ANEXO TÉCNICO PARA CONTRATAR LOS SERVICIOS ESPECIALIZADOS EN SEGURIDAD DE LA INFORMACIÓN PARA LA CONSTRUCCIÓN DE UN MODELO DE IMPEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN SGSI, Y LA EJECUCIÓN DEL MODELO EN SU PRIMERA FASE PARA EL ICFES

METODOLOGÍAS / MARCOS NORMATIVOS A APLICAR	
1	**ESPECIFICACIÓN TÉCNICA MÍNIMA**

El Proveedor deberá aplicar y exponer los siguientes marcos normativos que corresponden a buenas prácticas de aceptación internacional:

1. Para la implementación de los controles de seguridad tener en cuenta la norma ISO/IEC 27002:2013
2. Aplicar los requerimientos de certificación del SGSI enunciados en la norma internacional ISO/IEC27001:2013.
3. Para la gestión de servicio deberá utilizar la el marco normativo ISO20000.
4. Para efectos del análisis y tratamiento del riesgo, se debe adoptar lo expresado en la norma internacional ISO 31000, ISO 27005 y los lineamientos de gobierno en Línea.
5. Para las pruebas de seguridad en redes y aplicaciones se debe utilizar las metodologías OSSTMM (Metodología de pruebas a redes) y/o OWASP (Metodología enfocada a pruebas de seguridad a aplicaciones).
6. Garantizar que el sistema de Gestión de Seguridad de la Información esté alineado con lo que establece el Manual 4.0 de Gobierno en Línea, así como seguir el Modelo 3.0 de Seguridad y Privacidad de la información y el Decreto 2573 de 2014, al momento de ejecución del proyecto. Considerar los aspectos del Sistema de Gestión de Calidad (SGC) con que cuenta la Entidad basado en la Norma ISO 9001.
7. Garantizar que el sistema de gestión de seguridad de la información a implementar se encuentre alineado y complemente al sistema de gestión de calidad del ICFES. De acuerdo a los resultados del análisis de brechas proponer la implementación del sistema de gestión de seguridad de la información a mínimo los procedimientos que se listan a continuación ó a nuevos procedimientos recomendados a partir de la ejecución del contrato:

PROCESO	SUBPROCESO	PROCEDIMIETO	
C. GESTIÓN DE PRUEBAS Y OPERACIONES	C1.CONSTRUCCIÓN Y MANTENIMIENTO DE ITEMS	C1.P1 Construcción de Ítems	
	C2. ASEGURAMIENTO DE RECURSOS	C3.P1 Aseguramiento de Infraestructura C3.P3 Aseguramiento de Material C3.P4 Aseguramiento Distribución de Material	
	C3.REGISTRO	C4.P3 Registro y Citación	

8. El proveedor incluirá en el costo del proyecto la adquisición legal de las normas ISO requeridas para uso en la entidad.

#	Actividad	Descripción de la actividad	Entregables
1	Kick Off Y Cronograma	Reunión de apertura: El Proveedor, debe presentar un cronograma detallando al inicio del contrato del desarrollo de todas las actividades de acuerdo a todas las actividades del ciclo PHVA. Las etapas del proyecto y sus actividades deben presentarse identificadas por semana y contener el equipo de trabajo asignado a cada actividad.	Cronograma detallado, el cual será aprobado por el supervisor del contrato. El contratista hará entrega de este cronograma al supervisor del contrato dentro de los 7 días hábiles siguientes a la aprobación de la garantía de cumplimiento del mismo.
2	Informes semanales	El Proveedor deberá reportar con informes semanales y consolidados del avance y los resultados obtenidos, al personal del ICFES asignado para la ejecución del proyecto. Debe quedar constancia documental de las decisiones de la dirección en todo el avance de la implementación del sistema de gestión de seguridad de la información en el alcance del contrato.	Actas de reunión con el resumen ejecutivo del avance del proyecto firmado por los asistentes. Actas de las decisiones y aprobación de la dirección y/o comité y personal involucrado en el desarrollo de la implementación del sistema de gestión de seguridad de la información.
ETAPA 1: ANÁLISIS DE LA SITUACIÓN ACTUAL Y DEFINICIÓN DE BRECHAS			
#	**Actividad**	**Descripción de la actividad**	**Entregables**
	Diagnostico	El Proveedor debe identificar y revisar la operación actual de todo el ICFES, para lo cual deberá considerar y analizar toda la infraestructura tecnológica y el detalle de todos los procesos y subprocesos que soportan el sistema de gestión de calidad del ICFES. Realizar el análisis GAP a todos los procesos y subprocesos que soportan el sistema de gestión de calidad del ICFES. Hallar la valoración del nivel de madurez alcanzado en la implementación actual de la práctica de gestión de seguridad contra la norma ISO/IEC 27001:2013 la cual dispone de unas cláusulas cuya finalidad es establecer, implementar, operar, monitorear, revisar, mantener y mejorar un SGSI, en el contexto de los requerimientos de la institución. Esta verificación deberá realizarse como mínimo sobres 114 controles establecidos por la norma ISO 27001:2013 contra lo existente en el ICFES. Determinar el estado actual de la gestión de seguridad y privacidad de la información al interior de la Entidad, teniendo en cuenta la infraestructura de red de comunicaciones (IPv4/IPv6).	El Proveedor debe hacer entrega de un documento con los resultados finales del análisis de brechas (GAP), y la identificación del nivel de madurez y principales hallazgos y recomendaciones resultado del análisis GAP para cada dominio de la Norma ISO27001:2013. Este documento estará sujeto a la aprobación del supervisor del contrato. Documento con el resultado de la autoevaluación realizada a la Entidad, de la gestión de seguridad y privacidad de la información e infraestructura de red de comunicaciones (IPv4/IPv6), revisado y aprobado por la alta dirección. Documento con el resultado de la estratificación de la entidad, aceptado y aprobado por la dirección. Documento con la justificación y aprobación por parte de la dirección y del personal

		Se recomienda utilizar alguno de estos modelos definidos: CMMI (Capability Maturity Model Integration) Modelo ISM3 (Information Security Management Maturity Model), ó Escala de valoración del nivel de madurez COBIT	responsable de los procedimientos a los cuales debe iniciarse la implementación del SGSI. El Proveedor entregará las especificaciones y detalle del modelo de madurez definido, y la escala de cálculos para la valoración del nivel de madurez. Modelo de implementación del sistema de gestión de seguridad de la información SGSI. Toda esta información (documentos) debe quedar preparada para ser gestionada dentro del Software de SGSI con que cuente el ICFES en el momento de la ejecución del contrato. Estos entregables y sus documentos estarán sujetos a la aprobación del supervisor del contrato.
	Inventario y clasificación de activos	Realizar el inventario y clasificación de activos orientado a los activos que soportan el alcance definido y demás aprobado en el análisis de brechas. El Proveedor debe definir y documentar la clasificación de todos los activos de información definidos y aprobados; y demás aspectos que considere relevantes, permitiendo su gestión de acuerdo con la Norma ISO 20000; y dando cumplimiento con los lineamientos definidos en la Norma ISO/IEC 27001:2013 en el ítem de "Gestión de Activos; y la metodología de clasificación de activos- modelo de seguridad de la información para la estrategia de gobierno en línea en su última versión. La clasificación de los activos de información debe estar basada según la necesidad, las prioridades, y el grado de criticidad o importancia de cada activo. Debe evaluarse el impacto, del daño o perjuicio resultante en caso de resultar comprometido el contenido específico del activo. Se debe definir una guía de publicación de información sujeta al cumplimiento de todas las leyes vigentes para el acceso a la información pública, su tratamiento y su publicación.	Documento con la clasificación e inventario de todos los activos de información definidos y aprobados y demás aspectos que considere relevantes. Guía de publicación de información sujeta al cumplimiento de todas las leyes vigentes para el acceso a la información pública, su tratamiento y su publicación. Toda esta información (documentos) debe quedar preparada para ser gestionada dentro del Software de SGSI con que cuente el ICFES en el momento de la ejecución del contrato. Estos entregables y sus documentos estarán sujetos a la aprobación del supervisor del contrato.
	Estructura de	El Proveedor deberá definir y crear un	Documento con la estructura de

	seguridad	documento y determinar si se establece como procedimiento para la actualización, mantenimiento, implementación y sostenibilidad del modelo de seguridad de la Información en implementación. Definir la estructura de seguridad de información del ICFES explicando la importancia de esa estructura, sus funciones y los roles que se necesitan, los responsables de seguridad de la información del ICFES, así como los perfiles y funciones de las personas que la deben integrar y recomendar mejoras teniendo en cuenta todos los requisitos de la norma ISO27001:2013. El proveedor deberá definir un documento plan y la estrategia de transición de IPv4 a IPv6.	seguridad del ICFES, explicando la importancia de esa estructura, sus funciones y los roles que se necesitan, los responsables de seguridad de la información del ICFES, así como los perfiles y funciones de las personas que la deben integrar. Documento que establezca los lineamientos para la actualización, mantenimiento, implementación y sostenibilidad del modelo de seguridad de la Información en implementación. Toda esta información (documentos) debe quedar preparada para ser gestionada dentro del Software de SGSI con que cuente el ICFES en el momento de la ejecución del contrato. Estos entregables y sus documentos estarán sujetos a la aprobación del supervisor del contrato.
ETAPA 2: ANÁLISIS DE RIESGOS (Identificación de riesgos, de la metodología para evaluar los riesgos y determinar los criterios para la aceptación de los riesgos)			
#	**Actividad**	**Descripción de la actividad**	**Entregables**

	Metodología de análisis de riesgo.	Definición e implementación de la metodología de análisis de riesgo. El Proveedor deberá definir y describir la metodología de Análisis de Riesgos a utilizar por él, la cual deberá basarse como mínimo en las normas ISO 31000:2009 ó NTC 5254 o NIST SP 800-30 o ISO 27005 y acoger las recomendaciones de la ISO/IEC 27001:2013 aplicables y la metodología de gestión del riesgo modelo de seguridad de la información para la estrategia de gobierno en línea en su última versión. Crear el plan de tratamiento de riesgos que identifique como mínimo las acciones, recursos, responsabilidades y prioridades en la gestión de los riesgos de seguridad de la información. Tener en cuenta en el plan de tratamiento de riesgo la recomendación de revisión de los riesgos y proponer los intervalos/periodos de revisión, los riesgos residuales y sus niveles aceptables, teniendo en cuenta los posibles cambios que hayan podido producirse en las entidades, la tecnología, los objetivos y procesos misionales, las amenazas identificadas, la efectividad de los controles implementados, los requerimientos legales y obligaciones contractuales, entre otros. Convocar reunión con la alta dirección, mostrar los resultados obtenidos en el análisis de riesgos, como se realizara el tratamiento del riesgo, que controles se implementaran, y decidir con la alta dirección la aceptación de los riesgos, cuales riesgos se transfieren, cuales se aceptan y cuales se evitan. Es decir aprobar por parte de la dirección tanto los riesgos residuales como la implantación y uso del SGSI para el alcance definido.	Definición y presentación de de la metodología para el análisis de riesgo. Documento plan para el tratamiento del riesgo que oriente a la priorización, implementación y mantenimiento de los controles definidos de acuerdo con lo definido en la declaración de aplicabilidad, revisado y aprobado por la alta Dirección. Documento con la estrategia de planificación y control operacional, revisado y aprobado por la alta Dirección. Documento con las decisiones tomadas por la alta dirección respecto al tratamiento del riesgo, aceptación de los riesgos residuales, uso del SGSI para el alcance definido y demás acciones relacionadas en la actividad. Toda esta información (documentos) debe quedar preparada para ser gestionada dentro del Software de SGSI con que cuente el ICFES en el momento de la ejecución del contrato. Estos entregables y sus documentos estarán sujetos a la aprobación del supervisor del contrato.
	Evaluación del Riesgo	De acuerdo al levantamiento de los activos de información definidos y aprobados, se debe realizar la evaluación del riesgo asociado a dichos activos para mínimo 100 activos, como mínimo especificar amenazas internas y externas, vulnerabilidades, escenarios de riesgo, probabilidad de ocurrencia de la amenaza e impacto si llega a materializarse la amenaza y demás aspectos que considere relevante para la identificación de los riesgos. De acuerdo a la identificación de los activos: - Identificar las amenazas en relación a los activos;	Documentos con el análisis de riesgo teniendo en cuenta lo solicitado en la actividad del mismo. Toda esta información (documentos) debe quedar preparada para ser gestionada dentro del Software de SGSI con que cuente el ICFES en el momento de la ejecución del contrato.

		- Identificar las vulnerabilidades que puedan ser aprovechadas por dichas amenazas; - Identificar y evaluar (cualitativa, cuantitativamente) el impacto al negocio de un fallo de seguridad que afecte la confidencialidad, integridad y disponibilidad de cada uno de los activos de información identificados. - Evaluar de forma realista la probabilidad de ocurrencia de un fallo de seguridad en relación a las amenazas, vulnerabilidades, impactos en los activos y los controles que ya estén implementados; - Estimar los niveles de riesgo.	Estos entregables y sus documentos estarán sujetos a la aprobación del supervisor del contrato.
	matriz de identificación y valoración del nivel de riesgo	El Proveedor debe elaborar la matriz de identificación y valoración del nivel de riesgo basados en la confidencialidad, integridad y disponibilidad, en la que se deberá reflejar 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, probabilidad de ocurrencia, y el nivel de desempeño de los controles planeados o existentes, para reducir o eliminar el riesgo.	Documento mapa de riesgos de gestión de seguridad de la información para los procedimientos definidos y aprobados del sistema de gestión de seguridad de la información y la explicación detallada de la matriz de riesgos. Toda esta información (documentos) debe quedar preparada para ser gestionada dentro del Software de SGSI con que cuente el ICFES en el momento de la ejecución del contrato. Estos entregables y sus documentos estarán sujetos a la aprobación del supervisor del contrato.
	Declaración de Aplicabilidad	Elaborar la Declaración de Aplicabilidad – DDA que cubra todo el ICFES. El proveedor deberá crear un documento denominado la declaración de aplicabilidad, que contiene los objetivos de control y los controles de seguridad contemplados en la norma ISO 27001:2013/27002:2013 y demás controles que se consideren necesarios incluir de otros catálogos, basados en los resultados de los procesos de evaluación y tratamiento de los riesgos, justificando detalladamente las inclusiones y exclusiones de los controles.	Documento denominado la declaración de aplicabilidad de seguridad de la información que debe contener como mínimo: La enumeración y descripción al detalle de todos los controles, y la justificación de cuáles controles son aplicables al ICFES y cuáles no, definir los motivos de la decisión de aplicabilidad, los objetivos que se lograrán con los controles y describir cómo se implementarán; alineado este documento al anexo A de la norma ISO 27001:2013

			Toda esta información (documentos) debe quedar preparada para ser gestionada dentro del Software de SGSI con que cuente el ICFES en el momento de la ejecución del contrato. Estos entregables y sus documentos estarán sujetos a la aprobación del supervisor del contrato.
	Revisión y Definición de políticas de seguridad de la información	Revisión y Definición de políticas de seguridad de la información, procesos y procedimientos de seguridad de la información. El Proveedor deberá realizar la revisión, ajuste y actualización de las 15 políticas implementadas, y el subproceso GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN, junto con sus 3 procedimientos implementados en la entidad, separando políticas, de estándares, mejores prácticas, guías y procedimientos. Estos lineamientos deben definirlos y ajustarlos de acuerdo con las buenas prácticas de seguridad de la información, la norma ISO/IEC 27001:2013 y deberá tenerse en cuenta el resultado obtenido en el numeral de “Evaluación del riesgo” de este anexo. El proveedor debe documentar una política para desarrollo seguro de software y sistemas donde se definan las reglas básicas para el desarrollo de aplicaciones en el ICFES. Para la estructuración de esta política se recomienda basarse en la última edición de la Guía para Construir Aplicaciones y Servicios Web Seguros (OWASP) Las políticas actualizadas y definidas deben alinearse a los dominios de la Norma ISO 27001:2013 y para dar cumplimiento de las políticas de seguridad establecer los objetivos de control asociados a cada política. Se deberá utilizar la guía de implementación de políticas del modelo de seguridad de la información para la estrategia de gobierno en línea en su última versión.	Documentos de las políticas de seguridad de la información actualizados y aprobados. Documentos definidos como estándares, procedimientos, mejores prácticas y guías, aprobados y formalizados. Toda esta información (documentos) debe quedar preparada para ser gestionada dentro del Software de SGSI con que cuente el ICFES en el momento de la ejecución del contrato. Estos entregables y sus documentos estarán sujetos a la aprobación del supervisor del contrato.
	Ejecución y análisis de Pruebas de seguridad	Ejecución y análisis de Pruebas de Vulnerabilidades y Penetración a fallas(internas y externas) a aplicativos y a infraestructura (perimetral) El Proveedor mediante la realización de las pruebas de vulnerabilidades y penetración deberá encontrar las áreas de la red y de las aplicaciones del ICFES donde los intrusos	Documento con la planeación y alcance de las pruebas donde se incluya metodología, Intensidad de las pruebas (denegación o no del servicio) si se requiere afinamiento de direcciones IP, y aplicativos, definición de los escenarios de ejecución de las pruebas, Tipo de prueba, fechas, duración, Puntos desde los cuales se realizará la

		pueden sacar ventaja de las vulnerabilidades existentes es decir medir el nivel de seguridad de la plataforma. El Proveedor deberá realizar las pruebas de penetración a la infraestructura tecnológica que soporta los procesos críticos del ICFES (Firewall, enrutadores, bases de datos, servidores web, servidores de correo, servidores FTP (File Transfer Protocol - protocolo de transferencia de archivos) y servidores DNS (domainnamesystem, sistema de nombres de dominios, etc.), Determinar entre proveedor y el ICFES aquellos objetivos específicos a realizar las pruebas. El proveedor deberá enviar informes periódicos del avance de las pruebas realizadas. Seguridad perimetral: se centra en validar el entorno (la red) por donde circula la información, revisando la infraestructura que se tiene y los controles que se tienen sobre acceso y ataques de seguridad desde puntos externos al entorno. Seguridad de aplicativos: se encarga de validar las diferentes aplicaciones que se tienen en el ICFES como estas se comunican y sirven de puertas de acceso afuera del perímetro, las aplicaciones generalmente se exponen a entornos sensibles a ataques de seguridad y por ende es necesario validar los riesgos asociado y la robustez, protección e integridad que estas brindan de la información que allí se almacena o transmite. **Tipos de pruebas mínimas a realizar para infraestructura y aplicativos:** • Adivinar claves mediante fuerza bruta. • Acceso no autorizado a sistemas. • Suplantar algún usuario a partir de claves no confiables, planas o almacenadas. • Conocer información confidencial. • Predecir o adivinar URLs que deben tener acceso restringido. • Cambiar el código fuente en ambiente de producción sin ser certificado (Solo para aplicativos). • Administrar un sistema desde ubicaciones no confiables. • Inyectar software o código malicioso. • Engañar a un usuario para que ejecute acciones no intencionales en una aplicación. • Capturar credenciales administrativas. • Provocar comportamiento inestable del sistema debido a software en estado inmaduro.	prueba, las Ips desde donde Se realizarán los ataques, y la solicitud de insumos para la realización de las mismas. Documento con el reporte de la ejecución de las pruebas, análisis de vulnerabilidades, catalogación y clasificación de la vulnerabilidad de acuerdo a su severidad e impacto sobre el dispositivo afectado en alto, medio, bajo, descripción de la vulnerabilidad, e impacto que represente para el negocio según: Common Vulnerabilities and Exposures (CVE) y los requisitos de seguridad propios del proceedor, y la validación de la métrica Métricas CVSSv2; eliminación de falsos positivos del informe, verificación de puertos TCP/UDP, resultados de las pruebas de penetración, priorización de las vulnerabilidades y recomendaciones para el tratamiento de mitigación de la vulnerabilidad, e informes ejecutivos del resultado de las pruebas y plan de acción a seguir para corregir las vulnerabilidades y mejorar del nivel de seguridad de los activos analizados. Al terminar la ejecución de las pruebas el proveedor debe realizar una presentación final al personal definido por el ICFES donde muestren a groso modo toda la ejecución del proyecto y muy importe los resultados de seguridad y recomendaciones urgentes e importantes priorizados por nivel de impacto, plan de acción a seguir, oportunidades de mejoramiento y el informe ejecutivo de los hallazgos urgentes críticos e importantes a darles prioridad y conclusiones. Estos entregables y sus documentos estarán sujetos a la aprobación del supervisor del contrato.

		• Aprovechar vulnerabilidades conocidas en los activos definidos para las pruebas e intentar explotarlas. • Registrar un falso usuario en el sistema. La cantidad de activos a analizar son: 10 URL's correspondientes a aplicativos web que prestan diferentes servicios a los usuarios del ICFES. 12 IP's externas SERVICIO/APLICATIVO/SERVIDOR 12 IP's internas de SERVICIO/APLICATIVO/SERVIDOR El Proveedor deberá utilizar herramientas para estas pruebas de exploración y penetración, las cuales deben estar licenciadas y deberán anexar la información o comprobante que indica su propiedad, una vez se inicie la ejecución del contrato. El Proveedor debe cumplir a cabalidad con el acuerdo de confidencialidad para la ejecución de estas pruebas y de todo el desarrollo del proyecto.	
	Pruebas de ingeniería social	Ejecución de pruebas de ingeniería social, a 10 personas que apoyan en los procesos críticos identificados a implementar el SGSI y a 20 personas del resto de la entidad, usando técnicas directas o físicas, invasivas, seductivas o inadvertidas.	Documento con la planeación de las pruebas de ingeniera social a realizar, la descripción de las actividades y los resultados de la prueba de ingeniera social. Estos entregables y sus documentos estarán sujetos a la aprobación del supervisor del contrato.
	Análisis de Riesgos en el modulo de construcción de ítems.	Analizar el modulo de construcción de Ítems y evaluar el nivel de seguridad. Realizar el análisis de Riesgos en el modulo de construcción de ítems del aplicativo PRISMA. En el análisis de riesgos del módulo de Construcción de Ítems que está destinado a ofrecer servicios a través de una plataforma web y deben identificarse como mínimo las medidas de seguridad requeridas para evitar la aparición de vulnerabilidades que afecten la confidencialidad, integridad y disponibilidad. La identificación de los riesgos debe realizarse sobre 5 frentes analizando: 1. Aspectos de desarrollo, 2. Aspectos de arquitectura de aplicaciones y de base de datos, 3. Manejo de la seguridad de la información, 4. Aspectos de	Informe con la metodología para el análisis de riesgos del modulo de construcción de ítems y el cronograma de actividades. Informe de la evaluación del riesgo sobre los 5 frentes principales, teniendo en cuenta la probabilidad de una amenaza y la magnitud del impacto sobre el sistema con respecto a: confidencialidad, disponibilidad e integridad. Informe de las medidas mínimas de seguridad que debe tener en cuenta el módulo de construcción de Ítems tanto a nivel de Intranet, como a nivel WEB con el fin de mitigar los riesgos en la

		infraestructura, 5 Manejo de archivos; teniendo en cuenta para cada uno como mínimo aspectos técnicos (Tecnología, complejidad e interfaces, rendimiento, fiabilidad y calidad), Externos(Subcontratistas, condiciones legales, cliente, condiciones de seguridad física del área interna de construcción de Ítems) De la organización(Dependencia del proyecto, Recursos, Financiación, Priorización), Dirección del proyecto (Estimación, planificación, control, comunicación).	confidencialidad, integridad y disponibilidad de la información. Adicional al informe debe entregar el prototipo ó guías de implementación de las recomendaciones de solución. Estos entregables y sus documentos estarán sujetos a la aprobación del supervisor del contrato.
	Casos de abuso	Crear casos de abuso sobre el 30% del total de casos de uso para el modulo de construcción de ítems del aplicativo misional, y determinar cómo mitigar los riesgos identificados y posibles ataques.	Informe determinando las partes del sistema que son más fáciles de comprometer, cual es el impacto y la identificación y priorización de amenazas. Estos entregables y sus documentos estarán sujetos a la aprobación del supervisor del contrato.
	Propuesta de mejoramiento arquitectura de ítems.	Propuesta de arquitectura. Conocimiento de la arquitectura actual de la entidad en relación con la sistematización del proceso de construcción de Ítems. Basado en el conocimiento de la arquitectura recomendar dos modelos de arquitectura segura que permitan mantener una postura de seguridad aceptable sobre los activos de tecnología que van a soportar el proceso de construcción de ítems.	Informe y hallazgo de vulnerabilidades en la arquitectura. Propuesta de los dos modelos de mejoramiento de arquitectura segura teniendo en cuenta las mejores prácticas y tendencias del mercado de soluciones tecnológicas de seguridad. Estos entregables y sus documentos estarán sujetos a la aprobación del supervisor del contrato.
	Análisis de Riesgos en la plataforma de pruebas electrónicas.	Analizar la plataforma de pruebas electrónicas y evaluar el nivel de seguridad. Realizar el análisis de riesgos a la plataforma de pruebas electrónicas que ofrece servicios a través de una plataforma web, por lo tanto deben identificarse las medidas de seguridad mínimas para evitar la aparición de vulnerabilidades que afecten la confidencialidad, integridad y disponibilidad. La identificación de los riesgos debe realizarse sobre 5 frentes analizando: 1. Aspectos de desarrollo, 2. Aspectos de arquitectura de aplicaciones y de base de datos, 3. Manejo de la seguridad de la información, 4. Aspectos de infraestructura, 5 Manejo de archivos; teniendo en cuenta para cada uno como mínimo aspectos técnicos (Tecnología, complejidad e interfaces, rendimiento, fiabilidad y calidad), Externos(Subcontratistas, condiciones legales, cliente, condiciones de seguridad física del área	Informe con la metodología para el análisis de riesgos de la plataforma de pruebas electrónicas y el cronograma de actividades. Informe de la evaluación del riesgo sobre los 5 frentes principales, teniendo en cuenta la probabilidad de una amenaza y la magnitud del impacto sobre el sistema con respecto a: confidencialidad, disponibilidad e integridad. Informe de las medidas mínimas de seguridad que debe tener en cuenta en la plataforma de pruebas electrónicas con el fin de mitigar los riesgos en la confidencialidad, integridad y disponibilidad de la información. Adicional al informe debe entregar el prototipo ó guías de implementación de las

		interna de construcción de Ítems) De la organización(Dependencia del proyecto, Recursos, Financiación, Priorización), Dirección del proyecto (Estimación, planificación, control, comunicación).	recomendaciones de solución. Estos entregables y sus documentos estarán sujetos a la aprobación del supervisor del contrato.
ETAPA 3: IMPLEMENTACIÓN Y CONCIENTIZACION DE SEGURIDAD DE LA INFORMACIÓN			
#	**Actividad**	**Descripción de la actividad**	**Entregables**
	Manual del SGSI	Elaboración del Manual del SGSI: Documento que inspira y dirige todo el sistema, el que expone y determina las intenciones, alcance, objetivos, responsabilidades, políticas y directrices principales, del SGSI.	Documento manual del sistema de gestión de seguridad de la información aplicable a toda la entidad, e integrado con el sistema de gestión de calidad. Toda esta información (documentos) debe quedar preparada para ser gestionada dentro del Software de SGSI con que cuente el ICFES en el momento de la ejecución del contrato. Estos entregables y sus documentos estarán sujetos a la aprobación del supervisor del contrato.
	Matriz, política y manual de tratamiento de información.	Identificar las áreas de tratamiento de datos personales, los servicios que prestan y en base a esto y a la normatividad legal vigente elaborar una matriz de custodios por área- responsable del tratamiento. Revisión y ajustes de la política de Tratamiento de Información para los usuarios internos y externos del ICFES. Revisión y ajuste del manual de tratamiento de datos personales del ICFES.	Matriz de custodios de la información. Documento actualizado de la política de tratamiento de información. Documento Manual de tratamiento de datos personales. Documento Política de tratamiento de información para los usuarios internos y externos del ICFES. Toda esta información (documentos) debe estar contenida y gestionada dentro del Software de SGSI, por lo cual el Proveedor debe dar las instrucciones requeridas al personal asignado por el ICFES para el diligenciamiento de la información. Estos entregables y sus documentos estarán sujetos a la aprobación del supervisor del contrato.
	Concientización	Ejecución de programas de concientización de seguridad. El Proveedor deberá diseñar un plan de	Plan de comunicación, sensibilización y capacitación, con los respectivos soportes, revisado y aprobado por la alta Dirección.

		formación y generación de cultura en seguridad de la información que permita a los usuarios la formación y sensibilización con respecto a la seguridad de la información. Así mismo, debe incluir en el plan la comunicación y divulgación (determinar los grupos objetivo, temas, tiempos de ejecución y cómo se les debe comunicar, y qué material debe ser usado para cada grupo) y definir un mecanismo para medir el nivel de concientización en seguridad de la información. Elaboración de material y contenidos de la capacitación de acuerdo con el público objetivo. (Videos, souvenirs, posters, obra teatral, show humor, etc.) Mínimo una (1) actividad lúdica de sensibilización en seguridad de la información para mínimo 150 usuarios internos de la entidad donde se incluya la divulgación de las políticas de seguridad definidas por el ICFES. Esta sensibilización puede dividirse en grupos para los diferentes perfiles del personal que laboran en el ICFES. Curso de auditor Líder ISO 27001 que incluya el material, Examen Internacional Lead Auditor ISO 27001 por el certificador internacional avalado, y entrega de certificación oficial como Lead Auditor a quienes aprueben el exámen.	Mínimo una (1) actividad lúdica de sensibilización en seguridad de la información para mínimo 150 usuarios. Resultados del nivel de medición de la concientización en seguridad de la información. Un evento de concientización para el personal directivo del ICFES, un total de 26 personas. Informe con las evidencias de todas las actividades llevadas a cabo en la concientización del personal. Curso de auditor Líder ISO 27001 para diez (10) funcionarios. Toda esta información (documentos) debe quedar preparada para ser gestionada dentro del Software de SGSI con que cuente el ICFES en el momento de la ejecución del contrato. Estos entregables y sus documentos estarán sujetos a la aprobación del supervisor del contrato.
ETAPA 4: VERIFICACION DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION Y PLAN DE CONTINUIDAD DEL NEGOCIO			
#	**Actividad**	**Descripción de la actividad**	**Entregables**
	Indicadores y métricas	Determinar cómo medir la eficacia de los controles. Proponer, definir y establecer indicadores y métricas para medir la eficacia, cumplimiento y evolución de los dominios y controles implantados dentro del marco del SGSI con el objetivo de medir la efectividad de los controles si realmente cumplen con los requisitos de seguridad con una visión orientada a los niveles de madurez de cada uno (Declaración de aplicabilidad) y establecer el grado de seguridad de la información. Suministrar los insumos necesarios para realizar la medición de los indicadores.	Documento con los indicadores definidos para el SGSI y sus respectivos controles de acuerdo a la declaración de aplicabilidad revisado y aprobado por la alta Dirección. Documento con el detalle para realizar la medición de los indicadores, que contenga entre otras las fórmulas para su cálculo respectivo. Toda esta información (documentos) debe estar contenida y gestionada dentro del Software de SGSI, por lo cual el Proveedor debe dar las instrucciones

			requeridas al personal asignado por el ICFES para el diligenciamiento de la información. Estos entregables y sus documentos estarán sujetos a la aprobación del supervisor del contrato.
	Verificación del SGSI	Verificación de los controles implementados durante el desarrollo del proyecto. Evaluación del plan de tratamiento de riesgos. El Proveedor realizará una verificación sobre la efectividad de la operación de los controles implementados durante el desarrollo (Auditoria). El Proveedor será el responsable de la coordinación de las actividades que se contemplen para la auditoría del SGSI definido en el alcance del proyecto. Para ello considerará tres (3) grupos de controles: 1. Controles identificados durante el desarrollo del proyecto como efectivos. 2. Controles rediseñados durante el desarrollo del proyecto. 3. Controles nuevos sugeridos e implementados durante el desarrollo del proyecto. Validar una muestra del 30% de la totalidad de los controles implementados. Los controles nuevos no serán verificados pero si debe revisarse el diseño y generar las recomendaciones necesarias.	Informe con las recomendaciones del resultado de la verificación de la controles seleccionados, la estructura del informe deberá contener como mínimo los siguientes aspectos: Documento informe de resultado de hallazgos por cada control verificado. Análisis de riesgos. Recomendaciones orientadas a mitigar el riesgo. Evidencias de las mejoras implementadas. Evidencias de medidas preventivas y correctivas. Documento de lecciones aprendidas. Toda esta información (documentos) debe quedar preparada para ser gestionada dentro del Software de SGSI con que cuente el ICFES en el momento de la ejecución del contrato. Estos entregables y sus documentos estarán sujetos a la aprobación del supervisor del contrato.
	Plan de continuidad del Negocio para el área de tecnología.	Elaborar el plan de continuidad del negocio para el área de tecnología. (Business Continuity Plan) donde indique la logística para la práctica de cómo el ICFES debe recuperar y restaurar sus funciones críticas parcial o totalmente interrumpidas dentro de un tiempo predeterminado después de una interrupción no deseada o desastre.	Documento BCP (Plan de continuidad del negocio). Toda esta información (documentos) debe quedar preparada para ser gestionada dentro del Software de SGSI con que cuente el ICFES en el momento de la ejecución del contrato.

			Estos entregables y sus documentos estarán sujetos a la aprobación del supervisor del contrato.
	Documentación del sistema de gestión de seguridad de la información.	Elaborar los procedimientos que regulan cómo se realizan, gestionan y mantienen los documentos de políticas de seguridad, metodología de la evaluación del riesgo, plan de tratamiento del riesgo, la declaración de aplicabilidad y demás que regulan el sistema de gestión de seguridad de la información implementada en el ICFES. Elaborar los procedimientos que aseguran que se realicen de forma eficaz la planificación, operación y control del proceso de seguridad de la información y describen cómo medir la efectividad de los controles. Elaboración de instrucciones, checklists y formularios que corresponde a documentos que describen cómo se realizan las tareas y las actividades específicas relacionadas con la seguridad de la información. Establecer formatos estándar para el cumplimiento con los lineamientos del protocolo de comunicaciones del ICFES y que proporcionen una evidencia objetiva del cumplimiento de todas las actividades del SGSI. Establecerse un lineamiento para el control de la documentación del SGSI que defina las acciones de gestión necesarias para: • Garantizar que los cambios y el estado actual de revisión de los documentos están identificados. • Garantizar que las versiones relevantes de documentos vigentes están disponibles en los lugares de empleo. • Garantizar que los documentos se mantienen legibles y fácilmente identificables. • Garantizar que los documentos permanecen disponibles para aquellas personas que los necesiten y que son transmitidos, almacenados y finalmente desechados acorde con los procedimientos aplicables según su clasificación. • Garantizar que los documentos procedentes del exterior están	Se deben entrar los documentos solicitados en las actividades. Toda esta información (documentos) debe quedar preparada para ser gestionada dentro del Software de SGSI con que cuente el ICFES en el momento de la ejecución del contrato. Estos entregables y sus documentos estarán sujetos a la aprobación del supervisor del contrato.

		identificados. • Garantizar que la distribución de documentos está controlada. • Prevenir la utilización de documentos obsoletos • Aplicar la identificación apropiada de documentos y si son retenidos por algún propósito.	
ETAPA 5: CIERRE DEL PROYECTO			
#	**Actividad**	**Descripción de la actividad**	**Entregables**
	Informe final	Presentación del Informe final de resultados de la implementación del Sistema de Gestión de Seguridad de la Información en el ICFES. Este informe debe incluir como mínimo las conclusiones, y recomendaciones para seguimiento al SGSI. Realizar el plan de auditorías internas para el año 2016 para hacer el seguimiento y verificación del a implementación del SGSI.	Informe final de resultados de la implementación del Sistema de Gestión de Seguridad de la Información en la entidad es decir el plan de seguimiento, evaluación, análisis y resultados obtenidos del SGSI revisado y aprobado por la alta Dirección. Documento con el plan de auditorías internas, revisado y aprobado por la alta Dirección. Toda esta información (documentos) debe quedar preparada para ser gestionada dentro del Software de SGSI con que cuente el ICFES en el momento de la ejecución del contrato. Estos entregables y sus documentos estarán sujetos a la aprobación del supervisor del contrato.
	Soporte Post Implementación del SGSI	El Proveedor debe ofrecer sesenta (60) horas de soporte y acompañamiento post implementación del SGSI, para garantizar la estabilización del sistema y la atención de requerimientos de seguridad que se presenten.	Este tiempo se contará a partir de la entrega a satisfacción del SGSI. Actas de ejecución. Estos entregables y sus documentos estarán sujetos a la aprobación del supervisor del contrato.

EXPERIENCIA MÍNIMA ESPECÍFICA DEL EQUIPO DE TRABAJO

El proponente debe diligenciar el formato de hoja de vida con la experiencia requerida para cada uno de los roles, de las personas que ejecutarán el servicio especializado de seguridad en la implementación del sistema de gestión de seguridad de la información para el presente proceso, será el que se describe a continuación:

ROL	REQUISITOS ACADÉMICOS	REQUISITOS DE EXPERIENCIA
Gerente de Proyecto	-Debe tener título Profesional en alguna de las siguientes áreas: Ingeniería de Sistemas, o Ingeniería Informática, o Ingeniería Electrónica. Auditor Líder Certificado ISO 27001 y adicional deberá contar con alguna de las siguientes certificaciones vigentes: CISSP (Certified Information System Security Professional). o CPP (Profesional Certificado de Protección), o CISM (Certified Information Security Manager) o CISA (Certified Information Systems Auditor).	-Debe acreditar experiencia profesional de cuarenta y ocho (48) meses como gerente de proyectos de tecnología y/o seguridad de la información. -Experiencia específica gerenciando al menos (3) tres proyectos relacionado con la norma ISO 27001 Contar con al menos treinta y seis (36) meses de experiencia como consultor de seguridad de la información. , para lo cual deberá adjuntar las certificaciones expedidas directamente por las empresas contratantes.
Consultor Sénior en Seguridad	-Debe tener título Profesional en alguna de las siguientes áreas: Ingeniería de Sistemas, o Ingeniería Informática, o Ingeniería Electrónica. - Auditor Líder Certificado ISO 27001 Y adicionalmente contar con alguna o varias certificaciones como: Certificado CISA (Certified Information Systems Auditor) y/o CISM (Certified Information Security Manager) y/o CRISC (Certified in Risk and Control) y/o CISSP (Certified Information System Security Professional).	-Experiencia profesional de treinta y seis (36) meses en proyectos de consultoría de seguridad de la información. -Haber participado como mínimo en dos (2) proyecto de implementación de sistemas de gestión de seguridad de la Información, para lo cual deberá adjuntar las certificaciones expedidas directamente por las empresas contratantes.
Consultor de pruebas de seguridad	- Debe tener como mínimo título profesional en alguna de las siguientes áreas: Ingeniería de Sistemas, o Ingeniería Informática, o Ingeniería Electrónica. -Certificado CEH (Certified Ethical Hacker versión 6 o superior.) y/o OSCP (Offensive Security	-Experiencia profesional de treinta y seis (36) meses en realización de pruebas de seguridad. -Haber participado como mínimo en dos (2) proyectos de seguridad de la Información, realizando pruebas de vulnerabilidades, para lo cual deberá adjuntar las

	Certified Professional).	certificaciones expedidas directamente por las empresas donde se implementó el Sistema de Gestión de Seguridad de la Información.
2 Consultores complementarios del equipo del Proyecto	- Debe tener como mínimo título profesional en alguna de las siguientes áreas: Ingeniería de Sistemas, o Ingeniería Informática, o Ingeniería Electrónica. - Debe contar con la certificación ISO 27001 de auditor interno.	-Experiencia profesional de doce o (12) meses, en proyectos de consultoría de implementación de sistemas de gestión de seguridad de la Información.