo análisis de vulnerabilidades para determinar las debilidades reales existentes en los sistemas de información, en sus componentes Tecnológicos (software, hardware), humano y organizacional. Mediante el análisis de vulnerabilidades se deben determinar las fallas existentes en los sistemas de información que pueden ser utilizadas para vulnerar efectivamente su seguridad física y lógica. Esta evaluación deberá realizarse para detectar vulnerabilidades de todos los servicios a nivel externo e interno (explicar actividades y/o metodología para realizar el análisis de vulnerabilidades).
E3.7	Entregar el diseño que contiene todos los ítems descritos para la implementación en la red, con sus características y la descripción técnica de la función de cada uno de ellos en la arquitectura propuesta y las interacciones que existen entre los elementos de la arquitectura.

E3.8	Entregar el diseño para máximo ocho (8) requerimientos de los equipos necesarios para la implementación de la arquitectura de seguridad, plasmados en los RFP (pre pliegos) iniciales, de acuerdo a las necesidades de la Imprenta Nacional de Colombia y basados en los estándares técnicos recomendados independiente de marcas en el mercado. Para esto se deberán definir cantidades, características y descripción de cada una de las características requeridas.
E3.9	Se debe llevar a cabo un análisis de impacto para lo cual se deberá realizar un estudio cuidadoso de la Entidad y su dependencia de la tecnología, la misión del sistema de información, su criticidad, y la sensibilidad de la información que contiene. A partir de este estudio, se deberá determinar el impacto cualitativo y cuantitativo por pérdida de integridad, disponibilidad y confidencialidad para los sistemas de información y para cada uno de sus componentes. El Análisis de impacto debe facilitar la clasificación de los procesos de negocio de acuerdo a su criticidad. El análisis debe incluir además el impacto reputacional, financiero, operativo, económico, o de responsabilidad social, identificando los que son cuantificables y los que no y las razones por lo cual no es posible tal cuantificación. (Explicar actividades y/o metodología para realizar el análisis de Impacto).
E3.10	Definir la determinación del riesgo a través de la realización de una matriz de niveles de riesgo, en la que se refleje la probabilidad de que un actor intente materializar una amenaza utilizando una vulnerabilidad dada, la magnitud del impacto en caso de que se vulnere el sistema, y el nivel de desempeño de los controles planeados o existentes, para reducir o eliminar el riesgo. (Explicar actividades y/o metodología para la determinación del riesgo).
E3.11	Posterior a la determinación del riesgo, se debe identificar en la matriz de niveles de riesgo los aspectos que deben ser asegurados, o cuyo aseguramiento debe ser reforzado en el sistema de información. Una vez se identifiquen estos aspectos, se deberá realizar todas las recomendaciones de controles necesarios para mitigar y/o transferir el riesgo. Esta etapa deberá retroalimentar el diseño de la arquitectura de seguridad propuesto.
E3.12	Hacer entrega de toda la documentación en donde quede plasmado el producto de todas las actividades exigidas en los presentes pliegos, además debe generar los siguientes entregables: ▪ Informe de identificación de controles necesarios para mitigar o transferir el riesgo. ▪ Informe completo del análisis de amenazas.

	▪ Informe completo del análisis de vulnerabilidades. ▪ Arquitectura de seguridad (De acuerdo a los requerimientos exigidos en estos pliegos). ▪ Informe de los resultados del análisis de impacto. ▪ Matriz de niveles de riesgo (De acuerdo a los requerimientos exigidos en estos pliegos). ▪ Reporte completo y detallado en el que se incluya: ✓ La descripción de las actividades llevadas a cabo para cada una de las fases. ✓ La información levantada en el proceso. ✓ Las conclusiones del estudio, y las todas las recomendaciones asociadas. (Toda la documentación deberá entregarse en idioma español).
E4 - Definición de Políticas de Seguridad de la Información	
Identificar los objetivos y los requerimientos corporativos con relación a la creación de las políticas, normas y procedimientos de seguridad para la Imprenta Nacional de Colombia, junto con sus oportunidades de mejoramiento y definir éstas de acuerdo a las mejores prácticas, con base en las normas ISO/IEC 27001:2013 e ISO 27002:2013.	
Actividad	**Descripción**
E4.1	Definir las Políticas, Normas y Procedimientos de seguridad que reflejen las necesidades de seguridad de la información para el negocio de la Imprenta Nacional de Colombia, así como todos los requerimientos estatales en seguridad de la información del Estado Colombiano e internacionales y que por ley deberían ser tenidos en cuenta.
E4.2	Los dominios mínimos sobre los cuales se deberá desarrollar las políticas, normas y procedimientos, con base en las normas ISO/IEC 27001:2013 e ISO 27002:2013, son los siguientes: ▪ Políticas de Seguridad corporativa. ▪ Organización de seguridad. ▪ Clasificación y control de activos. ▪ Seguridad del personal. ▪ Seguridad Física. ▪ Administración de Redes y Computadores. ▪ Sistemas de Control de Acceso. ▪ Mantenimiento y desarrollo de sistemas. ▪ Cumplimiento de políticas y normatividad legal.
E4.3	Para las políticas de seguridad de la información se debe definir:

	▪ Quién la crea. ▪ Quién la aprueba. ▪ Quién la implanta. ▪ Acciones para su despliegue e implantación. ▪ Definición de la Política.
E4.4	Para las normas se debe definir: ▪ Objetivo. ▪ Definición de la Norma. ▪ Comentarios y Requisitos para su implantación.
E4.5	Para los procedimientos se debe definir: ▪ Objetivo. ▪ Actividades. ▪ Recursos. ▪ Comentarios y Requisitos para su implantación.
E4.6	Definir la estructura de seguridad a lo largo y ancho de la Empresa que debe incluir las responsabilidades directas e indirectas de los funcionarios en seguridad de la información (Se deben definir específicamente: cantidad de personal, perfil, rol y responsabilidades).
E4.7	Definir los procesos para la continuidad y el mantenimiento del esquema de Políticas de Seguridad a implementar, a través de la definición de los procedimientos necesarios para el manejo de documentación, control de cambios y versiones, definiendo los roles y las responsabilidades del personal involucrado en el mantenimiento de las políticas de seguridad.
E4.8	Llevar a cabo previo al desarrollo de las Políticas, Normas y Procedimientos las siguientes actividades: ▪ Definición de requerimientos y restricciones. ▪ Se deberán tener en cuenta todos los aspectos que puedan afectar el desarrollo de las actividades involucradas en la metodología para la determinación de las Políticas, normas y procedimientos de Seguridad. ▪ Determinar la manera como se van a involucrar las áreas de las cuales se requiere información, con las que se va a interactuar y que van a hacer impactadas durante la ejecución del proyecto. ▪ Definición de los recursos utilizados para el proyecto.

	▪ Realizar todas las labores propias de la planeación de la ejecución del Proyecto y entregar un informe que contenga los resultados de cada uno de los componentes de la fase de planeación.
E4.9	Hacer entrega de: ▪ Documento de políticas, normas y procedimientos de Seguridad Informática (De acuerdo a los requerimientos exigidos en estos pliegos). ▪ Documento del proceso de mantenimiento, revisión, actualización y aprobación de políticas.
E5 - Gestión de Incidentes	
Es muy importante realizar una integración entre el proceso de seguridad informática y el proceso de atención de incidentes. El proceso de seguridad informática debe ser activado por el proceso de atención de incidentes. Lo anterior con el objetivo de realizar una verificación de la existencia de un incidente y de un adecuado tratamiento. Adicionalmente, el proceso de seguridad informática debe funcionar como una retroalimentación del proceso de atención de incidentes. La investigación debería arrojar el análisis detallado de nuevos ataques o fraudes informáticos para mejorar los procedimientos de análisis de incidentes.	
Actividad	**Descripción**
E5.1	Definir el proceso de seguridad informática y de atención de incidentes así como los procedimientos específicos de la Imprenta Nacional de Colombia.
E5.2	Definición de procedimientos para administradores: ▪ Procedimiento de Alta, Baja y Modificación (ABM) de usuarios. ▪ Procedimiento de Backup y recuperación de información. ▪ Procedimiento de Atención de Problemas. ▪ Procedimiento de Manejo de Eventos.
E5.3	Definición de procedimientos para usuarios: ▪ Procedimiento de Solicitud de acceso a recursos Informáticos. ▪ Procedimiento de escalamiento ante problemas de seguridad.
E5.4	Generación de Manuales de soporte procedimental para respuesta a incidentes.
E5.5	Definición de la documentación para el proceso que contenga: ▪ Análisis de capacidades de detección, contención y recuperación frente a incidentes. ▪ Definir la clasificación de incidentes (Tipos y niveles de servicio asociados dados por la Imprenta Nacional de Colombia).

	▪ Procedimientos de declaración y mecanismos de notificación de incidentes. ▪ Definición del procedimiento de Atención y Escalamiento de incidentes. ▪ Procedimientos de seguridad informática (recopilación, manejo, almacenamiento, procesamiento y protección de la evidencia digital). ▪ Contingencia y Recuperación frente a incidentes. ▪ Plan de Pruebas y simulacros.

E6 – Plan de Continuidad de Información y Tecnología	
Definir el plan de continuidad a nivel de tecnología e información para propender por la continuidad de procesos y operaciones del área de IT de la Imprenta Nacional de Colombia. Para esto se deberá definir y desarrollar un modelo en una serie de fases tendientes a tener como producto final un plan de continuidad de TI para su ejecución por parte de la Imprenta Nacional de Colombia.	
Actividad	**Descripción**
E6.1	Definir en el plan de Continuidad del Área de Tecnologías de la Información los siguientes elementos: ▪ Definición del problema. ▪ Objetivos y requerimientos del plan de continuidad. ▪ Costos de ejecución del plan de continuidad. ▪ Definición del comité de maneja del plan de continuidad. ▪ Políticas de continuidad del área de tecnología. (Explicar actividades y/o metodología para realizar esta fase)
E6.2	Definir en el plan los requerimientos funcionales mediante los siguientes elementos: ▪ Análisis de Riesgos y controles (con base en lo solicitado en E3.1) ▪ Análisis de impacto del negocio y funciones del negocio sensibles al tiempo. ▪ Estrategias alternativas de continuidad. ▪ Selección de estrategias con base en el análisis costo beneficio. ▪ Presupuesto requerido para la ejecución del plan de continuidad. (Explicar actividades y/o metodología para realizar esta fase)
E6.3	Para el diseño del plan se deberán definir los siguientes elementos: ▪ Alcance del plan y objetivos. ▪ Definición de tareas y responsables. ▪ Principales componentes del plan. ▪ Análisis de escenarios para la ejecución del plan. ▪ Definir los procedimientos para escalar, notificar y activar el plan de continuidad.

	▪ Definición de registros e información vital y programa de almacenamiento protegido (externo). ▪ Programa de administración del plan de continuidad. (Explicar actividades y/o metodología para realizar esta fase).
E6.4	Definir la manera como se va a llevar a cabo la implementación del plan y como mínimo debe incluir los siguientes elementos: ▪ Procedimientos de respuesta a emergencias. ▪ Delegación y designación de autoridad. ▪ Procedimientos detallados de reanudación, recuperación y restauración. ▪ Contratos con fabricantes y adquisición de recursos para la recuperación. (Explicar actividades y/o metodología para realizar esta fase).
E6.5	Definir los ensayos y pruebas a realizar para el Plan con mínimo los siguientes elementos: ▪ Programa de ensayo y objetivos. ▪ Plan de ensayo y escenarios. ▪ Evaluación del plan. ▪ Entrenamiento y plan de sensibilización. (Explicar actividades y/o metodología para realizar esta fase)
E6.6	Para el mantenimiento y actualización del plan se deberá definir los siguientes elementos: ▪ Agenda y presupuesto para la actualización y mantenimiento del plan de continuidad. ▪ Herramientas de software para actualización y mantenimiento del plan. ▪ Criterios de revisión. ▪ Estado del plan, reporte y auditoría. (Explicar actividades y/o metodología para realizar esta fase)
E6.7	Entregar un plan de acciones e inversiones que ayuden a mejorar la continuidad de los procesos más críticos de la Imprenta nacional de Colombia.
E6.8	Definir los tiempos mínimos de recuperación, tiempos máximos de tolerancia aceptados por los procesos, y estimar los recursos mínimos de operación y tiempos de entrega del servicio requeridos por la Imprenta Nacional de Colombia para mantener en operación sus procesos críticos.

E6.9	Hacer entrega de: ▪ Plan de acciones e inversiones que ayuden a mejorar la continuidad de los procesos más críticos. ▪ Documento de resultados de requerimientos funcionales. ▪ Documento de resultados del diseño del plan. ▪ Documento del plan y elementos para la implementación. ▪ Análisis de impacto del negocio y funciones del negocio sensibles al tiempo. ▪ Programa de administración del plan de continuidad. ▪ Procedimientos de respuesta a emergencias. ▪ Procedimientos detallados de reanudación, recuperación y restauración. ▪ Tiempos mínimos de recuperación, tiempos máximos de tolerancia aceptados por los procesos, y estimar los recursos mínimos de operación y tiempos de entrega del servicio requeridos.

E7 - Definición del Proceso de Administración de la Cultura de Seguridad de la Información	
Una cultura de seguridad que reconoce en los incidentes o materialización de los riesgos, una forma de actuar y conocer que tan inseguros son, es capaz de construir un lenguaje de seguridad, de percepción, no basado en una visión de invulnerabilidad tecnológica, sino en la confiabilidad de su reacción humana frente a la vulnerabilidad propia de los sistemas.	
Actividad	**Descripción**
E7.1	Llevar a cabo el entendimiento del estado actual del negocio en cuanto a cultura de Seguridad de la Información: ▪ Revisión de las Políticas de seguridad Corporativas y su nivel de cumplimiento. ▪ Identificación de situación actual a nivel de cultura en seguridad informática. ▪ Identificación de planes de capacitación en seguridad de la información.
E7.2	Definir la Estrategia de Implementación del Proceso, así como de los recursos que se deberán tener por parte tanto de la Imprenta Nacional de Colombia para llevarlas a cabo, considerando las siguientes actividades: ▪ Presentación del Plan de Sensibilización: Definir la presentación del plan a las directivas, mandos medios, y a la organización de la Imprenta Nacional de Colombia. ▪ Plan de Entrevistas: Definir la metodología y el personal de la Imprenta Nacional de Colombia que va a participar de las entrevistas, definir perfiles y los grupos de

	trabajo. Esta actividad debe ayudar a determinar el nivel actual de sensibilización en seguridad de la información del personal. ▪ Plan de Promoción: Definir la estrategia de promoción interna del Plan de Sensibilización y los recursos necesarios: ✓ Identificación de Objetivos de promoción del Plan de sensibilización. ✓ Identificación de los recursos de apoyo requeridos. ▪ Plan de Comunicación y divulgación: Determinar los grupos objetivo, cuando y como se les debe comunicar, y que material debe ser usado para cada grupo. Se lleva a cabo la identificación de los Objetivos de Comunicación, (que se le quiere decir y divulgar a la gente). ▪ Definir el procedimiento de Gestión y Monitoreo del proceso. ▪ Definición de los Indicadores del proceso. ▪ Definir Recursos Humanos con la definición de los roles y las responsabilidades asociadas al proceso.
E7.3	Desarrollar un plan de manejo del cambio.
E7.4.	Hacer entrega de: ▪ Proceso de Administración de la Cultura de Seguridad de la Información. ▪ Plan de Sensibilización. ▪ Plan de Promoción. ▪ Plan de Comunicación y divulgación.

E8 - Implementación del Proceso de Administración de la Cultura de Seguridad de la Información	
Para establecer y gestionar un Sistema de Gestión de la Seguridad de la Información en base a ISO 27001, se utiliza el ciclo continuo PHVA, tradicional en los sistemas de gestión de la calidad.	
Actividad	**Descripción**
E8.1	Ejecutar el plan de sensibilización definido en la etapa anterior en todas sus fases.
E8.2	Divulgar y comunicar las mejores prácticas de seguridad que apliquen a la entidad, así como las políticas de Seguridad definidas en el proyecto.
E8.3	Deberán realizarse charlas y talleres de sensibilización en seguridad de la información a todo nivel de la organización. Se debe definir en este punto cuales son las charlas a desarrollar, grupos objetivo y contenido de las mismas. Deben definirse mínimo una charla y un taller de dos (2) horas cada una, adicional a las actividades propias de la "*Semana de la Seguridad de la Información*".

E8.4	Para la ejecución de la promoción se deberá suministrar el diseño y desarrollo de los siguientes materiales: ▪ *Comunicados físicos y digitales*: Una cartilla pedagógica que deberá ser enviada físicamente a todos los empleados (300 unidades), se diseñarán treinta (30) comunicados digitales que se enviarán electrónicamente vía e-mail a todo el personal de la Imprenta Nacional de Colombia para la promoción de la Sensibilización (Información de la sensibilización, Invitaciones a participar de las actividades, compromisos, coordinación de actividades, etc.) y se diseñaran veinte (20) piezas gráficas que se publicaran en el sistema de carteleras electrónicas. ▪ *Afiches promociónales*: Se diseñarán veinte (20) afiches para la promoción de la sensibilización que deberán ser publicados en los sitios definidos para ello en el Ministerio, en las diferentes áreas de la entidad.
E8.5	Desarrollar un programa de Autoaprendizaje mediante un curso corto de autoaprendizaje en línea a través de plataforma Web, para realizar en ocho (8) horas. Este material será publicado en el servidor Web interno de la Imprenta Nacional de Colombia para que todos los empleados puedan acceder a este. La efectividad del impacto de este material debe ser evaluado por el contratista mediante una encuesta que deberá ser diligenciada por el personal de la Imprenta Nacional de Colombia en línea.
E8.6	Realización de la "*Semana de la Seguridad de la Información*": Esta Semana de la Seguridad arropa al *Día Internacional de la Seguridad de la Información*, que se celebra el *30 de noviembre* en todo el mundo y busca promover la realización de acciones de concientización en la materia, velando porque el mensaje llegue a la totalidad de funcionarios de la entidad: Divulgación del material promocional (comunicados digitales y afiches) y realización de cinco (5) charlas (una diaria) sobre el estado actual de la seguridad de la información en el ámbito mundial, latinoamericano y nacional.
E9 - Test de Intrusión (Externo e Interno)	
El test de intrusión proporciona mayor protección y fiabilidad a los sistemas de información de la entidad gracias a que permite evaluar el nivel de seguridad, prevenir a la entidad de los ataques externos e internos y fortalecer la seguridad de los Sistemas de Información, determinando el grado de acceso que tendría un atacante con intenciones maliciosas.	
Actividad	**Descripción**

E9.1	Recolectar toda la información necesaria para la realización del test de intrusión externo e interno a toda la plataforma de información y tecnología de la Imprenta Nacional de Colombia , lo cual incluye como mínimo: ▪ Elementos de Red. ▪ Servidores. ▪ Bases de Datos. ▪ Aplicaciones.
E9.2	Determinar los problemas y debilidades de seguridad en los elementos identificados en la etapa de "*Recolección de Información*". Estos problemas de seguridad se deben determinar usando no solo herramientas especializadas automáticas sino aplicando técnicas especializadas de "*hacking ético*".
E9.3	Las pruebas de vulnerabilidad mínimas a desarrollar sobre los elementos de información y tecnología son las siguientes: ▪ La Imprenta Nacional de Colombia. ✓ Debilidades de Autenticación. ✓ Cross Site script. ✓ Ataques Java. ✓ Ataques al Browser. ✓ Keylogger. ▪ Red. ✓ Comprobación de password y protocolos de ciframiento débiles. ✓ Enumeración de la red. ✓ Reconocimiento de la red. ✓ Sniffing. ✓ Ataques man-in-the-middle. ✓ Spoof de DNS. ✓ Reenrutamiento. ✓ Enumeración y Explotación de Wi-Fi. ✓ Enumeración y Explotación de BlueTooth. ▪ Gateway. ✓ IP-email-Spoof. ✓ Explotación de vulnerabilidades. ✓ Filtering bypass. ✓ Sniffing. ▪ Sistemas operativos.

	✓ Identificación del sistema operativo del objetivo. Instalaciones por defecto de servicios y aplicativos. ✓ Identificación de los puertos abiertos en los objetivos (TCP, UDP). ✓ Identificación de los servicios que se están ejecutando en los objetivos. ✓ Rompimiento de claves. ✓ Identificación de vulnerabilidades del SO. ✓ Negación de Servicios. ✓ Búsqueda de información sensible accesible por la red, como la existente en las carpetas compartidas. ✓ Sniffing. ▪ Servidores Web. ✓ Identificación del sistema operativo del objetivo. ✓ Vulnerabilidades asociadas a malas prácticas de programación. ✓ Identificación de los servicios que se están ejecutando en los objetivos. ✓ Explotación de vulnerabilidades. ✓ Búfer Overflow. ✓ Configuración por defecto. ✓ Negación de Servicios. ▪ Aplicaciones. ✓ Formas. ✓ Directory Transversal. ✓ Meta-caracteres. ✓ Session Hijacking. ✓ Códigos de error. ✓ Búfer Overflow. ✓ Rompimiento de claves. ▪ Base de datos. ✓ SQL Injection. ✓ Queries estructurados. ✓ Claves por defecto. ✓ Claves fáciles. ✓ Autenticación de base de datos. ✓ Extracción de información confidencial.
E9.4	Relacionar las herramientas que utilizará para la realización de esta actividad, el personal y la metodología a desarrollar.

E9.5	Basado en la información de vulnerabilidades detectadas, se deberá determinar los objetivos específicos que puedan proporcionar una mayor probabilidad de éxito durante el ataque o aumentar el grado de penetración para alcanzar cualquiera de las metas definidas.
E9.6	Adicionalmente, incluir una clasificación de riesgo desde el punto de vista técnico sobre cada elemento por cada vulnerabilidad encontrada.
E9.7	Generar un informe detallado con los resultados obtenidos durante todo el proceso de ejecución de las pruebas de la siguiente forma: ▪ Informe Ejecutivo. ✓ Descripción del trabajo realizado. ✓ Resumen de las actividades realizadas. ✓ Descripción del informe final entregado. ✓ Descripción de principales hallazgos. ✓ Conclusiones. ✓ Recomendaciones. ▪ Informe Técnico de seguridad: ✓ Descripción de las pruebas realizadas. ✓ Metodología utilizada. ✓ Elemento evaluado. ✓ Puertos y servicios habilitados. ✓ Listado de vulnerabilidades encontradas en los elementos de la plataforma tecnológica. ✓ Descripción de la vulnerabilidad. ✓ Nivel de criticidad (Alto, Medio, Bajo). ✓ Riesgo asociado o impacto. ✓ Recomendación. ✓ Procedimiento de corrección.
E10 - Definición de Arquitectura de Seguridad	
Presentar una propuesta de arquitectura de seguridad para mitigar los riesgos tecnológicos sobre la Información y definir las prioridades para la implementación de los controles de la arquitectura diseñada. La Arquitectura de Seguridad se define como el conjunto de controles de infraestructura de TI recomendados para brindar, un ambiente que minimice los riesgos asociados a la utilización de tecnologías de información y apoye las estrategias de negocio.	
Actividad	**Descripción**

E10.1	Con base en el análisis de riesgo, llevar a cabo un análisis, selección y diseño de la arquitectura de seguridad informática (como mínimo para redes, aplicaciones, servidores, bases de datos, controles de seguridad y administración).
E10.2	Definir las prioridades para la implementación de los controles de la arquitectura diseñada y definir esto a manera de proyectos de inversión que incluya: Objetivo, descripción, beneficios, costos, actividades, productos esperados, requisitos técnicos de la solución basados en estándares de la industria.
E10.3	Definición del esquema de Autenticación, Autorización y Auditoria: La infraestructura informática de la Imprenta Nacional de Colombia posee servidores de diferentes sistemas, los cuales interactúan entre sí a través de una infraestructura de red. Con el fin de minimizar los riesgos en cuanto a la identificación y autenticación de los usuarios en la utilización de recursos, es necesario implementar un esquema que permita establecer la certeza de la persona que usa el servicio está autorizado para hacerlo.
E10.4	Definición de los controles de seguridad perimetral: Es necesario asegurarse que las personas sólo accedan a aquellos sistemas y servicios a los cuales tengan autorización, por lo cual debe diseñarse un esquema de seguridad para la red que cumpla esto y al mismo tiempo que no afecte el desempeño de la misma. A su vez el esquema de seguridad perimetral permitirá mitigar muchos riesgos asociados a las conexiones con redes públicas como Internet, redes WAN internas o de proveedores de servicio.
E10.5	Definición de conectividad segura: Las conexiones con otras redes y las conexiones acceso remoto se han convertido en un requisito para el intercambio de información en las empresas. Se pretende implementar un esquema de conexión adecuado, de tal forma que no se viole la confidencialidad, integridad y disponibilidad de la información sobre las redes de datos de la Imprenta Nacional de Colombia.
E10.6	Definición de esquema de monitoreo: El monitoreo proactivo de la seguridad permite identificar ataques y remediar vulnerabilidades presentes en los sistemas antes de que estos ocurran. El tener un esquema de monitoreo efectivo es una ventaja para cualquier organización para mitigar los riesgos de seguridad de la información.
E10.7	Definición del esquema de administración centralizada de la seguridad.
E10.8	Hacer entrega de:

	▪ Diseño de la arquitectura que contiene todos los ítems descritos para la implementación de los mismos en la infraestructura de IT de la Imprenta nacional de Colombia. ▪ Diagramas del diseño del modelo de arquitectura. ▪ Definición de prioridades para la implementación de los controles de la arquitectura diseñada.
E11 - Transición de IPv4 a IPv6	
Diagnosticar, planear la transición y sensibilizar el protocolo IPv6 en la entidad, con el propósito de adoptar el nuevo esquema de funcionamiento de manera paralela con el actual protocolo IPv4 y cumplir de esta manera con los objetivos de innovación tecnológica que exige el país. Para entrar en el proceso de adopción de este nuevo protocolo, se realizará un inventario de los activos de información, una revisión la actual infraestructura de computación y de comunicaciones, se validaran todos los componentes de hardware y software de que se disponga, se revisarán los servicios que se prestan, los sistemas de información, los estándares y políticas para conocer el impacto de adopción de la nueva versión del protocolo IP, a fin de facilitar las labores de planeación e implementación de IPv4 a IPv6, garantizando que las operaciones continúen funcionando normalmente. El diagnóstico de la infraestructura tecnológica (Hardware y Software) será el apoyo que facilitará las acciones necesarias para la adopción del nuevo protocolo en las entidad hasta la fase final que contemple la implementación y el monitoreo del nuevo protocolo.	
Actividad	**Descripción**
E11.1	La fase de planeación representa una etapa crítica e importante del proceso de transición por cuanto comienza con el plan de diagnóstico de la infraestructura de TI de la Entidad. Las siguientes son las actividades a tener en cuenta en esta fase: ▪ Elaborar y validar el inventario de Activos de Información de servicios tecnológicos de la entidad y la interrelación entre ellos. Para esta actividad se requiere desarrollar y mantener el inventario de hardware y software, identificando claramente cuáles equipos soportan IPv6 (IPv6-ready o IPv6-web), cuales requieren actualizarse y cuáles no soportan el nuevo protocolo, dejando la respectiva documentación en constancia al momento de optar hacia IPv6. ▪ Analizar, diseñar y desarrollar el plan de diagnóstico del protocolo IPv4 a IPv6. ▪ Identificar la topología actual de la red, su funcionamiento dentro de la organización. ▪ Identificar los esquemas de seguridad de la red de comunicaciones y sistemas de información

	▪ Evaluar el grado de afinamiento del protocolo IPv6 a nivel de hardware y software con miras a preparar la nueva infraestructura de red. ▪ Generar el plan detallado del proceso de transición de esta fase hacia IPv6. ▪ Revisar las políticas de enrutamiento para IPv6 entre los segmentos de red internos, de tal manera que el tráfico IPv6 generado internamente este plenamente controlado a través de zonas desmilitarizadas desde el *firewall* respectivo de cada entidad. ▪ Planear la migración de los siguientes servicios tecnológicos: Servicio de Resolución de Nombres (DNS), Servicio de Asignación Dinámica de Direcciones IP (DHCP), Directorio Activo, Servicios WEB, Servidores de Monitoreo, Validación del Servicio de Correo Electrónico, Validación del Servicio de la Central Telefónica, Servicio de Backups, Servicio de Comunicaciones Unificadas e Integración entre Sistemas de Información; así mismo revisar los procedimientos de implementación de estos servicios y las aplicaciones identificadas en esta fase, con base en los estándares de la RFC3 de IPv6 (Request For Comments de IPv6) . ▪ Establecer el protocolo de pruebas para la validación de aplicativos, equipos de comunicaciones, plan de seguridad y coexistencia de los protocolos IPv4 e IPv6. ▪ Establecer los acuerdos de confidencialidad que sean necesarios sobre el tratamiento de la información ante terceros. ▪ Capacitar a funcionarios de las Áreas de TI de las Entidades de conformidad con los planes de capacitación establecidos, en el protocolo IPv6 y establecer la sensibilización a las personas de toda la organización a fin de dar a conocer el nivel de impacto del nuevo protocolo.
E11.2	Hacer entrega de: ▪ Plan de trabajo para la adopción de IPv6. ▪ Plan de diagnóstico que debe contener los siguientes componentes: Inventario de TI (Hardware y software), Informe de la Infraestructura de red de comunicaciones, recomendaciones para adquisición de elementos de comunicaciones, de cómputo y almacenamiento con el cumplimiento de IPv6, plan de direccionamiento en IPv6, plan de manejo de excepciones, definiendo las acciones necesarias en cada caso particular con aquellos elementos de hardware y software (aplicaciones y servicios) que sean incompatibles con IPv6, Informe de preparación (“*Readiness*”) de los sistemas de comunicaciones, bases de datos y aplicaciones. ▪ Documento que define los lineamientos al implementar la seguridad en IPv6 en concordancia con la política de seguridad de la entidad.

	▪ Plan de la migración de los siguientes servicios tecnológicos: Servicio de Resolución de Nombres (DNS), Servicio de Asignación Dinámica de Direcciones IP (DHCP), Directorio Activo, Servicios WEB, Servidores de Monitoreo, Validación del Servicio de Correo Electrónico, Validación del Servicio de la Central Telefónica, Servicio de Backups, Servicio de Comunicaciones Unificadas e Integración entre Sistemas de Información; así mismo revisar los procedimientos de implementación de estos servicios y las aplicaciones identificadas en esta fase, con base en los estándares de la RFC3 de IPv6 (Request For Comments de IPv6) . ▪ Protocolo de pruebas para la validación de aplicativos, equipos de comunicaciones, plan de seguridad y coexistencia de los protocolos IPv4 e IPv6. ▪ Plan de capacitación en IPv6 a los funcionarios de la Oficina de Sistemas e Informática de la entidad y plan de sensibilización al total de funcionarios de la entidad.
E12 – Diagnóstico del cumplimiento de la estrategia de Gobierno en Línea - GEL	
El diagnóstico del cumplimiento de la estrategia de Gobierno en Línea – GEL, tiene como propósito determinar el estado de avance de su implementación en la entidad para formular planes de acción que faciliten el logro de los objetivos de la estrategia en cada uno de sus componentes: TIC para servicios, TIC para el Gobierno Abierto, TIC para la Gestión y Seguridad y privacidad de la Información.	
Actividad	**Descripción**
E12.1	Definición del Plan de acción para las vigencias 2016 (último trimestre), 2017 y 2018, que contenga todas las iniciativas definidas por la entidad que buscan dar cumplimiento a la Estrategia de Gobierno en Línea conforme el Manual GEL 3.1, aplicable al momento, todo ello en pleno cumplimiento a las directrices definidas por el Ministerio de las Tecnologías de la Información y las Comunicaciones – MinTIC, y atendiendo a los lineamientos estipulados en el Plan Nacional de Desarrollo 2014 -2018 "*Todos Por un Nuevo País*" en torno al avance de la estrategia.
E12.2	Hacer entrega del Documento: ▪ *"Plan de acción del cumplimiento de la estrategia de Gobierno en Línea – GEL -para las vigencias 2016 (último trimestre), 2017 y 2018"*.
E13 – Implementación del Sistema de Gestión de Seguridad de la Información – SGSI – para los procesos misionales (Gestión Comercial, Gestión de Producción, Gestión Financiera y Gestión Informática)	

El establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora del SGSI documentado, en el contexto de los riesgos del negocio de la Imprenta Nacional de Colombia (actividades esenciales para la existencia de la entidad), tiene como propósito de asegurar controles de seguridad suficientes y proporcionales que protejan los activos de información y brinden confianza a las partes involucradas.

Actividad	Descripción
E13.1	Establecimiento y gestión del SGSI: Establecimiento, implementación y operación, seguimiento y revisión, mantenimiento y mejora, requisitos de documentación, responsabilidad de la Dirección, auditorías internas, revisión por la Dirección y mejora.
E13.2	Hacer entrega de los Documentos: ▪ "*Alcance del SGSI*": Ámbito de la entidad que queda sometido al SGSI, incluyendo una identificación clara de las dependencias, relaciones y limites que existen entre el alcance y aquellas partes que no hayan sido consideradas. ▪ "*Política y objetivos de seguridad*": Documento de contenido genérico que establece el compromiso de la dirección y el enfoque de la organización en la gestión de la seguridad de la información, alineada con el contexto organizacional estratégico de gestión del riesgo en el cual tendrá lugar el establecimiento y mantenimiento del SGSI, así como, la definición de la política por cada dominio de la norma ISO/IEC 27002:2013. ▪ "*Procedimientos y controles del SGSI*": Aquellos procedimientos que regulan el propio funcionamiento del SGSI. ▪ "*Declaración de aplicabilidad (SOA -Statement of Applicability)*": Documento que contiene los objetivos de control y los controles contemplados por el SGSI, basado en los resultados de los procesos de evaluación y tratamiento de riesgos, justificando inclusiones y exclusiones. ▪ "*Metodología de evaluación de riesgos*": Descripción de la forma como se realizará la evaluación de las amenazas, vulnerabilidades, probabilidades de ocurrencia e impactos en relación a los activos de información de la entidad dentro del alcance definido, y los criterios de aceptación de riesgo. "*Informe de evaluación y plan de tratamiento de riesgos*": Estudio resultante de aplicar la metodología de evaluación anteriormente mencionada a los activos de información de la entidad dentro del alcance definido y el Plan de tratamiento de los riesgos, en concordancia con el ítem "*E3 - Gestión de Riesgos (Análisis y Evaluación de Riesgos)*"**.**

	▪ "*Procedimientos del SGSI*": Todos los necesarios para asegurar la eficacia de la planificación, operación y control de los procesos de seguridad de la información, así como para la medida de la eficacia de los controles implantados (gestión de incidentes de seguridad de la información, seguimiento y revisión, auditorías internas del SGSI, revisión por la dirección, control de documentos y control de registros, mejora continua, entre otros). ▪ "*Registros*": Todos los que evidencien de manera objetiva la conformidad con los requisitos y la operación eficaz del SGSI y los controles necesarios para Ia identificación, almacenamiento, protección, recuperación, tiempo de retención y disposición de los registros.

2. RESULTADOS O PRODUCTOS ESPERADOS

A continuación se encuentra la descripción detallada de los servicios requeridos y de los resultados o productos esperados, según el objeto del proyecto:

No	Resultado o Producto esperado
1	**PLAN DE TRABAJO (Primer pago)** ▪ Elaboración, presentación para revisión y aprobación por parte de la Imprenta Nacional de Colombia de los siguientes documentos: ✓ "*Metodología de Trabajo*" que se pretende aplicar para el desarrollo del proyecto. ✓ "*Plan de Gerencia del Proyecto*" (que incluya la estrategia y plan de participación interinstitucional y el Plan de comunicaciones). ✓ "*Conformación de equipo de trabajo*" (Organigrama, número de funcionarios, rol que cada uno de ellos desempeñara durante la ejecución del contrato y dedicación que cada uno va a tener con el proyecto, así como, Hojas de Vida y Tarjetas Profesionales del equipo de trabajo junto con los documentos que certifiquen la experiencia requerida). ✓ "*Cronograma general de actividades*". ✓ "*Esquema de aseguramiento de calidad*". ✓ "*Procedimiento sugerido de control de cambios*". El contratista deberá presentar los anteriores documentos dentro de los cinco (5) días hábiles siguientes a la firma del Acta de Inicio del contrato y serán revisados y aprobados por el Supervisor del contrato por parte de la Imprenta nacional de Colombia. ▪ Realizar una reunión de inicio de proyecto en la que se realice una presentación general del proyecto y que cuente con la presencia del equipo de trabajo.

No	Resultado o Producto esperado
2	**E1 - Análisis GAP (Diagnóstico ISO 27001 e ISO 27002)** ▪ Documento "***Análisis GAP (ISO 27001:2013 e ISO 27002:2013)***" que incluya, entre otros: Informe de resultados de evaluación y diagnóstico por cada dominio de la norma ISO/IEC 27002:2013 e informe de resultados de evaluación y diagnóstico de revisión documental del modelo actual de seguridad de la información (documentación de nivel 1, nivel 2, nivel 3 y nivel 4). **E2 – Gestión de Activos de Información (levantamiento, inventario y clasificación de activos de información e índice de información clasificada y reservada)** ▪ Documento "*Gestión de activos de información*" que incluya, entre otros: Informe de resultados del levantamiento de información, instructivo para el proceso de inventario de activos de información, inventario de activos de información, instructivo de clasificación de activos de información y su nivel de clasificación y confidencialidad, activos de información clasificados según inventario e instructivo de clasificación, caracterización de Usuarios, índice de información Clasificada y Reservada y recomendaciones para la revisión, gestión y actualización de la clasificación de la información. **E3 - Gestión de Riesgos (Análisis y Evaluación de Riesgos) (Segundo pago)** ▪ Documento "*Gestión de Riesgos de seguridad de la información*" que incluya, entre otros: Informe completo del análisis de amenazas, informe completo del análisis de vulnerabilidades, informe de los resultados del análisis de impacto, matriz de niveles de riesgo e informe de identificación de controles necesarios para mitigar o transferir el riesgo y arquitectura de seguridad sugerida, diseño de requerimientos de equipos necesarios para la implementación de la arquitectura de seguridad y análisis de impacto.
3	**E4 - Definición de Políticas de Seguridad de la Información** ▪ Documento "*Políticas, normas y procedimientos de seguridad de la información*" que incluya: Políticas, normas y procedimientos para los dominios contemplados en las normas ISO/IEC 27001:2013 e ISO 27002:2013 y el "*Proceso de mantenimiento, revisión, actualización y aprobación de políticas de seguridad de la información*". **E5 - Gestión de Incidentes** ▪ Documento "*Proceso de gestión de incidentes*" que incluya, entre otros: Análisis de capacidades de detección, contención y recuperación frente a incidentes, Clasificación de incidentes (tipos y niveles de servicio asociados), procedimientos de declaración y mecanismos de notificación de incidentes, procedimiento de Atención y Escalamiento de incidentes, procedimientos de informática forense (recopilación, manejo, almacenamiento, procesamiento y protección de la evidencia digital), contingencia y

No	Resultado o Producto esperado
	recuperación frente a incidentes, plan de pruebas y simulacros y Manuales de soporte procedimental para respuesta a incidentes. **E6 - Plan de Continuidad de Información y Tecnología** ▪ Documento "*Plan de Continuidad de Información y Tecnología*" que incluya, entre otros: Metodología, Plan de acciones e inversiones que ayuden a mejorar la continuidad de los procesos más críticos, Plan de requerimientos funcionales, resultados del diseño del plan, Plan de implementación, análisis de impacto del negocio y funciones del negocio sensibles al tiempo, programa de administración del plan de continuidad (mantenimiento y actualización), procedimientos de respuesta a emergencias, procedimientos detallados de reanudación, recuperación y restauración, tiempos mínimos de recuperación, tiempos máximos de tolerancia aceptados por los procesos, y estimación de recursos mínimos de operación y tiempos de entrega del servicio requeridos. **E7 - Definición del Proceso de Administración de la Cultura de Seguridad de la Información** ▪ Documento "*Proceso de Administración de la Cultura de Seguridad de la Información*" que incluya, entre otros: Identificación de situación actual a nivel de cultura en seguridad informática, Identificación de planes de capacitación en seguridad de la información , estrategia de implementación del proceso, Plan de Sensibilización, plan de Entrevistas, plan de Promoción y plan de comunicación y divulgación, procedimiento de Gestión y Monitoreo el proceso, indicadores del proceso y plan de manejo del cambio. **E8 - Implementación del Proceso de Administración de la Cultura de Seguridad de la Información (Tercer pago)** ▪ Documento "*Plan de Implementación del Proceso de Administración de la cultura de seguridad de la información*" que incluya, entre otros: Ejecución del Plan de Talleres de sensibilización, Diseño y desarrollo de Comunicados físicos y digitales, una cartilla pedagógica para la promoción de la sensibilización, afiches promociónales y un programa de Autoaprendizaje mediante un curso corto de autoaprendizaje en línea a través de plataforma Web, así como, la realización de la "*Semana de la Seguridad de la Información*".
4	**E9 - Test de Intrusión (Externo e Interno)** ▪ Documento "*Test de intrusión (Nivel de seguridad de los sistemas de información)*" que incluya, entre otros: Metodología, Informe de evaluación y diagnóstico en donde se indican los resultados por cada dominio de la norma ISO/IEC 27002:2013 y para cada objetivo de control (representados en gráficos y tablas de datos), observaciones

No	Resultado o Producto esperado
	(evidencias, hallazgos, comentarios), pruebas de vulnerabilidad mínimas a desarrollar (Red, Gateway, Sistemas operativos, Servidores Web, Aplicaciones, Bases de Datos), recomendaciones (oportunidades de mejora). ▪ Documento "*Diagnóstico documental del modelo de seguridad de la información*", que incluya, entre otros: Nivel de cumplimiento de la documentación con respecto a la norma, observaciones (evidencias, hallazgos, comentarios) y recomendaciones (oportunidades de mejora). **E10 - Definición de Arquitectura de Seguridad** ▪ Documento "*Arquitectura de seguridad de la información*" que incluya, entre otros: Diagramas del diseño del modelo de arquitectura (redes, aplicaciones, servidores, bases de datos, controles de seguridad y administración), definición de prioridades para la implementación de los controles de la arquitectura diseñada, definición del esquema de Autenticación, Autorización y Auditoria, definición de controles de seguridad perimetral, definición de conectividad segura, definición del esquema de monitoreo y definición del esquema de administración centralizada de la seguridad. **E11 - Transición de IPv4 a IPv6** ▪ Documento "*Diagnóstico para la adopción de IPv6*" que incluya, entre otros: Inventario de TI (Hardware y software), Informe de la Infraestructura de red de comunicaciones, recomendaciones para adquisición de elementos de comunicaciones, de cómputo y almacenamiento con el cumplimiento de IPv6, plan de direccionamiento en IPv6, plan de manejo de excepciones, definiendo las acciones necesarias en cada caso particular con aquellos elementos de hardware y software (aplicaciones y servicios) que sean incompatibles con IPv6, Informe de preparación ("*Readiness*") de los sistemas de comunicaciones, bases de datos y aplicaciones y lineamientos al implementar la seguridad en IPv6. ▪ Documento "*Plan de migración de servicios tecnológicos para la adopción de IPv6*" que incluya, entre otros los siguientes servicios tecnológicos: Servicio de Resolución de Nombres (DNS), Servicio de Asignación Dinámica de Direcciones IP (DHCP), Directorio Activo, Servicios WEB, Servidores de Monitoreo, Validación del Servicio de Correo Electrónico, Validación del Servicio de la Central Telefónica, Servicio de Backups, Servicio de Comunicaciones Unificadas e Integración entre Sistemas de Información; así mismo revisar los procedimientos de implementación de estos servicios y las aplicaciones identificadas en esta fase, con base en los estándares de la RFC3 de IPv6 (Request For Comments de IPv6) . También debe incluir el protocolo de pruebas para la validación de aplicativos, equipos de comunicaciones, plan de seguridad y coexistencia de los protocolos IPv4 e IPv6.

No	Resultado o Producto esperado
	▪ Documento "*Plan de capacitación en IPv6*". **E12 – Diagnóstico del cumplimiento de la estrategia de Gobierno en Línea – GEL (Cuarto pago)** ▪ Documento "*Plan de acción del cumplimiento de la estrategia de Gobierno en Línea – GEL -para las vigencias 2016 (último trimestre), 2017 y 2018*". **E13 – Implementación del Sistema de Gestión de Seguridad de la Información – SGSI – para los procesos misionales (Gestión Comercial, Gestión de Producción, Gestión Financiera y Gestión Informática)** ▪ Documento "*Alcance del SGSI*": Ámbito de la entidad que queda sometido al SGSI, incluyendo una identificación clara de las dependencias, relaciones y límites que existen entre el alcance y aquellas partes que no hayan sido consideradas. ▪ Documento "*Política y objetivos de seguridad*": Documento de contenido genérico que establece el compromiso de la dirección y el enfoque de la organización en la gestión de la seguridad de la información, alineada con el contexto organizacional estratégico de gestión del riesgo en el cual tendrá lugar el establecimiento y mantenimiento del SGSI . ▪ Documento "*Procedimientos y controles del SGSI*": Aquellos procedimientos que regulan el propio funcionamiento del SGSI. ▪ Documento "*Declaración de aplicabilidad (SOA -Statement of Applicability)*": Documento que contiene los objetivos de control y los controles contemplados por el SGSI, basado en los resultados de los procesos de evaluación y tratamiento de riesgos, justificando inclusiones y exclusiones. ▪ Documento "*Metodología de evaluación de riesgos*": Descripción de la forma como se realizará la evaluación de las amenazas, vulnerabilidades, probabilidades de ocurrencia e impactos en relación a los activos de información de la entidad dentro del alcance definido, y los criterios de aceptación de riesgo. ▪ Documento "*Informe de evaluación y plan de tratamiento de riesgos*": Estudio resultante de aplicar la metodología de evaluación anteriormente mencionada a los activos de información de la entidad dentro del alcance definido y el Plan de tratamiento de los riesgos, en concordancia con el ítem "*E3 - Gestión de Riesgos (Análisis y Evaluación de Riesgos)*"**.** ▪ Documento "*Procedimientos del SGSI*": Todos los necesarios para asegurar la eficacia de la planificación, operación y control de los procesos de seguridad de la información, así como para la medida de la eficacia de los controles implantados (gestión de incidentes de seguridad de la información, seguimiento y revisión, auditorías internas del SGSI, revisión por la dirección, control de documentos y control de registros, mejora continua, entre otros).

No	Resultado o Producto esperado
	▪ Documento "*Registros del SGSI*": Todos los que evidencien de manera objetiva la conformidad con los requisitos y la operación eficaz del SGSI y los controles necesarios para Ia identificación, almacenamiento, protección, recuperación, tiempo de retención y disposición de los registros.
5	**Garantía** El contratista debe dar una garantía de mínimo doce (12) meses, la cual consiste en: ▪ Seguimiento a los planes de tratamiento de riesgos, a través de un banco de horas de soporte especializado en sitio de doscientas (200) horas, con tiempo de respuesta para dar solución a inquietudes e inconvenientes con la implementación del SGSI, así: Requerimientos urgentes o con prioridad alta (entre 2-4 horas), requerimientos con prioridad media (entre 12-24 horas), Requerimientos con prioridad baja (entre 24-36 horas). Además se debe contar con una línea telefónica de atención para solicitudes y un correo electrónico. Los tiempos de traslado no se consideran parte de las horas de soporte. ▪ Ejecución de mínimo un (1) test de intrusión adicional (no hace parte de las horas de soporte técnico que conforman el banco de horas de soporte especializado en sitio).
6	Entregar a la Imprenta Nacional de Colombia, el "*PLAN DE TRANSFERENCIA DE CONOCIMIENTO*" que incluya: ▪ Sensibilización en seguridad de la información (4 horas, total de funcionarios de la entidad). ▪ Implementación y auditoría de un Sistema de Gestión de Seguridad de la Información (40 horas, 12 funcionarios). ▪ Buenas prácticas de seguridad de la información (16 horas, 6 funcionarios). ▪ Ethical Hacking (24 horas, 6 funcionarios).
7	Por cada uno de los talleres de transferencia de conocimiento, el "*REGISTRO DOCUMENTAL DE LOS TEMAS TRATADOS*", "*MATERIAL UTILIZADO*", "*CERTIFICADOS DE ASISTENCIA*", "*EVALUACION*" y el "*INFORME DE RESULTADOS DEL PLAN DE TRANSFERENCIA DE CONOCIMIENTO*" que incluya las "*ACTAS DE TRANSFERENCIA DE CONOCIMIENTO*".

3. EXPERIENCIA DEL PROPONENTE

3.1. EXPERIENCIA ESPECÍFICA

Se ha considerado como requisito mínimo de verificación, **cumple o no cumple**, que los proponentes acrediten con las certificaciones respectivas, expedidas por los contratantes, la celebración, ejecución y terminación de al menos dos (2) contratos suscritos con entidades públicas, dentro de los tres (3) años anteriores a la fecha de cierre de esta invitación, donde la sumatoria de las dos (2) certificaciones sea igual o superior al cien por ciento (100%) del presupuesto asignado a la presente contratación, es decir, equivalente a un monto mínimo de $ 468.000.000,00, incluido IVA y cuyo objeto o alcance del mismo sean actividades desarrolladas en el marco del objeto de la presente invitación, lo cual debe expresarse claramente en el texto de la certificación o evidenciarse mediante documentos relacionados con la ejecución del contrato, tales como, actas de entrega, actas de recibo a satisfacción, actas de liquidación o informes finales de actividades, o el contrato mismo. (Formato N° 5).

Las certificaciones de experiencia deberán reunir los siguientes requisitos:

a. Fecha de expedición.
b. Nombre legible de la persona y de la empresa que la expide.
c. Nombre o razón social del contratista.
d. Objeto del contrato.
e. Plazo del contrato.
f. Valor del contrato (en pesos colombianos, para contratos celebrados en el territorio colombiano), incluido IVA y demás costos directos e indirectos relacionados con el servicio.
g. En caso que la certificación sea expedida a una propuesta conjunta, en la misma debe identificarse el porcentaje de participación de cada uno de sus integrantes.
h. Si la certificación incluye varios contratos, se debe identificar en forma precisa si son contratos adicionales al principal o son contratos nuevos, indicando en cada uno de ellos sus plazos, y/o valor.
i. Concepto del servicio prestado. La calificación del bien suministrado debe ser excelente, buena, satisfactoria o expresiones positivas similares

Nota 1. Si la certificación no contiene estos datos, la entidad podrá solicitar al proponente que adjunte fotocopia legible del contrato firmado por ambas partes y con fecha de firma legible, para verificación de la información, acompañado con su respectiva acta de recibo final o el acta de liquidación, donde se pueda obtener toda la información requerida.

Nota 2. Cuando se trate de experiencia adquirida como integrante de consorcios o uniones temporales se deberá especificar el porcentaje de participación en cada certificación allegada. La Imprenta Nacional de Colombia tomará para la evaluación y calificación correspondiente, el porcentaje (%) de participación en la ejecución del contrato del integrante del Consorcio o de la Unión Temporal, porcentaje que debe estar discriminado en la certificación, si no es así el proponente debe presentar el documento que acreditó la conformación del Consorcio o de la Unión Temporal, donde conste el porcentaje de participación de cada uno de los integrantes para la ejecución del contrato.

Nota 3. Si el objeto de la certificación incluye bienes o servicios diferentes a los que se requieren, se deberá anexar la información necesaria (acta de recibo final, el acta de liquidación, etc.) para determinar el valor correspondiente del bien o servicio para el cual se presenta.

Nota 4. El proponente deberá especificar claramente cuáles de las certificaciones aportadas corresponden a certificaciones adicionales.

Nota 5: Se podrán subsanar aspectos de las certificaciones de experiencia, mediante una certificación debidamente suscrita por la persona facultada para expedirla al interior de la empresa en la que se ejecutó el contrato.

Nota 6. No se tendrán en cuenta las certificaciones que acrediten contratos que se encuentran actualmente en ejecución, los que no se relacionen con el objeto del proceso de la presente invitación, ni las relaciones de contratos, ni copia de los contratos por sí solos, ni copia de facturas, ni actas de recibo, de liquidación o aquellas certificaciones cuyo cumplimiento está por debajo de bueno.

Nota 7. La Imprenta Nacional de Colombia se reserva el derecho de verificar la información suministrada por los oferentes. Si se advierten discrepancias entre la información suministrada y lo establecido por la Entidad, la propuesta será rechazada.

Nota 8. No es necesario presentar las certificaciones de aquellos contratos ejecutados dentro de los tres años anteriores a la fecha de cierre de esta invitación, que haya suscrito con la Imprenta Nacional de Colombia; pero es obligatorio relacionar el (los) número (s) de el (los) contrato(s), o si hay contrato vigente para verificar internamente el cumplimiento de los mismos. Si no se relacionan en la propuesta, no podrán solicitar que sean tenidos en cuenta con posterioridad.

Nota 9. En caso de requerirse aclaraciones sobre los datos contenidos en las certificaciones, la Imprenta Nacional de Colombia podrá solicitar al proponente tales aclaraciones, quien contará con un (1) día hábil para suministrarlas, de no hacerlo o no presentar las aclaraciones solicitadas la propuesta será rechazada. Se podrán subsanar aspectos de las certificaciones de experiencia,

mediante una certificación debidamente suscrita por la persona facultada para expedirla al interior de la empresa en la que se ejecutó el contrato.

Nota 10. En caso de relacionarse más de dos (2) certificaciones de contratos, la Imprenta Nacional de Colombia, para salvaguardia de los principios de transparencia, lealtad e igualdad, evaluará sólo las dos (2) correspondientes a los mayores valores contratados.

4. PLAN DE TRABAJO

La propuesta debe contemplar la Elaboración y entrega del Plan de Trabajo: Metodología que se pretende aplicar para el desarrollo del proyecto, Plan de Gerencia del Proyecto (estrategia y plan de participación interinstitucional y el Plan de Comunicaciones), conformación del equipo de trabajo (Organigrama, número de funcionarios, rol y dedicación que cada uno va a tener con el proyecto), cronograma detallado de actividades (actividades, entregables, responsable, fecha de inicio y fecha de terminación), Esquema de aseguramiento de la calidad y procedimiento sugerido de control de cambios.

El cronograma detallado de la ejecución de todo el proyecto de implementación del SGSI servirá como línea base para el seguimiento a la ejecución, será revisado en conjunto con la Imprenta Nacional de Colombia y a fin de establecer los recursos y dedicaciones requeridos por parte de la Imprenta nacional de Colombia en la realización de las diferentes actividades y deberá contemplar actividades propias de la implementación, las relacionadas con la elaboración y aprobación de documentos y la transferencia de conocimiento e incorporar como hitos los entregables, la planeación, preparación y ejecución de pruebas, así como los diferentes hitos del proyecto de implementación dentro de los cuales deben estar las entregas y aceptaciones de los diferentes entregables.

5. SERVICIOS DE TRANSFERENCIA DE CONOCIMIENTO

5.1. OBJETIVO

El objetivo de los talleres de transferencia de conocimiento es asegurar la transmisión del conocimiento tecnológico generado en el proyecto hacia la entidad, con vías a su post-implantación (gestión).

Los talleres de transferencia de conocimiento estarán dirigidos hacia el grupo funcionarios seleccionados por la Imprenta Nacional de Colombia (internos y/o externos).

5.2. ALCANCE

La transferencia de conocimiento debe ser impartida a través de talleres teórico-prácticos (reuniones especializadas que tienen naturaleza técnica y académica cuyo objetivo es realizar un estudio profundo de determinados temas con un tratamiento que requiere una interactividad entre los especialistas), en concordancia con los requerimientos establecidos como "*Resultado o Producto esperado*" y según el "*Plan de Transferencia de Conocimiento*".

Los talleres de transferencia de conocimiento cubrirán, entre otros, los siguientes temas: Implementación y auditoría de un Sistema de Gestión de Seguridad de la Información (SGSI), Buenas prácticas de seguridad de la información, Ethical Hacking y Sensibilización en seguridad de la información.

Para efectos de la ejecución de las actividades asociadas a la transferencia de conocimiento, se debe tener en cuenta, entre otros, los siguientes aspectos:

- La transferencia de conocimiento debe ser impartida por el contratista, en las instalaciones de la Imprenta Nacional de Colombia.
- Los talleres de transferencia de conocimiento previstos serán presenciales y en idioma español. La conceptualización y diseño de los materiales requeridos son responsabilidad del contratista.
- Son responsabilidad del contratista el suministro de los materiales requeridos para el desarrollo de los talleres de transferencia de conocimiento, la instalación, puesta a punto y operación de la infraestructura tecnológica (hardware, software base, software de aplicación) requeridos para ejecutar los talleres.
- El contratista deberá presentar dentro los cinco (5) días hábiles siguientes a la firma del Acta de Inicio, un "*Plan de Transferencia de Conocimiento*" que incluya cada una de los temas que forman parte del alcance y el cronograma propuesto, el cual será revisado y aprobado por el Supervisor del contrato por parte de la Imprenta Nacional de Colombia.
- El contratista deberá presentar dentro de los cinco (5) días hábiles siguientes a la finalización de la ejecución del "*Plan de Transferencia de Conocimiento*", un "*Informe de Resultados del Plan de Transferencia de Conocimiento*" que incluya las "*Actas de Transferencia de Conocimiento*" debidamente aprobadas por parte del Supervisor del contrato, el material utilizado y entregado a los participantes y los Certificados de asistencia.
- El instructor del curso "*Implementación y auditoría de un Sistema de Gestión de Seguridad de la Información (SGSI)*" debe ser certificado como auditor líder en la norma BS 7799-2 o ISO 27001.

5.3. TEMARIO

Temario	Duración (h)	Funcionarios
Sensibilización en seguridad de la información	4	Total de funcionarios (Aprox. 300)
Implementación y auditoría de un Sistema de Gestión de Seguridad de la Información	40	12
Buenas prácticas de seguridad de la información	16	6
Ethical Hacking	24	6

5.4. CRITERIO DE ACEPTACIÓN DE LA TRANSFERENCIA DE CONOCIMIENTO

De cada taller de transferencia de conocimiento, el contratista deberá dejar registro documental de los temas tratados (material utilizado para el desarrollo del taller), de los asistentes (quienes se registrarán con nombre, documento de identidad, entidad a la que pertenecen y rol en el proyecto), de la evaluación diligenciada por cada uno(a) de ellos respecto al taller de transferencia de conocimiento y de los Certificados de Asistencia.

Un taller de transferencia de conocimiento se dará por aceptado cuando el mismo se haya realizado para la totalidad de funcionarios designados por la Imprenta Nacional de Colombia en concordancia con los requisitos establecidos en el numeral "*TEMARIO DE LA TRANSFERENCIA DE CONOCIMIENTO*", el contratista haga entrega de la totalidad de requisitos descritos en el párrafo anterior y se apruebe la respectiva "*ACTA DE TRANSFERENCIA DE CONOCIMIENTO*" por el supervisor del contrato por parte de la Imprenta Nacional de Colombia.

6. GARANTIA

El contratista debe dar una garantía de mínimo doce (12) meses, la cual consiste en:

- Seguimiento a los planes de tratamiento de riesgos, a través de un banco de horas de soporte especializado en sitio de trecientas (300) horas, con tiempo de respuesta para dar solución a inquietudes e inconvenientes con la implementación del SGSI, así: Requerimientos urgentes o con prioridad alta (entre 2-4 horas), requerimientos con prioridad media (entre 12-24 horas), Requerimientos con prioridad baja (entre 24-36 horas). Además se debe contar con una línea telefónica de atención para solicitudes y un correo electrónico.

- Ejecución de mínimo un (1) test de intrusión adicional, con personal especializado, debidamente acreditado, entregando a la Imprenta Nacional de Colombia (Oficina de Sistemas e Informática - OSI) el respectivo informe técnico, donde se plasme entre otros: Metodología, Informe de evaluación y diagnóstico en donde se indican los resultados por cada dominio de la norma ISO/IEC 27002:2013 y para cada objetivo de control (representados en gráficos y tablas de datos), observaciones (evidencias, hallazgos, comentarios), pruebas de vulnerabilidad mínimas a desarrollar (Red, Gateway, Sistemas operativos, Servidores Web, Aplicaciones, Bases de Datos), recomendaciones (oportunidades de mejora).

Se debe incluir el costo del Seguimiento a los planes de tratamiento de riesgos y el test de intrusión adicional, con el personal, herramientas y equipos requeridos, como parte de la propuesta.

7. EQUIPO DE TRABAJO

A continuación se presenta el equipo mínimo de trabajo que debe asignarse para la ejecución del proyecto. Sin embargo, el OFERENTE podrá, a su costo, utilizar los servicios de recursos adicionales si lo considera necesario para el cumplimiento oportuno de sus obligaciones:

Rol	No. de Personas	Experiencia Mínima.
GERENTE DE PROYECTO Profesional Universitario en Ingeniería o Administración de Empresas.	1	▪ Acreditar experiencia general acumulada en el ejercicio de la profesión igual o superior a cinco (5) años contados a partir de la fecha de terminación de materias. ▪ Acreditar certificación PMP (Project Management Professional), vigente. ▪ Haber participado en la implementación de dos (2) proyectos relacionados con el objeto de la presente invitación, en los últimos tres (3) años. ▪ Acreditar al menos una (1) de las siguientes certificaciones: CISSP (Certified Information Systems Security Professional) – ISC2 o CISM (Certified Information Security Manager) - ISACA.
AUDITOR LIDER Profesional Universitario en Ingeniería (Sistemas,	1	▪ Acreditar experiencia general acumulada en el ejercicio de la profesión igual o superior a cinco

Rol	No. de Personas	Experiencia Mínima.
industrial, o electrónico) especializado en Sistemas de Gestión de Seguridad de la Información.		(5) años contados a partir de la fecha de terminación de materias. ▪ Especialización o maestría en Seguridad de la Información. ▪ Haber participado en la implementación de dos (2) proyectos relacionados con el objeto de la presente invitación, en los últimos tres (3) años. ▪ Acreditar certificación Auditor Interno ISO 27001. ▪ Acreditar al menos dos (2) de las siguientes certificaciones: CISSP (Certified Information Systems Security Professional) - ISC2, CISA (Certified Information Systems Auditor)- ISACA, CISM (Certified Information Security Manager) – ISACA o Auditor Interno ISO 27001.
INGENIERO SENIOR Profesional Universitario en Ingeniería (Sistemas, industrial, o electrónico) y con especialización en seguridad informática.	3	▪ Acreditar experiencia general acumulada en el ejercicio de la profesión igual o superior a tres (3) años contados a partir de la fecha de terminación de materias. ▪ Especialización o maestría en Seguridad de la Información. ▪ Haber participado en la implementación de dos (2) proyectos relacionados con el objeto de la presente invitación, en los últimos tres (3) años. ▪ Acreditar al menos dos (2) de las siguientes certificaciones: CISSP (Certified Information Systems Security Professional) - ISC2, CISA (Certified Information Systems Auditor)- ISACA o CISM (Certified Information Security Manager) – ISACA. ▪ Uno (1) de los tres (3) debe acreditar la certificación CEH (Certified Ethical Hacker).

Rol	No. de Personas	Experiencia Mínima.
		▪ Uno (1) de los tres (3) debe acreditar la certificación BCLS 2000 (Administración Continuidad de Negocio) – DRI.
INGENIERO JUNIOR Profesional Universitario en Ingeniería (Sistemas, industrial, o electrónico)	3	▪ Acreditar experiencia general acumulada en el ejercicio de la profesión igual o superior a tres (3) años contados a partir de la fecha de terminación de materias. ▪ Haber participado en la implementación de dos (2) proyectos relacionados con el objeto de la presente invitación, en los últimos tres (3) años. ▪ Acreditar al menos una (1) de las siguientes certificaciones: CompTIA Security+ o Auditor Interno ISO 27001.
LIDER DE CALIDAD Profesional Universitario en Ingeniería (Sistemas, industrial, o electrónico) o Administrador de Empresas o Economista, con especialización en Gestión de la Calidad	1	▪ Acreditar experiencia general acumulada en el ejercicio de la profesión igual o superior a cinco (5) años contados a partir de la fecha de terminación de materias. ▪ Acreditar especialización o maestría o posgrado en Gerencia de la Calidad o Gestión de la Calidad. ▪ Haber participado en la implementación de dos (2) proyectos relacionados con el objeto de la presente invitación, en los últimos tres (3) años. ▪ Acreditar certificación Auditor Líder ISO 9001.
Los demás profesionales que el OFERENTE estime convenientes para el desarrollo y ejecución del proyecto.		

Nota 1. Las certificaciones a través de las cuales se acredite tanto la experiencia general, como la específica del equipo de trabajo, deben ser expedidas por la(s) Empresa(s) para la(s) cual(es) se realizaron los trabajos y deberán contener, como mínimo: Nombre o razón social del contratante, nombre del contratista, objeto del contrato, fecha de iniciación y terminación del contrato y venir debidamente suscritas por la persona facultada para expedir dicho documento.

Nota 2. Tanto la experiencia general como la específica se contarán a partir de la fecha de terminación de materias, por lo cual deberá allegarse fotocopias de los títulos y actas de grado, las certificaciones respectivas, o los documentos idóneos que así lo acrediten.

Nota 3. No se aceptarán los traslapes de tiempo con certificaciones que especifiquen una dedicación de tiempo completo.

Nota 4. Para efectos de determinar los requerimientos mínimos de experiencia general y específica acumulada, la Imprenta Nacional de Colombia realizará la sumatoria de los tiempos de ejecución relacionados exclusivamente en cada una de las certificaciones válidas.

Nota 5. Solamente serán admitidas las certificaciones de cumplimiento expedidas por entidades públicas o privadas. No se tendrán en cuenta copias de minutas de contratos, excepto que estén acompañadas del acta de liquidación, o actas de recibo final, o de un documento en el que certifique el cumplimiento a satisfacción.

Nota 6. Dentro de la experiencia específica no se aceptarán certificaciones por docencia.

Nota 7. Salvo que la Imprenta Nacional de Colombia acuerde lo contrario, no se efectuarán cambios en la composición del equipo de trabajo. Si fuere necesario sustituir a algún integrante del equipo de trabajo, por cualquier motivo que escape al razonable control del contratista, éste lo reemplazará de inmediato por otra persona con calificaciones iguales o superiores a las de la persona reemplazada.

Nota 8. Si la Imprenta Nacional de Colombia, i) tiene conocimiento de que un integrante del equipo de trabajo se ha comportado de manera inaceptable o ha sido acusado de cometer una acción penal, o ii) tiene motivos razonables para estar insatisfecho con el desempeño de cualquier integrante del equipo de trabajo, en tales casos el contratista, a petición por escrito de la Imprenta nacional de Colombia expresando los motivos para ello, lo reemplazará por otra persona cuya idoneidad y experiencia sean aceptables para la Imprenta Nacional de Colombia.

Nota 9. El contratista no podrá reclamar el reembolso de ningún gasto adicional resultante de la remoción y/o sustitución de algún integrante del equipo de trabajo, o inherente a ésta.

Nota 10. La Imprenta Nacional de Colombia se reserva el derecho de verificar la información suministrada por el proponente y de solicitar las aclaraciones que considere convenientes.

Nota 11: Se podrán subsanar aspectos de las certificaciones de experiencia, mediante una certificación debidamente suscrita por la persona facultada para expedirla al interior de la empresa para la cual se realizaron los trabajos.

Nota 12. La Imprenta Nacional de Colombia, para salvaguardia de los principios de transparencia, lealtad e igualdad, evaluará sólo las certificaciones que cumplan con el requisito de experiencia mínima.

7.1. CERTIFICACIONES EN SEGURIDAD DE LA INFORMACIÓN

El auge por la demostración de conocimientos ya sea técnicos o teóricos sobre temas usualmente relacionados con tecnología va en aumento, es por ello que las certificaciones son una medida muy útil y valorada en procesos de contratación bajo la modalidad Concurso de Méritos.

En el ámbito de la seguridad de la información existen múltiples certificaciones con validez nacional e internacional, algunas de ellas asociadas directamente a tecnologías de fabricantes, otras más genéricas o especializadas en normativas o estándares.

Las certificaciones en seguridad de la información demuestran prueba de conocimientos y pericia en temas de seguridad, tales como seguridad de las comunicaciones, seguridad de la infraestructura, criptografía, control de acceso, autenticación, ataques externos y seguridad operativa y de la organización.

A continuación se encuentran las certificaciones en seguridad de la información que serán tenidas en cuenta para asegurar la idoneidad de los integrantes del equipo de trabajo:

- CISSP (Certified Information Systems Security Professional) - ISC2.
- CISA (Certified Information Systems Auditor) - ISACA.
- CISM (Certified Information Security Manager) – ISACA.
- Lead Auditor BS7799-2 o ISO 27001
- Auditor Interno ISO 27001.
- ABCP (Associate Business Continuity Professional) – DRI.
- GSEC (GIAC Security Essentials Certification) – GIAC.
- BCLS 2000 (Administración Continuidad de Negocio) – DRI.
- PMI-RMP (PMI Risk Management Professional) – PMI.
- CompTIA Security+.
- CEH (Certified Ethical Hacker).

8. SUPUESTOS

La infraestructura tecnológica (hardware y software) requerida para la ejecución de los test de intrusión será provista por el contratista y los mismos se ejecutaran sobre la infraestructura tecnológica designada por la Imprenta Nacional de Colombia (p. ej. servidores, sistemas operativos, dispositivos de red, red LAN, red inalámbrica, equipos de cómputo, etc).

9. TIPO DE PROPUESTA

Propuesta Técnica Simplificada (PTS).

10. CRONOGRAMA

CRONOGRAMA DE ACTIVIDADES																		
Fase / Etapa				**Semana**														
				1	**2**	**3**	**4**	**5**	**.**	**.**	**.**	**.**	**15**	**16**	**17**	**18**
Plan de Trabajo	E0	-	Firma Acta de Inicio.													
Fase 1	E1		Análisis GAP (Diagnóstico ISO 27001 e ISO 27002).													
	E2	-	Gestión de Activos de Información (levantamiento, inventario y clasificación de activos de información, caracterización de Usuarios e índice de información clasificada y reservada).													
	E3	-	Gestión de Riesgos (Análisis y Evaluación de Riesgos).													
Fase 2	E4	-	Definición de Políticas de Seguridad de la Información.													
	E5	-	Gestión de Incidentes.													
	E6	-	Plan de Continuidad de Información y Tecnología.													
Fase 3	E7	-	Definición del Proceso de Administración de la Cultura de Seguridad de la Información.													

CRONOGRAMA DE ACTIVIDADES																		
Fase / Etapa				Semana														
				1	2	3	4	5	.	.	.	.	15	16	17	18		
	E8	-	Implementación del Proceso de Administración de la Cultura de Seguridad de la Información.															
Fase 4	E9	-	Test de Intrusión (Externo e Interno).															
	E10	-	Definición de Arquitectura de Seguridad.															
	E11	-	Transición de IPv4 a IPv6.															
Fase 5	E12	-	Diagnóstico del cumplimiento de la estrategia de Gobierno en Línea – GEL															
	E13	-	Implementación del Sistema de Gestión de Seguridad de la Información – SGSI – para los procesos misionales (Gestión Comercial, Gestión de Producción, Gestión Financiera y Gestión Informática)															

11. SEGUIMIENTO AL DESARROLLO DEL CONTRATO

11.1. REUNIONES

Como parte de las actividades de control al desarrollo del contrato, se efectuaran reuniones de seguimiento cuya periodicidad será definida en el Comité Técnico y en la cual participarán:

- El Gerente de Proyecto del contratista.
- El Gerente de proyecto de la Imprenta Nacional de Colombia.
- El supervisor del contrato por parte de la Imprenta Nacional de Colombia.

De estas reuniones el supervisor elaborará las actas respectivas, las cuales deberán ser formalizadas por las partes dentro de los siguientes cinco (5) días hábiles a su entrega para revisión y harán parte de la base documental del proyecto.

11.2. INFORMES

Quincenalmente, el contratista deberá presentar un informe de avance, que debe contener como mínimo:

- Relación de actividades desarrolladas durante el periodo del informe.
- Relación de actividades a desarrollar durante el siguiente periodo.
- Relación de logros (hitos) alcanzados en el período.
- Relación de logros (hitos) a alcanzar en el siguiente período.
- Cronograma actualizado.
- Situaciones que requieren de manejo porque afecta o podrían afectar el desarrollo del proyecto.
- Acciones sugeridas para resolver dichas situaciones.

Estos informes serán revisados y aprobados por el supervisor del contrato y harán parte de la base documental del proyecto.

11.3. CONTROL DE CALIDAD

11.3.1. RESPONSABILIDADES Y JURISDICCIÓN SOBRE LA CALIDAD

El contratista debe garantizar el desarrollo del objeto del contrato aplicando la metodología establecida en la propuesta. La responsabilidad por la Gestión de Calidad del desarrollo del objeto del contrato está a cargo del Gerente del Proyecto y cada colaborador es su propio inspector de calidad y está consciente de su responsabilidad como proveedor de servicios.

11.3.2. POLÍTICAS DE CALIDAD

Las políticas de calidad definidas para el proyecto son:

- Las acciones de calidad deben estar dirigidas a asegurar que los productos y entregables del proyecto cumplan los objetivos, los requerimientos y las especificaciones técnicas definidas.
- La responsabilidad de la calidad del proyecto es un asunto compartido entre las dos partes, las cuales tienen responsabilidades y obligaciones definidas en estos Pliegos de Condiciones, en los documentos contractuales y en los documentos aprobados oficialmente. Por ello, cada una de las partes debe establecer los mecanismos de calidad que aseguren que su participación en el proyecto es efectiva y eficaz.

- Las acciones u omisiones de cada una de los involucrados puede impactar la calidad del proyecto y por tanto cada integrante de los grupos de trabajo debe estar abierto al examen de su aporte al proyecto y a modificar la manera como participa en él en caso de ser necesario.
- La calidad cubre todo el ciclo de vida del proyecto y por tanto las acciones de calidad deben ser revisadas y actualizadas a la luz de los hechos y los cambios que ocurran en el proyecto.
- El aseguramiento de la calidad del proyecto requiere que exista evidencia que todos los productos y entregables han sido revisados antes de ser entregados oficialmente y que han pasado los controles correspondientes, es decir, verificar que los documentos cumplan con las siguientes características:
  - ✓ Que el documento este dentro de los lineamientos generales de calidad: Tiene estructura, tiene un control de cambios e indicar si está formando parte de otro documento.
  - ✓ Que siga la estructura definida y cumpla con todas las actividades necesarias para la entrega del documento.
- Mantener un respaldo de la información generada durante la ejecución de este proyecto.

11.3.3. CONTROL DE CALIDAD

El control de calidad implica verificar los resultados específicos del proyecto para determinar si estos cumplen con los estándares de calidad relevantes e identificar las causas de los resultados no satisfactorios.

Los controles de calidad se harán durante todo el desarrollo del proyecto y serán registrados sobre:

- Los entregables, de acuerdo al procedimiento de desarrollo del proyecto.
- Informes de avance del proyecto, en cuanto a lo planeado.

Antes de entregar cualquier producto (sea un documento o un informe) se realizará un proceso de revisión del cumplimiento de las especificaciones técnicas que estará a cargo del grupo de control de calidad del contratista.

Es importante mantener desde el inicio del proyecto un seguimiento continuo del mismo a través de reuniones periódicas entre el contratista y los representantes de la Imprenta Nacional de Colombia.

Las siguientes son pautas a tener en cuenta para obtener un buen resultado en las reuniones de seguimiento:

- Se debe tener una agenda y una mecánica en la cual se defina el tiempo para cada tema.
- Se deben revisar las tareas que se plantearon en la reunión anterior y cuando sea necesario se debe dejar en claro las tareas y compromisos que se adquieran y los responsables respectivos.
- Debe quedar un acta firmada por las dos partes de lo discutido en las reuniones de seguimiento.

11.3.4. ASEGURAMIENTO DE LA CALIDAD

Consiste en evaluar todas las actividades del proyecto en el marco del sistema de calidad, para brindar confianza de que el proyecto satisface los requerimientos de los usuarios.

Esta labor es proactiva más que reactiva, para mejorar no solo los productos finales sino el mismo proceso de desarrollo, con el fin de prevenir errores, más que detectarlos al final.

Las principales actividades para el aseguramiento de la calidad son:

- Controlar la calidad mediante muestreos de los productos contra los estándares establecidos para el proyecto.
- Recomendar acciones correctivas y preventivas para las actividades del proyecto en caso de ser necesario.
- Registro de las revisiones de Aseguramiento de la calidad para cada uno de los entregables.
- Asesorar al grupo de trabajo sobre cómo enfrentar las tareas de aseguramiento de calidad, tales como estándares, terminología, uso adecuado de modelos genéricos, etc.

11.3.5. GESTIÓN DOCUMENTAL

La información que sea procesada en el transcurso del proyecto, debe catalogarse y almacenarse en medio magnético e impreso, en un lugar seguro (repositorio documental). Sus directos responsables serán el Director de Proyecto por parte del Contratista y el Supervisor del Contrato por parte de la Imprenta Nacional de Colombia.

Además, se mantendrá un archivo cronológico en la carpeta del proyecto con la totalidad de los comunicados y se recomienda que para aquellas conversaciones telefónicas que resulten de relevancia, su contenido quede reflejado por escrito mediante carta, fax o cualquier otro medio, y que sean enviadas para que quede constancia.

Preparó: César Gustavo González Forero – Jefe de Oficina – Oficina de Sistemas e Informática

Revisó: María Liliana Navarro Martin – Técnico Calificado 05 - Oficina de Sistemas e Informática

Gladys Patricia Silva Cordero – Asesora de Gerencia